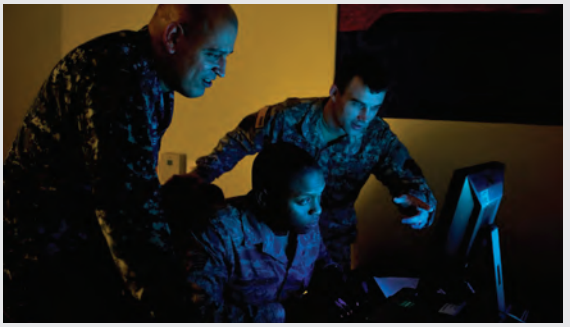
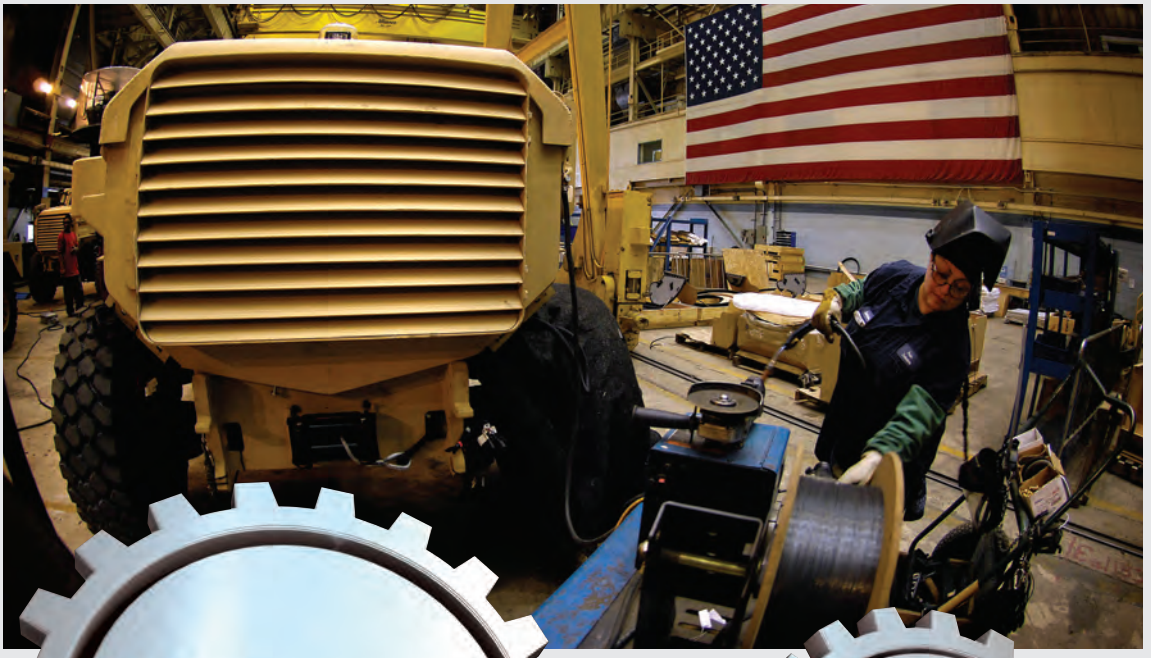
NDIA
National Defense Industrial Association

PROMOTING NATIONAL SECURITY SINCE 1919

TOP ISSUES 2014

NATIONAL DEFENSE INDUSTRIAL ASSOCIATION





ISSUE 1:
Chart a Future for Defense Industry

ISSUE 2:
Streamline the Procurement Process

ISSUE 3:
Help U.S. Defense Industry Compete for International Business

ISSUE 4:
Make IT Acquisition as Agile and Innovative as IT Development

ISSUE 5:
Secure Critical Infrastructure from Cyber Threats

ISSUE 6:
Assure Access to Energy and Make More of It While Using Less

ISSUE 7:
Educate the National Security Workforce

ISSUE 8:
Make it Easier for Small Businesses to Compete for 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

MAINTAINING A STRONG NATIONAL DEFENSE IN THE FACE OF SIGNIFICANT FISCAL CHALLENGES

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

The United States cannot maintain a strong defense without a healthy defense industrial base. Superior weapons and technology have become an essential element of American military power not only for winning wars but for deterring them. Whatever budget reductions DoD may face, Pentagon leaders must be able to make them with a focus on the long-term strength of the defense industrial base. We cannot prevent wars, or win them when necessary, any other way.

Some point to climbing stock values as a sign that the defense industry is doing well, but the industry is not as healthy as market prices suggest. The only recent real growth for defense industry has come from international sales and non-defense commercial sales. In many cases, share values have risen because of judicious workforce reductions, the repurchase of stock, and dividends paid to shareholders. These measures bolster a company's short-term outlook at the expense of long-term investments. But industry has no other option. Without clear guidance on what type of defense industry America will need, any dollar put toward long-term investment is as likely to be wasted as well-spent. In this period of budget reductions, sequestration, and uncertainty, the threats to the defense industry are more existential than at any other time since World War II. But if the Administration, the Congress, and the Department of Defense take into consideration the top issues described herein, defense industry may yet gain its footing for the coming years.

The legal and ethical exchange of information occurring at NDIA's many public conferences, symposia, exhibitions, workshops and seminars has been the principal vehicle for collaborative exchanges between the defense industry and government leaders. These NDIA forums have 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.

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: Chart a Future For Defense Industry

"To achieve an effective and affordable national security industrial base that will meet the needs of the coming years, the government must fundamentally change the way it conducts its business as the sole customer. To be successful, DoD must work closely with industry, Congress, and other key government agencies. In turn, industry must be prepared to respond and adapt to the evolving responsibilities of the supplier." Dr. Jacques Gansler, former Under Secretary of Defense for Acquisition, Technology, and Logistics, and at that time Chairman of the Defense Science Board Task Force on Defense Industrial Structure for Transformation, wrote these words in the cover memo for his 2008 task force final report. Dr. Gansler's message has only become more relevant in the intervening half decade, as the United States has concluded the War in Iraq, concludes the War in Afghanistan, contemplates what is meant by a pivot to Asia, and considers its post-war role in the world as the Arab Spring fades into winter, failing states become failed states, and the threat of transnational terrorism continues unabated.

Meanwhile, the reality of defense budgets in decline means that DoD must focus only on those aspects of defense manufacturing, production, and services it needs. If it does not set priorities, the Pentagon will over-invest in what it does not need, under-invest in what it does need, and maintain an inefficient defense industrial base designed for the last decade rather than for the next one. As Dr. Gansler proposed, we in defense industry are ready to respond and adapt to evolving responsibilities. But we can only do so with clear guidance from the Pentagon and Congress expressed in policy statements and program budgets. Our country cannot afford delay.

Recommendations

Create a Vision for the Defense Industrial Base

Challenge: There is no clearly-articulated vision of the defense industry of the next five to ten years and beyond. Although not necessarily a model for this coming period, Secretary Aspin's "Last Supper" in 1993 established a vision for the defense industrial base of that period. The debate over spending versus revenue, sequestration, and continuing resolutions year after year have paralyzed the Pentagon's ability to significantly restructure industry. Meanwhile, Congress has reacted negatively to the steps the Pentagon has taken toward significant change, such as the Air Force's budget in fiscal year 2013. Any significant new strategy for defense industry will need to come after a thorough and collaborative conversation between the Pentagon and the Congress and should review DoD's installation footprint and it's rapidly escalating manpower and operations and maintenance costs.

Solution: As part of the fiscal year 2015 budget review, the Armed Services Committees of both chambers of Congress should conduct hearings on the future of the defense industrial base. Real change and a new strategy cannot actually occur without first having this public discussion. And no one should expect that the conversation will resolve every issue or necessarily deliver up a clear vision for all of defense industry, but it should clarify the lowest common denominator of agreement among the parties, chambers of Congress, and branches of government. The hearings should explore what percentage of the DoD budget should go to investment, whether industry should consolidate and, if so, horizontally or vertically or both, how DoD will preserve real competition among its suppliers, whether DoD needs new tools to keep some bases of production on life support through difficult program cut-backs, how Congress can help DoD right-size other parts of its budget, whether defense firms should re-focus on commercial markets, how quickly the country can reconstitute lost defense production capacity and/or capability, how Congress and the Administration can help improve the system of export controls, and what role can and should international weapons sales play in sustaining defense industry. All sides must collaborate since neither the Pentagon nor Congress can unilaterally decide what defense industry will look like in the future.

Maintain the Defense Industrial Base We Need

Challenge: To maintain the defense industrial base our country needs, first we must know what we have in the industrial base today. DoD has initiated a Sector by Sector, Tier by Tier (S2T2) assessment of the defense industrial base which is intended to provide a baseline for any new vision. While this assessment is obviously perishable and requires effort to maintain, the information it provides is too critical to lose. The S2T2 study could also provide real-time information to DoD on how its program and budget decisions may impact long-term industry capability and capacity.

Further, as the country discusses its broader vision for the defense industrial base, DoD cannot preemptively lose capability that may later figure into that vision. As short-term program and budget changes threaten critical capabilities catalogued in the S2T2, when necessary, DoD should intervene to create or sustain competition, innovation, and essential industrial capabilities.

Solution: The S2T2 document should be a living, maintained, and on-going assessment of defense industrial base capabilities and capacity, continually refined, monitored, and used by DoD. The S2T2 assessment should expand to address what levels of activity are necessary to keep a capability viable. A living and well-maintained S2T2 will clarify overarching strategic acquisition planning, sustain critical capabilities, and limit adverse project-level acquisition planning that fails to identify and protect "bigger picture" industrial capabilities.

Further, as higher-level leaders decide that an industrial capability in S2T2 will not be sustained by the budget request, DoD can use mechanisms authorized by Title III of the Defense Production Act of 1950 (DPA, P.L. 81-774) to sustain the capability, such as direct investment in supplier infrastructure, leveraging research and development investments, procurement assistance, purchase commitments, or collaboration with other federal agencies. The Pentagon must request and Congress must provide levels of funding to the DPA that make it possible to step in and provide capability-saving assistance when other means are not available.

Design a Regulatory Process to Deliver the Industrial Base We Need

Challenge: DoD and the government in general have a famously sclerotic acquisition process, a matter explored specifically by Issue 2, "Streamline the Procurement Process." But in general terms, DoD is stymied by its own regulatory process from creating an industrial base that efficiently meets its needs.

Reports, studies, and initiatives recognize the inefficiencies created by DoD's regulatory framework time and time again. In 2010 DoD established the Better Buying Power initiative to increase efficiency and reduce costs. The 2012 House Armed Services Committee report, *Challenges to Doing Business with the Department of Defense*, recalled the 1994 Coopers and Lybrand study "which identified over 120 regulatory and statutory 'cost drivers' that, according to the contractors surveyed, increase the price DoD pays for goods and services by 18 percent." The report further states, "Despite the

many acquisition reform efforts that have taken place since that time, it is likely that costs, due to added regulations, have only increased. In 2012, the Defense Business Board recommended in its report to 'zero-base the entire system, including all directives and regulations.'" In May of this year, John Hamre, President and CEO of CSIS, wrote in *An Honest Look at the 'Military-Industrial' Complex* that "fully a third of our procurement dollars are going to 'overhead,' much of it dictated by the choking layers of redundant and competitive overseers." In April 2013, Secretary Hagel referred to the problem by saying "We need to challenge all past assumptions, and we need to put everything on the table."

DoD procures over $400 billion annually in goods and services; therefore, the cost of procurement overhead is somewhere between $80 and $130 billion each year not counting the billions consumed by internal acquisition personnel and processes.

Solution: The first step is to stop making the problem worse. As it conducts the Better Buying Power 2.0 initiative, the DoD—with thorough congressional oversight—should ensure that any new procurement process restriction or regulation is preceded by a publicly-available cost- benefit analysis posted in the *Federal Register*. That analysis should include a third party estimate of compliance costs with a review by private sector experts. All agencies would benefit from similar restrictions, and the Administration should consider putting a government-wide requirement in place.

Once DoD has slowed or even stopped the creation of new needless and burdensome regulations, it should subject regulations already on the books to similar scrutiny. NDIA has contributed to this review, having responded to DoD's request for suggestions by submitting nearly 200 separate recommendations to improve inefficient DoD processes or government-unique practices that add cost but yield marginal value. In addition to the work already done by NDIA, either the Pentagon or the Congress should establish a joint government-industry team tasked to examine the body of acquisition statutes and policy to see if each continues to satisfy the purpose for which it was enacted. After completing its review, the team should make recommendations to Congress and DoD to achieve a functional body of statute and policy that achieves Hagel's call for an acquisition system "that rewards cost-effectiveness and efficiency, so that our programs do not continue to take longer, cost more, and deliver less than initially planned and promised."

Invest in Improving the Government-Industry Relationship

Challenge: "Our study of defense management compels us to conclude that nothing merits greater concern than the increasingly troubled relationship between the defense industry and government." The preceding quote from the landmark 1986 Packard Commission report remains relevant today. A persistent but unfounded belief in defense industry profiteering compounds the mistrust when analysis shows that defense profit margins are typically a fraction of commercial profits. Thus industry clearly provides good value to the troops and the taxpayer.

As in all industries, some in the defense industry have not always met high ethical standards, but available data proves that on balance, defense industry can be trusted to deliver high-quality equipment at a reasonable price. The Department of Defense Inspector General's Semiannual Report to the Congress shows only rare improper billings. Indeed, as the Packard Commission observed in its own study so many years ago, "the nation's defense programs lose far more to inefficient procedures than to fraud and dishonesty. The truly costly problems are those of overcomplicated organization and rigid procedure, not avarice or connivance."

Solution: NDIA recommends the expansion of its Industrial Working Groups, where relevant industry and government leaders at the senior executive level convene to discuss matters of importance to the entire production sector. At present only five such groups exist to deal with matters of importance to chemical-biological defense, small arms production, ammunition production, test and evaluation, and program management. These groups provide a legal and ethical forum for all concerned parties to meet one another and transparently work through sector-wide problems while building trust and positive relationships. Clearly government and industry could both benefit from an expansion of this approach of collaborative problem solving. Because these entities depend on government participation, NDIA asks for the interest and participation of government purchasers in forming new Industrial Working Groups.

Bolster the Use of Defense Consortia for Research, Development, and Demonstration

Challenge: Despite declining budgets, DoD still needs to research, develop, and demonstrate new and innovative technologies. To do so it must gain access to new innovators while sustaining its current supplier base. Further, it must do

so in a way that leverages scarce resources without making the defense sector seem unattractive to the country's top scientists and engineers. Anything that reduces administrative lead times, the barriers separating individual services and their commands, and the barriers separating technology areas would all help DoD get more bang for its research and development dollar.

Solution: The best solution to all of these challenges is the use of defense consortia. Defense consortia are associations of industrial and academic institutions, organized along common interest areas for the purpose of developing and demonstrating weapon system technologies. Establishing a formal relationship between the DoD and a consortium in weapon system-specific technology interest areas creates a forum for engaging the broadest spectrum of industrial and academic resources with the fewest dollars.

Sec. 845 of National Defense Authorization Act of 1994 (P.L. 103-160), as amended by Sec. 804 of National Defense Authorization Act of 1997 (P.L. 104-201), authorizes DoD to enter into a legally binding "Other Transaction" (OT). OT authority is used for basic, applied, and advanced research and development or for prototype projects that are directly relevant to DoD weapons or weapon systems projects. The use of OT authority requires that at least one nontraditional defense contractor participates to a significant extent, or a mandatory one-third cost sharing for a traditional defense contractor. These requirements encourage networking and teaming opportunities among traditional and nontraditional companies, including small businesses and academic institutions, spur innovation and focus corporate internal research and development resources on technologies of mutual interest to DoD and industry.

Besides these advantages, using consortia alleviates the redundant processes of the current FAR□based contract for technology development, reducing the proposal-to-award process from 180-270 days to 60-120 days. Consortia also bypass the redundant procurement and contracting organizations found in the DoD and military services while engaging industry and academia collectively in full compliance with the Federal Advisory Committee Act.

Focus All Major Weapon Systems' Sustainment Strategies on Outcomes

Challenge: DoD must sustain all of its weapon systems through maintenance and repair for the projected lifetime of the system. The strategy for this sustainment has been based on discrete maintenance and repair events, for which DoD would contract with industry to provide spare parts and sometimes to perform the maintenance. This transactional sustainment strategy creates an incentive for industry to produce weapons in need of regular repair, since repair parts and maintenance activities contribute to the contractor's bottom line.

On the other hand, focusing weapons system sustainment on performance and availability outcomes rather than maintenance and repair events has achieved significant savings for DoD. Requiring a contractor to maintain a certain level of fleet-wide readiness, for example, simultaneously removes the burden and overhead from DoD while incentivizing quality production and maintenance techniques by the contractor in the interest of future savings. Outcome-based strategies firmly fix long term sustainment costs for the government and typically produce strong government-industry partnerships. Outcome-based sustainment strategies incentivize good behavior and quality work rather than the opposite and make the contractor, not the government, accountable when equipment fails. Individual government contracting officials retain the responsibility for the management and oversight of outcome-based strategy contract.

10 U.S.C. § 2327 requires DoD to employ outcome-based sustainment strategies for all major weapon systems. A recent *Proof Points Study* found that 12 of 13 programs that converted from transactional support to outcome-based support improved operational readiness at a reduced cost. Yet despite the statutory requirement for outcome-based strategies and the strong evidence that it is the better approach, over 80 percent of DoD product support is provided based on maintenance and repair transactions, not outcomes. Full implementation of outcome-based sustainment across all weapon systems would produce significant savings and improve logistics and sustainment.

Solution: DoD should fully implement outcome-based sustainment and complete business case analyses for all systems that are currently sustained on a transaction basis. This analysis should include a full cost accounting for transaction-based sustainment to guarantee, an accurate cost comparison with an outcome-based strategy, and a common and consistent definition of depot core capability to make effective public-private partnerships possible.

2

ISSUE 2: Streamline the Procurement Process

Despite perennial calls for improvement, failure typifies the procurement process. Legislators and regulators pursue corrective actions with good intentions, but the system grows increasingly unwieldy, in part due to proposed solutions. Meanwhile, the Pentagon's overhead costs spiral out of control, making it imperative that the remaining investment dollars be put to their best use.

Recommendations

Value Simplicity and Restraint in Defense Acquisition

Challenge: DoD must address the recent failures of its major defense acquisition programs. Some troubled programs are given development and production timelines numbering not in months or years but in decades, which they almost always exceed, have government-industry teams numbering in the thousand, have budgets that always grow with time and include multiple breaches of the Nunn-McCurdy Act (P.L. 97-252, 10 U.S.C. § 2433). (The F-22 Raptor is such a complex weapon that discovering the source of pilot hypoxia took four years of investigation to identify and correct.

What past major program failures share is a lack of proportion, simplicity, and requirements restraint. Instead of delivering success, failed programs have consistently produced long timelines, significantly increased budgets, and reams of changing requirements which have all contributed to failures.

Solution: As Dr. J. Ronald Fox of Harvard Business School suggests in the title of his book, *Defense Acquisition Reform, 1960–2009: An Elusive Goal*, fixes have not been easy to find. Members of Congress and political and military leaders looking for a quick solution will be disappointed. Failures of acquisition are not so often products of a flawed process, which legislation and regulation could address, as they are products of perverse incentives, inattentive management, and the absence of oversight. Yet the following steps, taken consistently over time, will yield positive acquisition outcomes.

- First, DoD leaders should only approve programs that will move from concept to full-rate production in a short timeframe. While some may scoff at the idea that a fully modern major vehicle program can be completed in just a handful of years, necessity is the mother of invention, as Plato said. Creating tight time constraints forces trade-offs in the user, engineering, and management communities to identify not all that a platform possibly could do but exclusively what it must do.

- Second, DoD leaders should shorten timelines which will certainly help reduce costs, since the largest cost driver for a major program is paying for technical manpower over long periods of time. Smaller budgets will also mean a preference for mature technologies in procurement programs and evolutionary rather than revolutionary advances in research and development. (Revolutionary advances typically don't materialize anyway, no matter how much money you throw at them.) Smaller budgets, like shorter timelines, also help separate wants from needs. Congress can help the DoD to shrink the size but grow the number of its program budgets.

- Last, DoD's programs need good management within the Pentagon and firm, consistent oversight from Congress. Everyone occasionally comes up with a hare-brained scheme, or forgets first principles and best practices. In those cases, civilian and military leaders at all levels need the courage to say no to their people. Congress must challenge a flawed premise rather than waiting for a program to utterly fail before terminating funding after sunk investments are lost. Early oversight in the concept phase and close scrutiny through the design phase will yield a better rate of success at a reduced cost.

Align the Requirements, Acquisition, and Budget Processes

Challenge: Currently, the business processes of a military service resemble a meal where one person orders the food, another person prepares it, and a third person pays. While this division of labor makes sense from the standpoint of how a military staff is organized—where operators develop requirements, acquisition professionals design the program, and comptrollers prepare and defend the program budget—the arrangement effectively shields any of the three camps from exclusive responsibility for an acquisition failure. The buck instead stops with the Service Chief of Staff, who has historically come from the operations community and may not have a thorough grasp of the principles that make some acquisition programs succeed and others fail.

Solution: The DoD and Congress should pilot proposals to more closely align military service business processes with each other and with industry, which is ultimately responsible for delivering the product itself. A pilot program might centralize the core responsibility for a program under one of the three functional areas, more strictly hold a Service Chief or Vice Chief accountable for program performance, or use collaboration with industry to help government streamline its requirements and program design.

Restore the COMMERCIAL in Government Commercial Item Practices

Challenge: Established technologies that do not require research and development by the government are less expensive than those that do. In addition to typically costing less, these commercial and non-developmental items are often state of the art goods, services, and solutions that require commercial demand to sustain their technological superiority, as in the case of information technology. Although government procurement authorities express preference for commercial items, statutory and regulatory changes of the past decade have inhibited access to them. In particular, additional differing military specifications and lengthy requirements lists make it difficult for government buyers to make commercial purchases.

Solution: In the near term, DoD should follow previous legislative and acquire commercial items, reaffirm the need for government purchasers to conduct fair and thorough market research, and reasonably limit the ability of government purchasers to add military-specific requirements to commercially-available products. In the long term, the Congress should order an industry-government overhaul of the laws and regulations that inhibit the purchase of commercial items by jointly conducting a cost-benefit analysis of each one.

Detect and Avoid the Use of Counterfeit Electronic Parts

Challenge: Sec. 818 of the fiscal year (FY) 2012 National Defense Authorization Act (NDAA) provides a strong baseline for preventing counterfeit electronic parts from entering the defense supply chain, and defense contractors continue to refine and enhance their internal systems to detect and avoid counterfeit electronic parts. But while Sec. 818 was a great start, it did not address important supply chain considerations and risk management business practices.

In that spirit of improving Sec. 818, NDIA supported Sec. 833 of the FY 2013 NDAA that protected contractors from financial liability for the repair or replacement of government-furnished property (GFP) as a result of the inclusion of a counterfeit or suspected counterfeit electronic part. This liability protection shields contractors when the contractor is not culpable.

While an improvement to the absence of policy that preceded it, the existing strict liability policy instituted by Sec. 818, as modified by Sec. 833, is the wrong approach. The current liability model assumes that liability for the repair or replacement of counterfeit or suspected counterfeit electronic parts "flows down" from one level of the supply chain to the next through sub-contracts, indemnifying prime contractors from risks in their supply chains. In practice, this assumption is false. Despite the presence of flow down language, contracts between prime contractors and subcontractors are individually negotiated and always represent a compromise of risk positions. While some companies' standard contract language does contain provisions requiring subcontractors to take full responsibility for delivery of a failed or counterfeit part, this language is frequently changed by the parties, with sub-tier suppliers limiting their liability in several ways, including making their liability subject to a limited express written warranty that applies only for a limited time (e.g. one year after delivery), adding an exclusion of any liability for incidental and consequential damages, and prohibiting any liability in excess of a fixed cap, often the total value of the contract.

Counterfeit parts are typically introduced several tiers deep in the defense supply chain. Flowing down liability becomes increasingly difficult from tier to tier because contracts are

worth less and less at the lower tiers. Eventually the risk of liability exceeds the value of the contract under the flow down model, and enforcement becomes illusory. A supplier with a contract worth $10,000 could face $50 million in retrofit costs. Even in a case where a lower-tier supplier agrees to a standard remedies clause, higher-tier suppliers and prime contractors may not be able to recover their remedial costs, whatever the liability provisions. Where the supplier is a small business, limits on liability are crucial to financial viability. Full subcontractor liability under the flow down model cannot be enforced and will lead to bankruptcy in some cases.

Solution: While the changes made by Sec. 818 and Sec. 833 are welcomed, they do not fully resolve the issue of liability for counterfeit parts in the defense supply chain. The Congress should enact further liability changes to target those companies that fail to implement counterfeit electronic part avoidance and detections systems, obtain counterfeit parts from a suspect source without implementing additional detection strategies, or fail to notify the government of counterfeits once they are detected. Congress should create broader safe harbors from liability for those companies that do take appropriate measures to detect and avoid counterfeit electronics. A failure to institute broad safe harbors will limit the ability of the DoD contractors to innovate, cultivate agile supply chains, or support government contracting and subcontracting goals to grow U.S. small business manufacturing capabilities.

Further, DoD should align itself with the intent of the counterfeit parts legislation by defining terms in a way the supply chain can enforce. Aside from the terms identified in the statutes themselves, DoD could further define "covered contractor," "trusted source or supplier," "becomes aware/ reason to suspect," and other terms that guide industry implementation and drive the resulting costs.

Properly Allocate Technical Data Rights

Challenge: A series of legislative changes has fundamentally changed the allocation of technical rights in defense contracting and created a complex, administratively burdensome intellectual property (IP) framework that contractors, subcontractors and commercial companies must carefully navigate to protect commercial and proprietary technical data delivered to DoD. Collectively, these changes have created uncertainty for contractors and subcontractors and have extended onerous requirements to commercial companies who provide technical data.

The FY 2007 NDAA ended the 10 U.S.C. § 2321(f) presumption of development exclusively at private expense previously afforded to commercial items after the enactment of the Federal Acquisition Streamlining Act (FASA) of 1994. The following year, the FY 2008 NDAA partially restored the FASA presumption for commercial items. However, the limited scope of the commercial definition requires that an item be "offered to the Government, without modification, in the same form in which it is sold in the commercial marketplace." Thus, the partially restored presumption is extremely limited (see the above recommendation on commercial items) and provides no coverage whatsoever for a contractor, subcontractor, or commercial company that adapts or modifies a commercial item or component.

The FY 2012 NDAA further altered technical data rights through Sec. 815, which guarantees the government the right to use technical data in the case of an item or process for which the contractor contributed less than 10 percent of the cost of development or an item or process that is integrated into a major system and either cannot be segregated from the system as a whole or was developed predominantly at government expense. DoD has not yet issued draft regulations implementing Sec. 815.

Solution: The U.S. Government would be best served by providing industry an opportunity to provide input to the regulation implementing Sec. 815. NDIA encourages its members to offer or use commercial products to satisfy military requirements to limit the applicability of 10 U.S.C. § 2320(b)(9) to commercial items and processes. In future legislation, Congress should exempt technical data associated with commercial items or processes, and for all other commercial items or processes, Congress should limit the applicability of technical data rights to only the technical data customarily provided to the public with the commercial item or process. (This limitation should exclude technical data related to form, fit, function, repair or maintenance, installation, operating, handling, or when the technical data provided to commercial users is not sufficient for military purposes.)

Make Contractor Labor Rates More Flexible

Challenge: The FY 2012 NDAA placed a temporary limitation on the aggregate annual amount DoD could pay for service contracts in FY 2012 and 2013. The provision froze the amount available for each of those years at the level of the President's Budget request for FY 2010. The provision also required the Secretary of Defense to establish, for contracts and task orders over $10 million awarded in fiscal years 2012

and 2013, a negotiation objective for labor rates and overhead rates not to exceed those rates paid to the contractor in fiscal year 2010.

Although the cap is a "negotiation objective" and not a mandate, some DoD agencies have used it as a cap. For example, several Navy commands have issued "tripwire" memos mandating high-level reviews for contracts that exceed the suggested cap, needlessly delaying decisions and harming businesses.

Due to the continuing fiscal austerity, federal agencies need flexibility now more than ever to implement funding reductions. While NDIA sympathizes with federal employees whose rates of pay remained steady from 2010 through 2013, the government contracts for services it cannot perform, or cannot perform as economically, as private industry. Any measures addressing service contracts should focus on the outcomes and program achievements of contractors relative to the expense rather than an arbitrary cap on labor rates.

Besides reversing the basic model for all contracts, which is pay for performance, freezing labor and overhead rates ignores market factors (meaning that the quality of human capital diminishes over time as qualified workers leave for better-paying jobs) and the expense of conforming to government mandates that drive up costs.

Solution: Congress should reject arbitrary caps and should instead focus on reinforcing contract pay for performance. Congress can effectively reinforce that principle by providing agencies with the discretion to achieve overall spending reductions consistent with mission needs.

Adhere to the Regulatory Process

Challenge: 41 U.S.C. § 423 requires that agency heads must publish agency acquisition regulations in the *Federal Register* for public comment when those regulations have a significant effect beyond the internal operating procedures of the agency or have a significant cost or administrative impact on contractors. Contrary to this requirement, in 2012 agencies published more than one-third of their interim and final Federal Acquisition Regulation (FAR) rules without notice or comment period. The DoD published almost half of the interim or final rules without an opportunity for the public to comment in advance. The rulemaking process is designed to improve agency regulations by inviting comment by outside experts and to keep the public informed. Failure to provide the required notice and comment period deprives the agency and the taxpayer of better, more effective regulation.

Equally troubling is the increased use of so-called class deviations—memoranda allowing acquisition executives to deviate from FAR rules for a specified class of acquisition activities. This type of rulemaking is necessary and appropriate when an agency has a statutory or policy reason to follow a different procedure than those specified by the FAR. Every procurement agency also has authority to create a one-time deviation for a unique solicitation. NDIA notes that the use of class deviations has increased significantly over the past several years. The DoD issued eight new class deviations and repealed one class deviation in January and February 2013 alone. In 2012, the DoD issued a total of 18 class deviations.

Worse still, in recent years the DoD has substituted guidance memoranda for rulemaking. On November 28, 2012, the Under Secretary of Defense for Acquisition, Technology, and Logistics and the acting Principal Deputy Under Secretary of Defense for Personnel and Readiness issued a joint memo titled "Enterprise-wide Contractor Manpower Reporting

Application." The memo requires DoD components to revise all contracts for goods and services with defined requirements. As of early 2013, DoD was using the contract clauses specified by the memo, but it has still not published a rule or class deviation. Similarly, the Air Force issued a November 13, 2012, memo to all Air Force contracting offices relating to implementation of contractor inventory reporting requirements. It directs contracting officers to "amend solicitations with the attached pre-solicitation statement" and to "modify existing contracts to reflect the (same) requirement." As of early 2013, DoD has made no public notice of these external actions nor published any changes to the DoD or Air Force acquisition regulations.

Solution: Agencies need flexibility to manage the regulatory process, and both 41 U.S.C. § 423 and the FAR offer the flexibility to address urgent or agency-unique circumstances. But whatever path a regulation may take, the regulation itself will be more effective if it is published and offered for comment by outside experts, even ex post facto comment if necessary. Therefore NDIA recommends that Congress consider amending 41 U.S.C. § 423 to require the FAR Council, with respect to the FAR, and each agency, with respect to its own agency-specific acquisition regulations, publish all new rules, class deviations, and memoranda with an impact on procurements on a public website and in the *Federal Register*. These publications should solicit public comment, even ex post facto, and publication should occur within two weeks of the adoption of the new rule. If timely publication is impracticable, notice shall be posted as rapidly as possible along with reasons for the delay. Congress should consider legislation to prohibit agencies from applying any class or one-time deviation unless it is made public and published as specified above.

3

ISSUE 3: Help U.S. Defense Industry Compete for International Business

One of the few bright spots for U.S. defense industry over the last several years of budget turmoil has been international sales. While international business can hardly replace substantial reductions in U.S. defense spending—since many of our allies and partners are also reducing their defense budgets as well—a well-timed international program can keep a business, supplier, or industrial base capability functioning when it might otherwise shut down. Therefore it is critical both from an industrial base sustainment perspective as well as an economic growth perspective for the United States to remove unnecessary fetters from international defense sales.

Recommendations

Continue the Export Control Reform Initiative

Challenge: The U.S. export control system is outdated, and the Administration has made efforts to reform it. That effort is critical to future innovation, manufacturing sustainment, and global competitiveness for U.S. defense industry. Particularly as defense budgets decline, U.S. defense industry must avail itself of all opportunities—domestic and foreign—to compete for contracts.

Solution: Many overdue reforms can be accomplished administratively without new legislation. For those regulatory changes, agencies should coordinate closely with defense industry to protect selected key U.S. technologies while allowing U.S. industry to compete in the international defense and security market. NDIA recommends that Congress consider the creation of a positive U.S. Munitions List that requires that the Commerce Department, with the coordination of the DoD and the DoS, oversee the trade of all items that do not pose national security concerns.

Encourage Defense Technology Transfers among U.S. Allies and Partners

Challenge: The United States military increasingly operates in tandem with allies and partners, and the success of coalition operations is helped by interoperable materiel and tactics. U.S. forces should also benefit from advanced ally and partner technologies. Both the sharing and receiving of improved technology requires the timely transfer of defense articles and technology among trusted partner and allied nations. Technology sharing is subject to export controls, but those controls should be efficiently and transparently administered.

Solution: The Administration should continue to invest it its Export Control Reform and Technology Security and Foreign Disclosure Initiatives, both of which should enable prudent defense technology transfers among our allies and partners. The U.S. defense industry should closely monitor both efforts and make necessary recommendations to the Administration to be sure they achieve their desired goals.

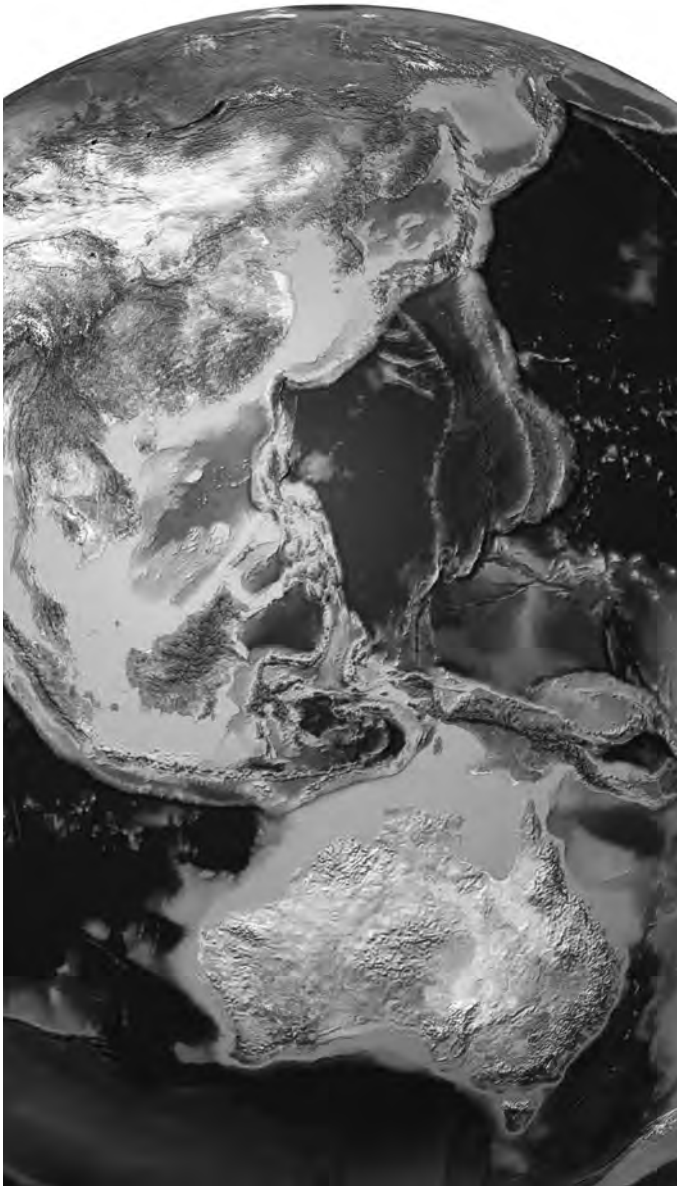
Fully Implement the U.S.-U.K. and U.S.-Australian Defense Trade Cooperation Treaties

Challenge: While the Defense Trade Cooperation Treaties with the United Kingdom and Australia enable appropriate technology transfer and co-development of defense technology, to date these treaty exemptions have been used only sparingly due to disincentives embedded in the regulatory implementation requirements. To be successful, the use requirements of these treaties must easily integrate into business processes.

Solution: All three governments should ensure that the regulatory implementation of these treaties fully supports the intent of seamless, rapid cooperation. Success will mean the creation of an attractive alternative to traditional defense licenses, with no new liabilities for U.S. companies.

Support the U.S. Strategic Rebalance to the Asia-Pacific Region

Challenge: The Administration's pivot to the Asia-Pacific should allow for more U.S. defense industrial integration with allies and partners in the region. That increased partnership should include Australia, Japan, and the Republic of Korea, including equipping partners to protect their own air and sea lanes with effective intelligence, surveillance, and reconnaissance capabilities interoperable with U.S. systems. In particular, Japan must liberalize its arms export procedures to enable armaments cooperation with the United States. Likewise, the United States must itself make it possible for U.S. defense industry to forge connections with emerging partners in Asia



who would like to grow their defense capabilities but cannot afford the most advanced systems.

Solution: The Administration should work with Japan and other close regional allies to ensure their export controls will allow for mutual sharing of defense articles. For emerging partners, DOS must have in place an export control system that can allow the transference of less cutting-edge technologies to help cultivate current regional partners into future close allies.

Pass Naval Vessel Transfer Legislation

Challenge: The U.S. Navy needs naval vessel transfer legislation to decommission and transfer Perry class frigates and other ships to our allies. The program is funded by foreign military sales money, is a job creator for U.S. industry, and saves Navy "mothballing" money by allowing "hot transfers" that further enhance the operational capabilities of allies and partners. Each frigate transfer equals $55–60 million in U.S. labor and services. Each transferred ship further creates sustainment opportunities for U.S. defense industry with foreign partners.

Solution: As the Administration has provided Congress with all the necessary information and rational justifying the transfer of these vessels, Congress should expeditiously pass the necessary transfer legislation.

Support Security Cooperation Reform Initiatives

Challenge: Security cooperation and foreign military sales (FMS) are critically important to sustaining our defense industrial base during a period of budget austerity. DoD should continue to improve its security cooperation and FMS business processes to make them more efficient.

Solution: NDIA endorses the security cooperation reform initiatives by the Defense Security Cooperation Agency (DSCA) to improve its business processes from program conception to delivery. DoD and DSCA should continue to incorporate Better Buying Power practices.

4

ISSUE 4: Make IT Acquisition as Agile and Innovative as IT Development

For years, the government's acquisition of information technology (IT) has lagged far behind IT innovation in the commercial sector. DoD has struggled to marry up its unique security and military specifications with hardware and software designed for business and personal use. In some cases, this divergence has led DoD to develop and acquire its own systems which have rarely proved to be of a quality approximating what is available on the commercial market. In other cases, DoD either adopts commercial systems late after they are adjusted to accommodate military-specific needs, or DoD adopts a commercial system that does not meet mission assurance standards. Rather than either of these sub-optimal approaches, DoD should consider adjusting its acquisitions to the unique innovation and development environment of the IT sector.

Recommendations

Acquire Cutting-Edge, Secure IT

Challenge: Defense acquisition programs are notoriously ponderous, bureaucratic, and slow—all qualities that contrast with the agile and quickly evolving IT sector. If DoD is to purchase the very best secure and effective IT, it will need to adopt purchasing practices that conform to the pace of IT innovation. Any other purchasing practice will yield obsolete IT

solutions unable to adapt to cyber threats that constantly probe and exploit our weaknesses.

Sec. 804 of the National Defense Authorization Act for Fiscal Year 2010 Public Law 111-84) directed the DoD to "develop and implement a new acquisition process for information technology systems." While this mandate led to a report with proposed reforms, as yet those reforms have not been implemented. Today's acquisition system cannot produce the agile outcomes the threat environment requires and Congress demands. Further, the new information assurance policy codified in the rewritten DoD Instruction 8510.01 could make a slow acquisition process even slower. Until acquisition policies are rewritten to deliver speed and security, IT acquisition will remain a significant problem.

Solution: DoD should fully implement the provisions of section 804 as soon as possible. In addition, DoD should thoroughly review the various ad hoc solutions that creative procurement executives have used to skirt the standard acquisition process—including indefinite delivery, indefinite quantity contracts with minimal task order procurement steps, special rapid acquisition processes, and single point procurements used to align with cycle of IT innovation—to determine if any could become a standard process for IT acquisition with necessary modifications. While these alternatives show promise, they remain exceptions to the rule rather than the rule itself.

Make Sure Innovative Technologies are Trusted and Secure

Challenge: Government and industry users want the latest and greatest gadgets, technology innovations, and communications tools. Unfortunately, some of these gizmos, web-portals, and apps are not built with security in mind. Yet policies that prohibit or significantly limit the use of these tools are likely to damage morale and are unlikely to be followed in any event.

For example, federal cloud storage has only become more popular in government since it first became an NDIA top issue last year. Cloud data storage poses new and unique cyber security challenges that the government must account for in any federal cloud solicitation.

Everyone wants the newest handheld device. But the ability to conduct one's work anywhere on a new and unproven device—particularly when some of that work may be classified—is uncharted territory. Network connections must be secure and the device itself must be secure from intrusion, among many other challenges.

Further, social media has become a widely accepted business tool in the Pentagon and the private sector, but embracing the most popular communications tools comes with risk. Any new communication tool becomes a vector for social engineering attacks and a temptation to be lazy about information assurance.

Solution: New IT tools need a speedy evaluation and fast security policy guidance. The Congress should mandate the creation of a cell that evaluates new technologies for the entire U.S. Government and quickly develops policies for how those technologies can be used safely depending on how tightly the device, system, or information must be secured. Having a small cell create timely government-wide policies limits the number of ad hoc or suboptimal practices.

As the Executive Branch develops security procedures, it should rely heavily on solutions developed in the private sector. Government may also be able to draw on industry best practices when consider how to safely use new technologies.

As in all security situations, IT demands continual vigilance on the part of government security personnel, including red team exercises, and regular oversight from the Congress. Because the cyber security landscape will keep evolving, we should not pretend that a couple of one-time solutions will solve our problem. This is likely to be an NDIA Top Issue for many years to come.

Strengthen the DoD Chief Information Officer (CIO)

Challenge: Information availability and demand have both grown exponentially with the shift to mobile computing. Military requirements and expectations have evolved with the commercial landscape. IT innovation has also benefited our adversaries. DoD faces dual challenges of leveraging advanced IT while defending against new threat vectors. Neither of these challenges existed when DoD established its CIO function. Without a stronger and modernized CIO function, DoD is likely to fall short.

Solution: DoD should take a series of related steps to strengthen its CIO position. First, it should carefully consider how to execute enterprise-level strategies, such as the Joint Information Environment, while improving information processing, network management, and information assurance, and cyber security. DoD should aim to meet these needs while saving money from virtualization, re-use, and consolidation. Second, DoD should evaluate how other federal agencies have aligned their CIO functions and assess how well those alignments support their missions. Third, DoD should consider the industry approach of establishing a powerful CIO who reports directly to the CEO to realize the full benefits of centralized and empowered strategy. Last, however DoD may choose to organize and empower its CIO, it should provide the position with the statutory and directive authority necessary to implement IT policies, procedures, and practices across the entire DoD enterprise.

5

ISSUE 5: Secure Critical Infrastructure from Cyber Threats

Defense industry approaches cyber security from two perspectives. First, as contractors to the federal government, defense firms must adhere to applicable laws and regulations such as the Federal Information Security Act (44 U.S.C. § 3541, P.L. 107-347). Second, as private companies holding valuable information, threat actors (e.g., nation states, criminals, terrorists, hack-tivists, and insiders) target defense firms. The dual importance of cyber security makes it an issue meriting immediate action.

Recommendations

Pass a Cyber Security Law

Challenge: Although Congress has contemplated legislation on cyber security for several years, its failure to pass a bill in 2012 led to the President's issuance of an Executive Order entitled "Improving Critical Infrastructure Cyber security" (EO 13636). As one element of U.S. critical infrastructure, the Executive Order directly impacts the defense industrial base.

The Executive Order directs various agencies to make recommendations for improving critical infrastructure cyber security. The National Institute of Standards and Technology (NIST) has drafted a Cyber security Framework that establishes "a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address

cyber risks." The Department of Homeland Security (DHS) will expand its Enhanced Cyber Security Services information sharing program and implement the NIST Cyber security Framework by creating incentives for companies to adopt the Framework. The Framework itself is scheduled for implementation on February 12, 2014, and as of that date defense firms will have new "voluntary" standards. These standards may also evolve into new "best practices" for defense industry cyber security, which may then translate into increased costs for compliance.

Further, the Executive Order directs the Department of Defense and the General Services Administration to recommend "the feasibility, security benefits, and relative merits of incorporating security standards into acquisition planning and contract administration." By implication the newly recommended security standards may become a prerequisite to submit bids for government contracts.

Last, the Executive Order instructs agencies to determine how they can improve cyber security under their existing authorities, including proposing new rules.

Solution: While the Executive Order is preferable in the absence of legislative guidance, it is far less preferable than a fully-negotiated and thoroughly-considered cyber security law passed with bipartisan support. NDIA urges Congress to work together with industry to resolve its outstanding problems and secure final passage of cyber security legislation. In the meantime, the Congress should closely oversee the implementation of the Executive Order to ensure that cost-benefit analyses are performed for all new "voluntary," but de facto mandatory, cyber security compliance measures, and to assist defense industry in securing venues to voice its concerns with new cyber security rules to the government regulators proposing them. All these actions should occur with an eye toward establishing a long-term public-private partnership in cyber security.

Work with Industry to Stop Insider Threats

Challenge: The U.S. Government pays billions of dollars annually for a vast counterintelligence and security establishment, but a handful of high-profile leak, terrorism, and workplace violence cases demonstrate that these measures still have gaps. Particularly for cyber security, the recent significant public release of sensitive classified data demonstrates that the U.S. intelligence community has done insufficient work to revisit and update its counterintelligence tradecraft for the internet era. Significant increases in classified information an explosion in the number of cleared individuals—mutually

reinforcing phenomena—also increase the likelihood that real secrets will fall into the wrong hands.

The U.S. security establishment needs to shift from its process orientation to a threat orientation. Today the government spends huge sums of time and money ensuring that those entrusted with secrets pass through a standard set of processes meant to gauge their overall trustworthiness. The same philosophy guides how clearances are passed and how access is granted to compartmentalized information. Although the processes overlap and form a type of defense-in-depth, their inherent predictability and systematic operation make them relatively easy for a determined bad actor to overcome. Furthermore, because so much time and money is invested in procedural approaches to security, very little investment of time, money, or energy is devoted to a threat-based approach to security.

Solution: The Executive Branch and Congress should pilot new approaches to cyber security (and physical security) against insider threats before scaling them up for community-wide adoption. Many of these measures will involve "crowd-sourced" security where all employees take responsibility for securing information, detecting insider threats, and reporting unusual behavior. In places where information is truly valuable and the United States cannot afford any leaks, "dual-key" measures and other practices developed and perfected by the nuclear establishment can help stop insider threats. No-notice and red team exercises should be considered. Technology-

enabled network surveillance can combat the insider cyber threat by detecting anomalies in user network behavior. Last, the government should adopt realistic training as opposed to the current compliance-driven "minimum required" model.

Government should consider industry its partner and resource in each of these approaches. The simplest way for government to quickly and effectively evaluate different cyber security solutions is to rely on trusted and secure contracts rather than investing in new security institutions and bureaucracies, which inevitably become sclerotic and process-driven. New approaches to security should favor innovations created and implemented by the private sector in concert with the Administration.

Improve the Cyber Security of the Manufacturing Supply Chain

Challenge: DoD is the world's largest purchaser of manufactured goods. As manufacturing supply chains become increasingly complex and global, the information that passes between nodes in the supply chain is susceptible to theft, sabotage, and exploitation. The results range from undetected access of military information to a loss of military capability and superiority.

While many of the well-publicized efforts involve attacks on larger companies, enemies can obtain sensitive information more easily and with less risk of detection. According to a recent report from the Stanford Graduate School of Business, "over 50 percent of the information exchanged between trading partners travels over fax, email, and phone." That percentage is likely higher in manufacturing supply chains, where technical product data and specifications and production processes are exchanged using unsophisticated means, particularly at the lower-tier suppliers. Much of DoD's manufacturing information can be located with a simple Google search.

Solution: The Administration should direct government agencies to work with industry to create a common manufacturing information system that allows manufacturers up and down the supply chain to exchange information while keeping it protected. The Administration should also direct government agencies to provide the small- and medium-sized manufacturers with training on information security and how to properly use of the new manufacturing coordination infrastructure.

6

ISSUE 6: Assure Access to Energy and Make More of It While Using Less

The Department of Defense is one of the largest consumers of energy in the world. U.S. security depends on our ability to maintain secure sources of energy. Because energy security is a basic enabler of American military power, addressing ongoing energy challenges is a top priority.

Recommendations

Invest in Energy Solutions

Challenge: DoD is the nation's largest energy user. DoD depends on traditional fossil fuel sources of energy. Last year, this heavy dependence on fossil fuels created a dramatic budget shortfall for the Army's overseas contingency operation account, leading to an $8 billion reprogramming of funds from other program accounts. Not only does a transfer of that much money away from other investments substantially harm DoD's ability to modernize its equipment and support other critical needs, but it reveals a deep and worrisome vulnerability in our country's ability to project power. Moreover, some of the individuals who profit from U.S. purchases of foreign oil underwrite committed enemies of the United States around the world.

Solution: The Administration should take an "all of the above" approach to developing assured domestic sources

of energy. Commendably, DoD has launched 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. Breakthroughs in these technologies will also create future commercial opportunities. History demonstrates that defense-sector innovation leads the way in developing next generation civilian commercial technologies. Congress should strongly support and fully fund DoD innovative energy solutions.

In the meantime, while DoD and commercial markets develop alternative energy sources and bring down the cost of these new technologies, Congress and the Administration should develop new assured sources of traditional energy. New sources of energy will drive down cost by increasing supply. More domestic production of traditional fuels limits our vulnerability to foreign powers and the off-shoring of our wealth.

Use Nuclear Power

Challenge: 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 percent by 2035. While wind and solar power are promising sources of plentiful renewable 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.

Solution: Small modular reactors (SMRs) are 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 sufficient energy demand to make SMR fabrication a cost-saving investment. Producing SMRs also gives DoD the chance to tackle some of the safety concerns involved in the increased use of nuclear power, including vulnerability to natural disasters and terrorism and how to safely dispose of spent fuel sources.

SMRs can be coupled with other energy sources, including renewable and fossil fuel energy, to leverage all energy resources, produce energy more efficiently, and increase grid stability and security. Some advanced SMR designs can produce a higher temperature process heat for either electricity generation or industrial applications.

DoD should request, and Congress should fund, cost-sharing projects to build modern and safe SMRs for use at military installations adjacent to civilian communities that can also benefit from an uninterrupted and entirely secure supply of energy that reduces DoD's energy costs.

7

ISSUE 7: Educate the National Security Workforce

The national security workforce will not sustain itself without careful planning and execution by the U.S. Government. Particularly in the areas of science, technology, engineering, and mathematics education, and cyber security training, the government should partner with industry to make sure the defense workforce is educated and trained for the jobs of tomorrow.

Recommendations

Rapidly Expand Science, Technology, Engineering and Mathematics (STEM) Education

Challenge: Our economic growth and national security rely more than ever on a technically- educated and -skilled workforce. To maintain our economic and military advantages, we must swiftly enlarge the STEM talent pool.

DoD and defense industry are critically dependant on STEM skills. Over 25 percent of the STEM workers in the defense industrial base are currently eligible to retire. That number will exceed 35 percent within five years. Further, DoD faces a shortage of STEM-interested and clearance-eligible students. Only 17 percent of high school-age students have a proficiency and interest in STEM. 25 percent have proficiency but no interest. This proportion is too low to replace retiring STEM workers.

Solution: Currently, support is provided to increase STEM skills through remedial programs to provide training to college and work entrants. This approach is both expensive and difficult in period of budget austerity. The Administration must create, and the Department of Education must implement, nationwide STEM programs. Lagging interest and proficiency in STEM means we need better teachers with industry-competitive incentives, nationwide best practices, and coordinated outreach to underserved student populations, including minority and female students. The status quo of the United States lagging behind competitors is unacceptable.

Other agencies and sectors should also consider marketing STEM to students. DoD uses advertising to attract recruits, and advertising and marketing campaigns could similarly attract young people to STEM education and careers. Current efforts are not effectively engaging students enough to persevere through difficult STEM subjects. If students are engaged, studies show they persevere through difficulty.

In the meantime, the White House Office of Science and Technology Policy should partner with NDIA and its members to collaborate on mutual efforts to stimulate STEM interest. This approach would energize assistance from the defense industrial base.

Educate the Cyber Security Workforce

Challenge: The United States needs a larger and more capable cyber security workforce. In April 2010, the Administration announced the National Initiative for Cyber Security Education (NICE), an education initiative coordinated by the National Institute of Standards and Technology. NICE will directly impact defense contractors, especially in the area of workforce training and professional development, where DoD is one of three agencies named to lead the effort.

To be successful in this endeavor, government must partner with private industry and academia. In addition to leveraging the know-how resident in the private sector, the government should partner with industry to certify cyber security professionals based on a common set of credentials for which the U.S. education system has developed degree or certificate paths. These credentials should also include continuing education requirements to keep the workforce up to date.

Solution: The Administration should create and Congress should authorize and fund a cyber security education program that specifies how the government will partner with and leverage the cyber security and education capabilities resident in industry.

8

ISSUE 8: Make it Easier for Small Businesses to Compete for Government Contracts

Small businesses face special challenges when competing for contracts with the government, whether that competition involves only other small businesses or also large corporations. The U.S. Government must take care that its programs meant to protect small business competitiveness are accomplishing their intended goals.

Recommendations

Even the Playing Field When Small Businesses Compete with Each Other

Challenge: The lack of parity among various types of small businesses limits the flexibility of contracting officers to seek innovative solutions while meeting small business contracting goals. Existing small business preference programs create a diverse set of regulations related to contract size, special competitive rules, eligibility for set-asides, and so forth. Because of these rules, contracting officers do not always have the ability to "plug in" any one of the several categories of small businesses, including woman-owned, service-disabled veteran-owned, HUBZone, and others. Sec. 1347(b) of the Small Business Jobs Act of 2010 (Public Law 111-210) removed the order of preference from the various small business preference programs, but until the programs are unified under a common and simple structure, small businesses will not have an even playing field and contracting officers may be forced to choose a less-qualified small business alternative instead of a better-qualified alternative due to the variety of small business contracting rules involved.

Solution: The Administration should create a universal set of standards for the entire community of small business preference programs that would grant maximum flexibility to contracting officers choosing from among different small business options.

Fix Flaws Created by the Reauthorization of SBIR and STTR in 2012

Challenge: When Congress reauthorized the Small Business Innovation Research (SBIR) and Small Business Technology Transfer program (STTR) programs in the FY 2012 NDAA, (Public Law 112-81) the subsequent implementation by the Small Business Administration (SBA) revealed flaws.

The SBIR program is designed to increase the participation of small, high technology firms in federal research and development (R&D) endeavors, provide additional opportunities for the involvement of 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 for use by small businesses to support mission-related work.

Further, the 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.

When Congress last reauthorized the SBIR and STTR programs, SBA proposed rules that would allow foreign-owned companies to compete for SBIR and STTR grants. Instead of requiring "domestic" to mean U.S.-owned, the SBA proposes only that a concern have a place of business located

in the United States. There are no rules to determine whether a venture capital company incorporated in the United States is actually a foreign-owned investor group. The new SBA rules eliminate affiliation tests for large minority shareholders and make exceptions for the SBIR program only, expanding the eligibility to firms that are not eligible for other small business programs. Last, the rules do not clearly stipulate SBA's role in enforcing the data rights of small business owners under SBIR.

Solution: 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 and STTR sections in the fiscal year 2012 NDAA legislation. DoD should create official policy for SBIR reporting goals and incentives as defined and consistent with the legislative intent outlined in the 2012 NDAA.

Keep the FAR Fair to Small Businesses

Challenge: Some parts of the Federal Acquisition Regulation (FAR) 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: that offers will be obtained from at least two responsible small business concerns offering the products of different small business concerns, and that the award from the set-aside will be made at fair market prices.

An amendment to the FAR was recently proposed that contracting officers shall set aside acquisitions for R&D 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. No clear reason is given for why R&D contracts should be held to a different standard than other small business contracts.

Solution: R&D contracts should be treated the same as all other contracts for small business set asides. Currently only eight percent of R&D contracts are awarded to small businesses—far below the government-wide goal of 23 percent. Providing set-asides with the same standards as other contracts could alleviate part of this shortfall.

Understand the Risks Involved with Federal Strategic Sourcing Initiative (FSSI)

Challenge: Some small business have expressed concern that FSSI will push them out of the government marketplace due to the sheer scale of FSSI acquisition programs.

In November 2005, the General Services Administration and the Department of Treasury launched FSSI to allow the entire government to work together across agency boundaries to purchase commodities used by multiple agencies, such as express and ground delivery services, office supplies, printer commodities, and telecommunications and wireless tools.

FSSI brings together the entire government's buying power to improve vendor performance, obtain lower bulk prices, and achieve vendor business practice and environmental goals.

Solution: Although FSSI seems to have achieved its initial goals, its long-term impact on the ability of all qualified small businesses to contract with the government is not well understood. The Department of Defense Strategic Sourcing Directors Board should review and report on the impact of FSSI on small businesses that sell commodities that are now, and planned for in the future, covered by FSSI.

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

Will Goodman
Director, National Security Issues Development and Legislative Policy
Phone: 703-247-2595
Email: wgoodman@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