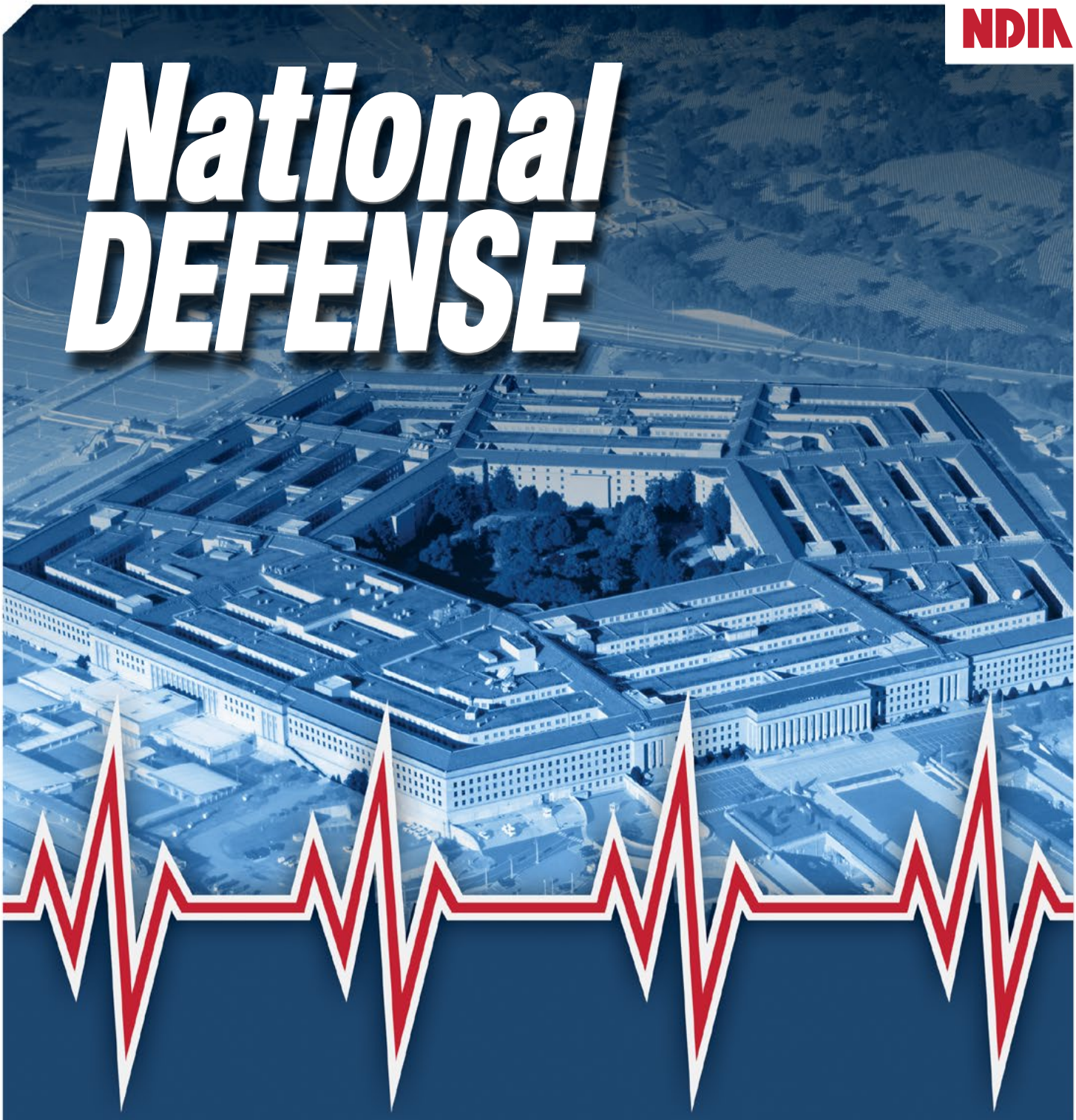
NDIA

National DEFENSE

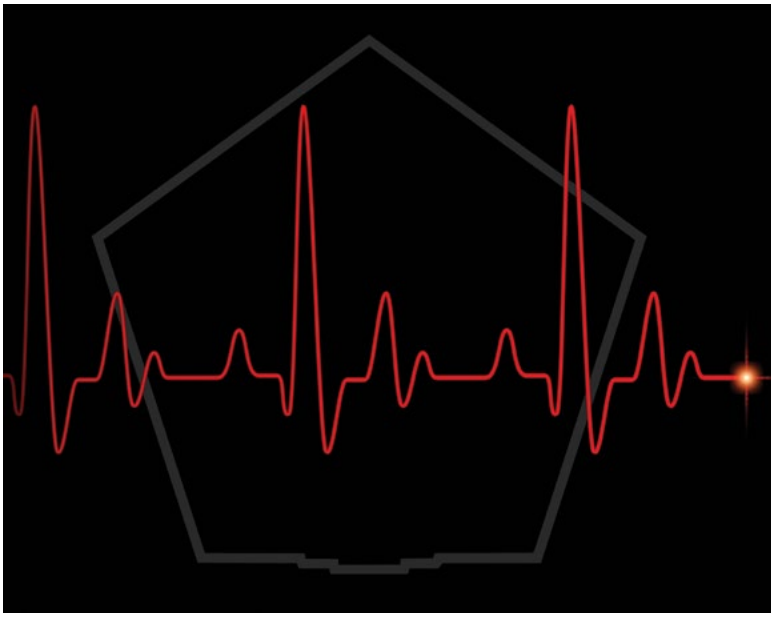


DEFENSE INDUSTRIAL BASE VITALITY OUTLOOK

COMPANION PUBLICATION TO NDIA'S STUDY,
"VITAL SIGNS: THE HEALTH AND READINESS OF THE DEFENSE INDUSTRIAL BASE"

SPECIAL REPORT

The Health of the Defense Industrial Base



The National Defense Industrial Association, partnering with data science company Govini, has kicked off an annual project called "Vital Signs." The subtitle of the report is "The Health and Readiness of the Defense Industrial Base." The assessment focuses on standardizing and integrating analyses of different elements of the sector and the business environment shaping its performance. This year's mediocre "C" grade reflects a business environment characterized by highly contrasting areas of concern and confidence.

Along with details from the report, *National Defense* has taken a further look into three of the its findings: the shortage of science, technology, engineering and math (STEM) talent; the ability of industry to protect itself from cybertheft and its ability to surge production in wartime.

Stew Magnuson
Editor in Chief
National Defense

ISTOCK

Table of Contents

DEFENSE DEPT.

Defense Industrial Base's Report Card Reveals 'C' Grade

BY WESLEY HALLMAN AND CHRISTOPHER SMITH

The Executive Order 13806 report on production risks to critical defense industrial supply chains in 2018 starkly framed the health of the U.S. defense industrial base as key to the readiness of the nation's armed forces to confront near-term threats and their ability to compete long-term against strategic adversaries.

Despite its high-resolution snapshot of the sector's "unprecedented set of challenges," the report does not provide the public and the defense policy community an unclassified summary measurement of the health and readiness of the defense industrial base or a simple way of tracking that over time.

To fill this gap, the National Defense Industrial Association, partnering with data science company Govini, has piloted what it plans as an annual project called "Vital Signs." The subtitle of the report is "The Health and Readiness of the Defense Industrial Base." The assessment focuses on standardizing and integrating analyses of different elements of the sector and the business environment shaping its performance.

This year's mediocre "C" grade reflects a business environment characterized by highly contrasting areas of concern and confidence. Deteriorating conditions in 2020 for industrial security and for the availability and cost of skilled labor and materials emerge from this analysis as areas of clear concern. Favorable conditions for competition in the defense contracting market, and rising demand for defense goods and services reflect recent year-over-year growth in the defense budget.

This first of an expected annual study contributes to the debate about national defense acquisition strategy by offering a common set of indicators — vital signs — of what some have called America's "sixth service," the industrial partners providing our warfighters their capability advantages.

To do this assessment, we conducted a months-long study of data from eight different dimensions shaping the performance capabilities of defense contractors including: market competition; cost and availability of skilled labor and critical materials;

COMPOSITE INDEX SCORES				
DIB Health Dimension	**2017**	**2018**	**2019**	**Change, 2017 – 2019**
Competition	94	95	96	+2
Production Inputs	70	68	68	-2
Demand	78	84	94	+16
Innovation	78	76	74	-4
Industrial Security	69	65	63	-6
Supply Chain	83	83	68	-15
Political and Regulatory	92	89	79	-13
Productive Capacity and Surge Readiness	68	70	77	+9
Overall Health and Readiness	***79***	***79***	***77***	-2

Source: NDIA

demand for defense goods and services; investment and productivity in the U.S. national innovation system; threats to industrial security; supply chain performance; political and regulatory activity; and industrial surge capacity.

We analyzed over 40 longitudinal statistical indicators, converting each into an index score on a scale of 0 (bad) to 100 (excellent). We did this over a three-year running average to control for data spikes such as last year's government shutdown. Last, we aggregated the individual indicator scores into scores for each dimension, and into an overall composite score for the defense industrial base with 2020 scoring at 77, a passing C grade but with a worrying downward trend.

The analysis reveals a stressed defense industrial base, trending negative. Composite scores for four of eight dimensions eroded in 2019 since 2018. And, six dimensions earned composite scores lower than 80, C or worse, and three dimensions earned scores below 70, failing grades. For a sector facing "unprecedented" challenges, these scores suggest a defense industrial base increasingly struggling to meet them.

Industrial security scored 63 for 2019, the lowest among the eight dimensions. Industrial security has gained prominence as massive data breaches and brazen acts of economic espionage by state and non-state actors plagued defense contractors in recent years. To assess industrial security conditions, we analyzed indicators of threats to information security and threats to intellectual property rights.

The indicators of global information security threats were already failing in 2017 and went even lower in 2019. This score incorporates the rising annual average number of new cyber vulnerabilities documented by MITRE Corp., which almost doubled between 2016 and 2018 when compared to 2014-2016. The score also incorporates MITRE's annual average of the threat severity of new cyber vulnerabilities, which improved slightly for 2016-2018 but remains high. In contrast, intellectual property rights threats scored 100 out of 100 for 2019, the result of new FBI investigations into IP rights violations, which have been steadily declining since peaking in 2011.

Defense industry production inputs also scored poorly in 2019, down from a barely passing 70 in 2017. Major production inputs include skilled labor, intermediate goods and services, and raw materials used to manufacture or develop end-products and services for Defense Department consumption. Relatively low 2019 index scores for defense industry workforce size helped drive the low score for this dimension. The estimate of the size of the defense industry workforce, currently about 1.1 million, falls substantially below its mid-1980s peak size of 3.2 million.

Security clearance process indicators also contributed to the low overall composite score for production inputs as backlogs shrink but persist. Onboarding new personnel in the defense industry often requires navigating the security clearance process. Contractors face a security clearance management process that worsened between 2017 and 2019. The index scores for the annual average number of pending security clearance investigations declined for 2019 with much of that decrease due to issues with initial top-secret clearances.

The state of defense contracting competition and the state of demand for military goods and services offer the industrial base a favorable outlook. An analysis of the top 100 publicly traded Pentagon contractors shows competition conditions in the defense industrial base earned a composite index score of 96 for 2019. Several high-scoring indicators drove the strength of market competition conditions, including the availability of cash assets, the low level of market concentration of total contract award dollars, the relatively low share of total contract award dollars received by foreign contractors, and the high level of capital expenditures. Last, the defense industrial base earned a solid score of 88 for profitability for 2019, based on index scores for average return on sales and the average return on assets.

Demand for defense goods and services received a high score of 94 for 2019, which constitutes an increase of 16 points over the year 2017. This comes from an increasing financial volume of contract obligations issued by the Defense Department. Total contract obligations issued grew from $306.7 billion in 2016 to $368.7 billion in 2018. Acquisition expenditures grew in all categories, rising by 11 percent for aircraft, ships and land vehicles, by 33 percent for electronic and communication equipment, 35 percent for weapons and ammunition, 39 percent for sustainment, and 23 percent for knowledge-based services.

Foreign military sales in aircraft, ships and land vehicles also grew by 113 percent between 2016 and 2018, and related services grew by 100 percent.

Conditions in the other dimensions of the defense industrial base conform to the pattern of moderate but declining health and readiness. For example, innovation conditions received a score of 74 for 2019, declining two points from its 2018 score. Accordingly, the U.S. share of global patent applications, a measure of innovation competitiveness, received an index score of 69 for 2019, a 4-point drop from the 2018 score. Similarly, the share of global research and development comprised by U.S. R&D expenditures saw its index score decrease between 2018 and 2019 from 75 to 74.

Political and regulatory conditions earned an overall index

score of 79 for 2019, dropping precipitously by 13 points from a 2017 index score of 92. Congressional defense budgeting process indicators helped drive this decline, as their composite index score decreased from 90 for 2017 to 77 for 2019.

Congressional interest in major defense acquisition programs decreased over this same period, as mentions of acquisitions in congressional hearings decreased from 86 in fiscal year 2016 to 18 in fiscal year 2018, echoed in an index score drop from 97 in 2017 to 54 in 2019. Regulatory conditions also eroded between 2018 and 2019, as the index score for our "red tape ratio" of non-restrictive rules to new restrictive rules decreased by 18 points from 100 to 82.

The capacity of the defense industrial base to grow its output and to fulfill a surge in military demand stands as a key test of industrial base health and readiness. Productive capacity earned an index score of 77 for 2019, a 9-point increase above the 2017 index score. Gains in output efficiency and stability in capacity utilization contributed to this rising trend.

An assessment of the surge capacity of the defense industrial base using industrial input-output analysis finds fewer shortages in critical defense supplier industries than estimated for the defense industrial base of the early 1980s, the last era of great power competition. That era's defense industrial base operated under a dramatic "buildup" in defense spending and force posture begun during the Carter administration and accelerated in the Reagan administration. The Carter-Reagan buildup involved a 31 percent surge in defense expenditures. We estimate the defense industrial base circa 1980 experienced shortages in the capacity of 54.5 percent (6 of 11) of critical defense supplier industries to generate sufficient supply.

Presently, 27.3 percent of critical defense supplier industries (3 of 11) would likely experience shortages in the event of a surge in demand for combat-essential defense programs equivalent to the Carter-Reagan buildup of the late-1970s through the mid-1980s.

The health and readiness of the defense industrial base poses a challenge to the defense acquisition community. With growing expectations of the defense industrial base to rise to unprecedented challenges, this year's "Vital Signs" report highlights several hurdles in doing so.

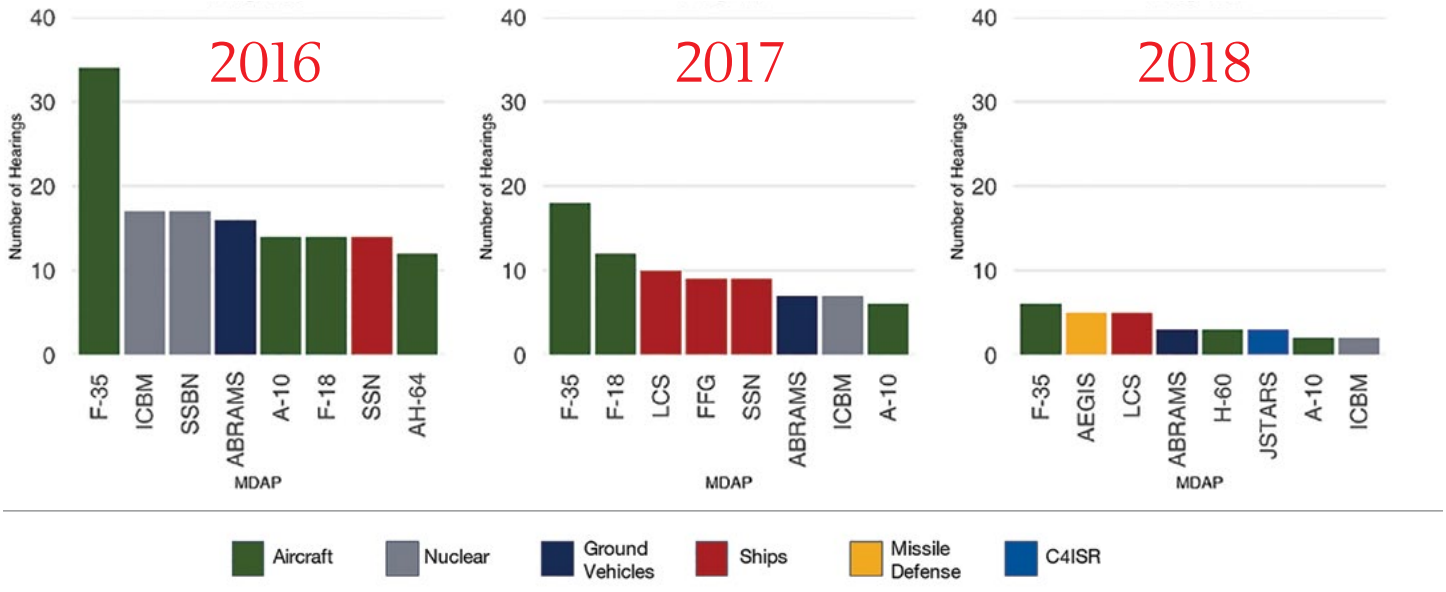
The overall defense industrial base health score of 77 suggests satisfactory capabilities to meet current mission requirements, but the fast-moving era of great power competition requires better — the delivery of extraordinary capabilities to maintain and extend eroding capability advantages over our competitors.

Further, the vulnerabilities shown in this study — industrial security and production inputs to include workforce — indicate a need for urgent attention and action. Thankfully, the areas of confidence this study highlights should confirm that the fundamentals of America's defense industry remain a sound foundation on which to build. The full "Vital Signs" report will be available in late January at NDIA.org/vitalsigns. **ND**

Wesley Hallman is senior vice president for strategy and policy and Christopher Smith is a regulatory policy associate at NDIA.

Top Major Defense Acquisition Programs (MDAPs) Mentioned in Congressional Hearings Year over Year

NUMBER OF HEARINGS WITH 5 OR MORE TERM MENTIONS



Defense Sector Straining To Attract STEM Talent

BY YASMIN TADJDEH

For years, experts and military officials have been sounding the alarm across the defense industry: More STEM — or science, technology, engineering and mathematics — talent is needed to meet the challenges of a volatile and uncertain future.

But despite these cautions, industry and government are still struggling to attract STEM students, particularly as they face steep competition from deep-pocketed commercial companies in places such as Silicon Valley. That could have dire consequences in a potential future fight with great power competitors.

In the National Defense Industrial Association's new report, "Vital Signs 2020: The Health and Readiness of the Defense Industrial Base," defense industry production "inputs" did poorly, scoring 67, or a D grade. That category includes skilled labor, intermediate goods and services, and raw materials used to manufacture or develop end-products and services for Defense Department consumption.

Relatively low 2019 index scores for defense industry workforce size helped drive the low score for this dimension. The estimate of the size of the workforce, currently about 1.1 million, falls substantially below its mid-1980s peak size of 3.2 million, resulting in an index score of 34.

Another recently released report, "The Contest for Innovation: Strengthening America's National Security Innovation Base in an Era of Strategic Competition," by the Ronald Reagan Institute's Task Force on 21st Century National Security Technology and Workforce, found that the U.S. government is straining to hire enough people with the proper STEM skills.

In one category, engineering, it found that the government is failing to attract and retain computer engineers and skilled software developers, as well as cultivating such talent internally. "The effect is a brain drain that is working against our national interest — the opposite of the one we benefited from in the 20th century," the report said.

DEFENSE DEPT.

U.S. universities are also having problems building and maintaining the talent pipeline needed for what the report calls the "national security industrial base." Schools rely on foreign students — many of whom are Chinese — to fill its graduate-level engineering programs, the report said. Around 80 percent of graduate students in technical fields are foreign nationals.

"This talent gap is partially due to the fact that private-sector companies attract American students graduating from bachelor's programs with lucrative salaries and immediate offers of employment following graduation, causing them to forgo graduate degrees," the report said.

Compounding the "war for talent" are U.S. immigration policies that often require foreign students graduating with technical degrees to return home instead of contributing to the U.S. national security industrial base, the study noted.

Far more Chinese students, in particular, are pursuing technical degrees than American students, at home and abroad, the report said.

Michael Brown, director of the Defense Innovation Unit — an organization stood up by former Secretary of Defense Ash Carter to connect Silicon Valley tech companies with the Defense Department — noted that many Chinese students are taking that knowledge back to Beijing.

"Living in Silicon Valley or any of the innovation hubs, you see how important talent from around the world is," he said during a discussion at the Center for Strategic and International Studies. "It adds to our economic prosperity and therefore is pretty important for national security. We need to be developing the leading edge of those game changing technologies here in the U.S. And to the extent that involves foreign talent [and] foreign capital to do that, we want to be encouraging that, but we don't want to be stupid."

While there should be an effort to retain as many of those students as possible, it is important to recognize that there is also a risk, he said. "Some of those folks are not interested just in economics but also interested in transferring the technology."

As recently as a few years ago, the FBI's Palo Alto office had only 10 agents.

"We're woefully short relative to the scale of the problem," he said. "In fact, you could argue that we don't have enough resources on this problem to even know what the scale is."

Right now, the United States has taken a "worst of both worlds" approach to foreign students, he said.

"We take a world-class resource of the United States — our educational system — and we allocate a big percentage of that for foreign students," he said. "We've allocated a huge percentage and then we send that educated talent home. So [we] probably need to rationalize one side or the other so we don't live with the worst case."

Brown said there have been numerous cases where Chinese students have taken research funded by the Defense Department, gone back home and then used that research to form the basis of a supplier to China's military.

"We, unfortunately, have to be more mindful of vetting some of the students and then putting in some basic protections," he said. "We have to do more to raise the costs there."

Meanwhile, China's investment in STEM talent is giving them an edge, said Gen. Stephen "Seve" Wilson, vice chief of staff of the Air Force.

"China is all-in to win," he said during remarks at the Interservice/Industry Training, Simulation and Education Conference in Orlando, Florida. "Last year, they produced eight times the STEM graduates [as the United States] and they're predicting that in the next five years that the number of STEM graduates will be 15:1."

Because of China's civil-military fusion concept — which requires its industrial and academic sectors to share information with the military — it would be a mistake to underestimate them, Wilson noted.

"Not only can they compete, I contend they have an advantage," he said.

Former Secretary of the Navy Richard Spencer said cultivating STEM talent will be a key differentiator in future conflicts.

The technology race is "going to be a horse race — one year we'll be ahead, the next year China will be ahead," he told reporters on the sidelines of the Halifax International Security Forum in Nova Scotia, Canada, a day before his resignation. "We're going to be fighting with similar weapons. What's going to be the gapping difference that we have? It's how we fight the ship, how we fight the weapon, how we use the Marine. It's going to be the gray matter that's going to be the gapping difference."

To counter the government "brain drain," the Reagan Institute recommended Congress authorize the creation of a new national civilian "STEM Corps."

"Modeled after the Reserve Officers' Training Corps and the National Guard, students would be selected through a competitive process to receive full tuition to attend public universities and study specified disciplines related to national security technology," the report said. "In return for accepting the scholarship, graduates would commit to spending several years serving in

Air Force Lt. Gen. Jack Shanahan, director of the Joint Artificial Intelligence Center, speaks to an audience at the National Security Innovation Network and JAIC hackathon challenge.

DEFENSE DEPT.

either the 'active' or 'reserve' STEM Corps, working within a component of the [national security innovation base] ecosystem."

Additionally, the report recommended the creation of a national security innovation base visa that would encourage vetted, highly skilled workers to come to the United States for employment and also allow foreign national students with relevant degrees to stay in the country. The visa should target fields such as AI, automation, cybersecurity and various dual-use technologies.

"This approach would incentivize them to contribute their education and talents to the long-term benefit" of the national security industrial base, the study said.

Meanwhile, organizations such as the Joint Artificial Intelligence Center — which was stood up last year to coalesce the Defense Department's many disparate AI projects — are working to better reach out to STEM talent.

"Like our counterparts in private industry, the JAIC and the larger DoD national security enterprise is engaged in a war for talent," said Lt. Cmdr. Arlo Abrahamson, a spokesman for the center. "As the U.S. military moves forward with its digital modernization efforts, attracting the requisite talent for organizations like the JAIC will be critical for the DoD to achieve its AI strategy and lead in AI innovation."

The center is executing a targeted outreach strategy aimed at recruiting talented artificial intelligence experts from across commercial industry and academia, he said in an email. Working alongside organizations such as the Defense Innovation Unit and the National Security Innovation Network, or NSIN, the center has facilitated a series of hackathons and technology challenges to solicit ideas from academia and industry on artificial intelligence technologies.

For example, in September the Joint AI Center and NSIN held a hackathon at the University of Michigan's School of Aerospace Engineering where experienced military aircraft maintenance personnel worked with students and industry to develop new solutions using AI for aircraft preventive maintenance, he said.

"These outreach activities provide valuable professional connections between STEM students and military organizations dedicated to technology innovation that these students might not otherwise experience," Abrahamson said. "While students may not implicitly choose careers in the DoD, technology challenges and hackathons provide an alternative venue for STEM students to contribute intellectual capital to contemporary national security problems while generating awareness about STEM careers in DoD and other U.S. agencies should they wish to seek government employment in the future."

The center is also working closely with the Defense Department's human resources team to offer appropriate incentives and opportunities for STEM graduates, Abrahamson noted. While the Defense Department cannot completely match the monetary compensation of private industry, it is working to improve the competitiveness of the compensation packages for individuals with advanced and rare technical skills.

Emma Moore, a research associate at the Center for a New American Security's Military, Veterans and Society Program, said one way to entice STEM talent to work for the military is by putting more emphasis on the entire benefits package it can offer servicemembers.

"When it comes to salaries, often leaders say we can't compete with private sector salaries, but they're failing then to convey the benefits of the total compensation package, which is very generous," she said. These packages include base pay, housing allowance, health care and discounted rates at base stores.

"The messaging is slightly off and could be flavored differently to actually attract people in that kind of gray area who might not be really considering the military but could be courted to actually join because of the value proposition," she said. "We pay really well, and we give you all these other perks, plus we are on the front lines."

A bigger issue is the way the military recruits potential STEM talent, Moore said. The process is too burdensome and makes it more likely interested students will pursue work with commercial industry.

"Every single commercial and recruiting effort ... is to try to get someone to talk to a recruiter. [But] that doesn't acknowledge all of the hurdles that the military then puts in front of individuals when it comes to the medical examinations, having to take time off from whatever you're doing to go talk to a recruiter," she said. "If somebody is not incredibly motivated ... to put in all of the effort that it takes, then you're going to lose them to begin with."

On the other hand, commercial companies send recruiters to go out and find talent and streamline the hiring process, she said.

"It's a much more, 'We want you because you are the talent' [approach], where the military does this thing where … you still have to get yourself through the process," Moore said.

Another obstacle is that the Defense Department is facing a "tech lash," said Peter W. Singer, a strategist and senior fellow at New America, a Washington, D.C.-based think tank.

There is a movement within the tech community and the broader cultural and political arena that is pushing back against big technology companies and the roles they play in warfare and security, he said. It's everything from "the Project Maven controversy at Google to larger discussions about, 'What's the future of AI and weaponization' to, 'Is Facebook too big and should it be broken up?'" he said.

The Pentagon is countering that narrative with two arguments, Singer said.

"One is: That's fine — that's your right [to not work for us] — but for those of you that want to work on programs and make a difference, we're where it's at," he said. The Pentagon is saying, "you could work on some app that's basically about optimizing click rate, or here you can work on a project that might help in a humanitarian disaster relief or it might defend the nation."

The Defense Department is also trying to entice talent by explaining that certain employees with unique STEM skills would be a rare commodity and especially valued in the Pentagon, he said. **ND**

VIEWPOINT

Taking on China Requires A Strengthened Workforce

BY REP. JIM BANKS

During my time in the Navy Reserves I saw the impressive capabilities the Defense Department could deliver to our men and women at the frontlines. It has seen enormous successes during the past several years: the fifth-generation capabilities of the F-35, the elaborate network of our satellite communication systems and advanced undersea detection capabilities. I am proud of our military and want to ensure that it is prepared for the future fight.

However, I've also seen some of the department's weaknesses during my time in the Navy and now in Congress. Many of these weaknesses revolve around thick government bureaucracies and inefficiencies.

For example, according to the department's own 2019 Digital Modernization Strategy, it maintains 10,000 information technology systems at a staggering cost of more than $46.4 billion annually, as requested for fiscal year 2019. Several of these systems are outdated and ill-managed, creating a self-imposed burden in the task of effective communication security.

The Defense Department also struggles with the fresh and strategic thinking needed to innovate and outpace our adversaries. For instance, we are still fighting our longest war — a war I served in during 2014 and 2015 — that began before the birth of some of our current servicemembers. The Defense Department vulnerabilities that have stalled the progress in Afghanistan continue to concern me, especially as we face growing threats from China.

Beijing is eager to exploit our weaknesses and build up areas in which the United States is vulnerable. The United States now needs to fight to cement its hard-fought place as the leader of the liberal world order. We can no longer ignore threats from revisionist powers. On the House Armed Service Committee, I constantly strive to provide congressional oversight that doesn't impede the Defense Department's efforts, but provides accountability and ensures our armed forces are equipped with the resources they need to operate at their level best.

To face our long-term strategic competitors, the department must focus time and resources to meet our greatest challenges and fully align to the needs addressed in the National Defense Strategy.

The Ronald Reagan Institute's Task Force on 21st Century National Security Technology and Workforce — which included several distinguished government and private sector thought-leaders — sought to shed light on the systematic and underlying challenges our military faces, and create a blueprint to adapt to challenges posed by revisionist powers like China. The result is the report, "The Contest for Innovation: Strengthening America's National Security Innovation Base in an Era of Strategic Competition."

The task force was well positioned to strengthen the national security innovation base, or NSIB, to better prepare the workforce for the 21st century by utilizing expertise in academia and incorporating the defense industry. Co-chairs former Sen. Jim Talent, R-Mo., and former Deputy Secretary of Defense Bob Work led the bipartisan effort to reform the Defense Department so it can adapt to the 21st century.

In addressing our most pressing needs, the task force brought in several of the brightest minds — from defense trailblazers, leaders of allied nations and academia — to discuss substantial reforms policymakers could implement to make our nation more competitive.

At the current pace, the United States will reach a point of technological deficit from which we will never be able to recover. The task force focused on China's strengths such as their masterful practice of stealing intellectual property, relocating American jobs, and quickly implementing technological innovations, to shape the policy recommendations to address threats to the U.S. innovation base. A stated national aim of China is to integrate their civilian and military dual-use technologies.

As an authoritarian state, it is well positioned to conduct research at state-owned enterprises or hybrid companies and allocate significant resources into technologies like artificial intelligence, 5G, autonomous capabilities, microchips, semiconductors and other emerging technologies. China also sees our latency in fully investing in military dominated domains, such as space warfare and hypersonic weapons. Without a healthy appreciation of China's rapidly growing capabilities, policymakers will quickly fall behind without ever realizing that the United States

ISTOCK

lost its grasp on its position as a global leader.

The Reagan Institute also utilized valuable survey data to understand the public's perception of current national security threats. According to the 2019 Ronald Reagan Institute National Survey, almost nine in 10 Americans, 89 percent, are concerned about cyberattacks on government computers and the electrical grid. Adversarial governments often look to this low-cost attack to steal critical data from U.S. citizens. From 2013 to 2015, the Chinese government hacked into the Office of Personnel Management's database, exposing 21 million current and former employees' private information, such as Social Security numbers and addresses, to the Chinese Communist Party.

Former Navy Secretary Richard Spencer recently stated that the service's industry partners are "under cyber siege" by Chinese hackers and others who have stolen national security secrets in recent years, exploiting critical weaknesses that threaten the United States' standing as the world's top military power. While the Defense Department has made significant strides in addressing the threats, the workforce, infrastructures and platforms must continue to fortify against these covert tactics. While this is just one example of how China exerts asymmetrical warfare, it demonstrates the long neglect of a critical infrastructure need.

To address such fears, the Reagan Institute provided key findings and recommendations to be able to compete with peer competitors like China. One such recommendation was the idea of a STEM Corps. As a member of the House Committee on Education and Labor and the Armed Services Committee, I am keenly aware of the science, technology, engineering and mathematics challenges facing the nation today. STEM majors at U.S. universities are often dominated by international students from countries like China, India and South Korea, whose students are eager to take on the challenge associated with advanced mathematics and science backgrounds.

Rather than shy away from the technologically complex problems of the 21st century, the United States needs its students to embrace the great challenges of our time in service of our national defense. To address this need, the STEM Corps would incentivize students to major in a STEM degree, ushering in a new era of U.S. technological supremacy.

In exchange for accepting critical employment opportunities at government agencies, program participants will have a significant portion of their college education paid for by a new public/private partnership. By exposing the brightest minds early to the rewards of government service, they will be able to serve their country and incur less student debt in the process.

Additionally, the task force found that the Defense Department needs a much higher risk tolerance when it comes to innovation. As Talent stated, the task of policymakers is to "focus the ecosystem on national security priorities, create a more comprehensive security consciousness among the private actors, and coordinate the segments enough to get the necessary synergies — all without straightjacketing the creativity of the ecosystem or sacrificing the freedom, openness and risk-positive culture that is one of the NSIB's greatest strengths."

Under great pressure, the U.S. government is able to innovate. When challenged to succeed, the U.S. space program was able to overcome early setbacks en route to one of mankind's greatest successes when Americans first set foot on the moon. China's challenge in cyberspace is this generation's Sputnik moment and we need to respond in kind.

But we've lost our way. Under financial constraints and looming deadlines, the Defense Department is forced to be as cautious as possible to demonstrate constant progress for their congressional funders. However, policymakers should be continually searching to remove red tape and encourage program officials to fail fast.

The private sector is naturally incentivized to innovate, whereas the Pentagon is not. Dramatic changes away from platforms and toward systems upsets the balance and slows innovation. The department needs to work closely with the private sector to monitor the supply chain, field emerging technologies at a much faster rate and learn from private sector contributions.

In addition to challenges like these, I have made China the focal point of my time in Congress. The National Defense Strategy states, "As China continues its economic and military ascendance, asserting power through an all-of-nation long-term strategy, it will continue to pursue a military modernization program that seeks Indo-Pacific regional hegemony in the near-term and displacement of the United States to achieve global preeminence in the future."

The United States must prepare a similar all-of-nation response. In March, I introduced the "Protect Our Universities Act" to create an inter-agency task force addressing the threat of espionage on our college campuses. The lack of coordination between the Department of Education, the Defense Department and the intelligence community is an example of the slow-moving bureaucracy that reduces government efficiencies and makes us more vulnerable.

In Congress, I co-chair the Future of Defense Task Force with Rep. Seth Moulton, D-Mass., where, like the Reagan Institute, we like to think ahead and tackle problems laid out in its report. As co-chairs, we continue to examine U.S. vulnerabilities and congressional responses to the China threat. The task force seeks to improve the Defense Department's agility as we examine its strategic thinking, the capabilities of autonomous systems, the capabilities of hypersonic weapons and several other challenges of the decade to come.

The important work of the Reagan Institute and the Future of Defense Task Force must be applied with a whole-of-government approach and a steadfast commitment to innovation. China will not allow bureaucracy to limit their innovation, and neither should we. To prepare for the future, the Defense Department and the national security innovation base must closely read recommendations from the Reagan Institute report and champion the next Sputnik moment. **ND**

Rep. Jim Banks, R-Ind., is a member of the Reagan Institute Task Force and co-chair of the Future of Defense Task Force. He also serves on the House Armed Services Committee and Veterans Affairs Committee.

Small Businesses Concerned About New Cybersecurity Certification

BY CONNIE LEE

The Pentagon is rolling out new cybersecurity regulations for handling unclassified information that may bar contractors from bidding on future programs if they do not obtain the required certifications.

Katie Arrington, chief information security officer at the office of the undersecretary of defense for acquisition and sustainment, said it will take until 2025 to fully implement the cybersecurity maturity model certification program, or CMMC.

"If we don't understand that this is a collective issue, that everybody needs to have cybersecurity requirements and in their day-to-day business, we're never going to get ahead of this game," she said in October during an interview with Exostar, a company focused on protecting the supply chain.

The Defense Department plans to tighten its policies as digital warfare becomes more prevalent, she noted. The CMMC will need to be continuously updated to keep pace with changing cyber threats, and these certifications will be especially important as technology continues to advance. One specific threat includes the development of quantum computing, which can be used to break encryptions, she said.

"The way it lives in 2020, I hope isn't the same model that is in existence in 2025 because the threat vectors will change," Arrington said. "This is electronic warfare. The moment that we move and we're capable of plugging that hole, our adversary will be … finding a new access point."

The Pentagon's supply chain currently consists of about 300,000 companies and about 290,000 of those have no cybersecurity requirements whatsoever, she said. Under the new regulations, Defense Department contractors and subcontractors will need to become certified regardless of the program.

In the National Defense Industrial Association's new report, "Vital Signs 2020: The Health and Readiness of the Defense Industrial Base," industrial security for 2019 scored a 64, or a D grade, the lowest among the eight dimensions the report measured.

Current regulations to address these shortcomings are implemented by the Defense Federal Acquisition Regulation Supplement Clause 252.204-7012 and NIST Special Publication 800-171. Companies must safeguard covered defense information, report cyber incidents and facilitate damage assessment, in addition to meeting other requirements.

But the Pentagon has decided that it needs more stringent regulations, Corbin Evans, NDIA's director of regulatory policy, said in an interview. NDIA is one of the organizations providing feedback on the program. The Defense Department is still finalizing details of the CMMC.

"They have basically decided that this is not working, that this regulatory scheme is not robust enough," Evans said. "It doesn't do enough to essentially protect the requirements or protect the data."

In the future, the new certifications will be baked into program contracts, making them a prerequisite for doing business with the government, he noted.

If the Pentagon remains on track, starting in October 2020 each issued request for proposals would outline which CMMC

ISTOCK

certification level a company needs to bid on the program, Evans said. These would range from levels one through five, with one being the lightest of security requirements. Less stringent regulations would be similar to those mandated for private homes or small businesses, he noted.

The first version of the CMMC framework will be released in January 2020, according to the office of the undersecretary of defense for acquisition and sustainment's new CMMC website. By June 2020, these requirements will be inserted into requests for information, the website said.

The Defense Department has not decided on the length of the certification's validation period.

One example of changes companies may need to make is improving access controls, which could be done by implementing technology that tracks all visitors who have access to a company's system, Evans noted. Two-factor authentication to ensure server security will be particularly expensive to implement, he said. Many companies will fall under certification level three, which has more regulations than the current rules, he noted.

Michael Flavin, director of IT sales at Saalex Information Technology, said these new requirements will largely affect small businesses because they may not be able to handle the financial burden associated with completing the certifications.

"Say it's a DoD contractor of like 20 employees," Flavin said. "To get all of this done, just a gap analysis from a consultant can run $25,000 to $50,000 bucks."

However, according to the CMMC website, certification costs "will be considered an allowable, reimbursable cost and will not be prohibitive."

Without obtaining the certifications, many companies will be unable to participate in future competitions, Flavin noted. The CMMC website says businesses could be disqualified.

"They can't bid on it" or recompete for contracts, he said. "It really could suck the lifeblood out of a company."

Additionally, the CMMC effort will be a big change because many companies are still working on coming into compliance with current cybersecurity guidelines, he noted. This doesn't necessarily mean that companies have not implemented any security features such as firewalls and encryption, he said, but many steps required by the current rules "probably haven't been done, which is why they're saying the vast majority are not in compliance."

Based on informal discussions at industry events, many small business members with less than 100 employees do not seem to understand technical controls for protecting data, Flavin said.

"It was shocking to me. … These people would become a deer in the headlights," he said. "These people have just not kept up with the pace of cybersecurity and risk-based cybersecurity philosophies."

For existing contracts, Evans said the Defense Department plans to insert the certification requirements during renegotiations. Officials will begin by working on high-priority contracts, which include major weapons programs.

"They will essentially go contract by contract for renegotiations if they are multi-year contracts," he said. "Then they're going to roll this out starting … with the most sensitive contracts and then moving … all the way down to apparel supplies."

This is expected to be a major change for many firms, he noted.

"The boots lace supplier will have to be CMMC at least level one compliant," he said.

The present October 2020 timeline may be "aggressive or optimistic," Evans said.

"This is an area where we understand and are sympathetic to the security concerns," he added. "But we are worried about the negative impacts of rolling this out department-wide and essentially pushing people out of the defense industrial base."

Arrington said to create the CMMC, the Defense Department was inspired by international cybersecurity standards such as the United Kingdom's General Data Protection Regulations.

"We took those standards into creating what is now the CMMC," she said. "Our international partners are looking to adopt the CMMC and integrate it, and we've done our best to try and incorporate all the different standards into the model." That includes NATO, she added.

Auditors from a third party will assess whether companies meet requirements, Arrington said. The Defense Department has already put out a request for information asking industry about creating an accreditation body that will be responsible for training companies and individuals on how to become auditors, she noted. Training will run from this January to April or May.

"We in the Department of Defense know very well that we are not set up or resourced to do these certifications and audits of 300,000 companies," Arrington said. "As it is, our $750 billion budget doesn't really cover all that we need to do. So we needed to look outside."

However, higher level assessments may be conducted by organizations such as the Defense Contract Management Agency or the Defense Counterintelligence and Security Agency, the CMMC website said. Companies' certification levels will be made public and firms will not be allowed to certify themselves. Auditors will make a "go/no go" decision rather than providing a score.

Arrington said program managers will also be taught how to determine which companies need to meet certain cybersecurity levels.

"Why would you need to put a CMMC level five on someone who's … selling pens to the government?" she said. "That's not obtainable and we need to teach our PMs to do that."

The Defense Department hopes to help industry develop critical thinking skills about cybersecurity and cause a cultural shift by implementing these certifications, Arrington said. A company should already have its own basic cybersecurity policies in place by the time it reaches level two, she noted. Most companies will not be asked to obtain the highest certification.

"It's very expensive and very hard to obtain that," she said. "To have the capability at CMMC level five — to have a 24-hour, seven day a week stock capability — isn't something that we would even think to ask of most contractors." **ND**

Pentagon Updating Cybersecurity Guidance

BY RYAN BURNETTE, SUSAN CASSIDY AND SAMANTHA CLARK

In December, the Defense Department released a new draft of its Cybersecurity Maturity Model Certification, or CMMC, an important guide for contractors.

Given the expected release of Version 1.0 of the CMMC framework in late January 2020, it is likely that the requirements in this draft will closely resemble those that will serve as the basis for the first contractor audits.

The two most significant updates are the addition of "practices" for obtaining Level 4 and 5 certifications, and an expansion of the "clarifications" section, which now covers the requirements of Levels 2 and 3 of the model, in addition to Level 1.

It retains the matrix format that we have seen in prior versions, composed of "domains," "capabilities," "practices" and "processes."

Each domain consists of multiple capabilities, and each capability consists of multiple practices. Capabilities are general achievements to ensure cybersecurity objectives are met within each domain. Practices more specifically outline the technical requirements necessary to achieve compliance with a given capability, while processes measure how well practices have been implemented across a contractor's business.

Version 0.7 now contains what we expect to be a near-final set of practices necessary for obtaining Level 4 and 5 certifications, and relegates all processes to a much-simplified table that is intended to apply across all domains.

The requirements in Levels 4 and 5 are greatly consolidated. However, they still represent a significant set of compliance obligations that contractors must follow in order to perform work on contracts designated at either of these two certification levels.

Level 4 now incorporates 13 controls set forth in the draft NIST SP 800-171B, and Level 5 certification includes requirements for an additional five controls from draft NIST SP 800-171B.

Levels 4 and 5 continue the practice of including multiple controls for certain practices, thereby increasing the possibility of conflicting guidance. Moreover, standards that are pulled from NIST SP 800-171B in some cases appear to have been incorporated into the CMMC on a modified or a partial basis. For this reason, even those contractors that have implemented sophisticated cybersecurity controls in line with the standards set forth in NIST publications should closely review how these requirements and others have been described in the CMMC to ensure that they will be compliant with all applicable practices at the time that they undergo an audit.

Perhaps the most helpful update for contractors is the inclusion of new clarification sections for Level 2 and 3 practices, in addition to new clarifications of processes. These sections include brief discussions of the requirements, clarifications to further explain Defense Department expectations, and in some cases, examples that describe scenarios where compliance is appropriately demonstrated within an organization.

The inclusion of clarifications for Level 3 in this draft is an unexpected but welcome addition.

We expect that these clarifications will be vital to understanding and interpreting the very brief and limited descriptions of practices and processes that are set forth in the matrix itself. Indeed, one of the new process clarifications applicable to process maturity Level 2 describes minimum elements that policy statements from a contractor's senior management should contain to appropriately document security requirements that are applicable to the network. Contractors should be mindful to read the CMMC as a whole to ensure they do not encounter unexpected issues during their third-party audits.

Thus far, the Defense Department has adopted a regular cadence for updating and revising the CMMC. Although we would expect to see more additions to the model in the future — potentially including an expansion of the clarification section to cover the newly added Level 4 and 5 requirements — the model is nearing a ready-to-release format. As of press time, it appears likely that the department will meet its January 2020 release date target for Version 1.0.

Contractors should continue to take steps to implement all requirements, as implementation may represent a significant effort, requiring input not just from an organization's information technology and legal departments, but from an organization's senior management.

The Pentagon has expressed a desire to revise the model on a continuous basis to rapidly address new and evolving threats. Thus, any contractors that are left playing catch up at the time that the department begins including certification requirements in its request for proposals in fall 2020 will have a difficult time staying ahead of the curve as the model continues to evolve.

A number of questions persist, including: how the Defense Department and its auditors will handle the immediate influx of contractors requiring certifications; the specific criteria for determining the certification level necessary to perform a contract; how the department and its accreditation body will ensure consistency of third-party audits; and how it will address the impact on commercial item and small business contractors, which ordinarily do not obtain significant cost recovery under reimbursable contracts with the government. Industry should stay well-informed of further developments in this area. **ND**

Ryan Burnette is an associate, Susan Cassidy is a partner and Samantha Clark is special counsel at Covington & Burling LLP.

Industrial Base Could Struggle to Surge Production in Wartime

BY JON HARPER

The U.S. industrial base would be challenged to ramp up production to meet wartime requirements in the event of a protracted great power conflict, analysts and Pentagon officials say.

The National Defense Industrial Association's new report, "Vital Signs: The Health and Readiness of the Defense Industrial Base," said 27 percent of critical defense supplier industries would likely experience shortages in the event of a surge in demand for combat-essential products.

That finding is of particular concern in the new strategic environment.

In the decades following the Cold War, the United States was focused on regional wars such as Iraq and Afghanistan, noted Mark Cancian, senior adviser at the Center for Strategic and International Studies.

"For the most part, losses [of equipment] have been low and your existing industrial base could handle it," he said. But in recent years "the focus changed to great power conflict with China and Russia, and in such a conflict attrition might be very high and the industrial base is not designed to handle that kind of demand" for more systems.

Susannna Blume, director of defense programs at the Center for a New American Security, noted that China has been investing heavily in its missile forces.

"Those forces are designed to cripple the U.S. military," she said. "That's a huge concern. The ability to reconstitute quickly could be critical in prevailing in that kind of conflict."

Cancian said that, based on historical analysis of attrition rates in large conventional wars, the U.S. Army could be reduced to just two armored brigades in the first nine months of a fight against another great power. Similar rates of attrition would be expected to be sustained by aircraft and other major systems, he added.

The Defense Department would struggle to replace losses or expand its force structure in such a scenario, analysts say.

"The industrial base has been designed to produce equipment in peace time as efficiently as possible, so much of the spare capacity has been squeezed out in order to reduce costs," Cancian said. "It is not a worthwhile business strategy to have a lot of unused capacity, and DoD has not been willing to pay for it."

Maiya Clark, a research assistant at the Heritage Foundation's Center for National Defense, said the capacity problem is widespread.

"Generally speaking, I would say that the U.S. defense industrial base really is poorly positioned for a production surge at this time," she said. "We're barely meeting the needs of our military in peace time. So it's definitely a great concern in pretty much every sector, although depending on the sector, the particular issues are different."

Cancian said replacing destroyed or damaged ships would be especially challenging because it takes years to construct major battle force vessels such as destroyers or aircraft carriers.

Clark said another issue is the shortage of skilled technical labor for people who have the training to do specialized tasks such as welding and electrical work.

The limited number of vendors is another problem, noted the Defense Department's 2018 report titled, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency." The document is often referred to as the 13806 Report after the executive order that led to it.

Today, the U.S. shipbuilding industrial base consists primarily of seven shipyards owned by four companies, plus their suppliers, the report noted. The number of vendors supplying specific types of platforms is even fewer. For example, only one firm — Huntington Ingalls Industries — currently builds aircraft carriers.

"In the case of a surge, we would be really poorly placed to increase our production capacity," Clark said.

The aircraft manufacturing sector faces similar workforce and supplier base issues.

Six companies provide the majority of platforms and possess the full range of capabilities to bring a new weapon system from the research, design and development phases into full production, according to the 13806 Report.

The big three — Boeing, Lockheed Martin and Northrop Grumman— have a virtual monopoly in many areas, Clark noted.

For example, Northrop Grumman is the only firm currently building bombers.

Industry consolidation across a number of sectors is already an issue that would only be exacerbated during a great power war, Clark noted. "These are all problems that we can see now … but if there were to be a surge required, all those problems would become massively obvious."

Vehicle manufacturing is one sector where the industrial base has recently demonstrated an ability to ramp up production to meet urgent wartime requirements. During the Iraq and Afghanistan wars, improvised explosive devices wreaked

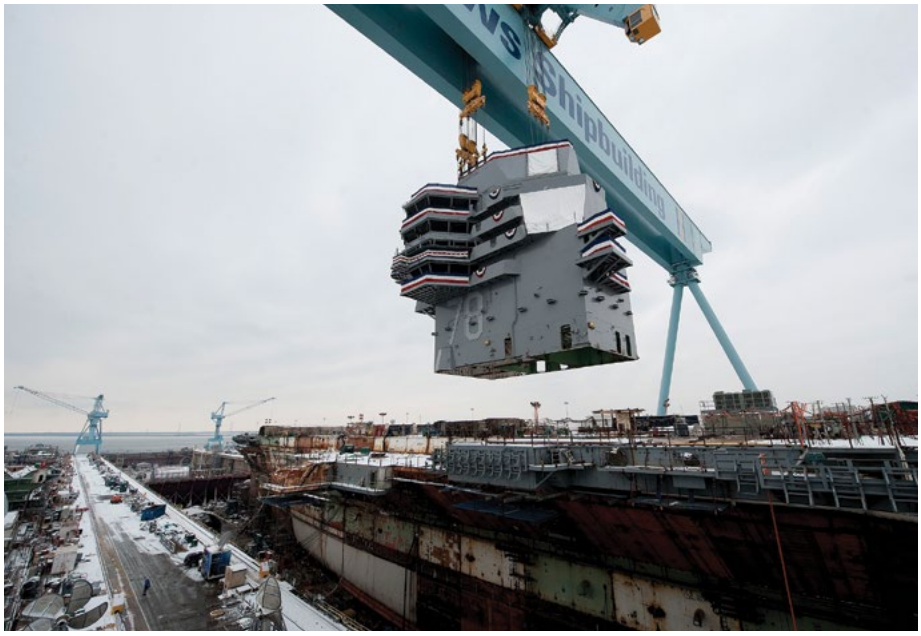
havoc on U.S. forces. In response, the Pentagon contracted for thousands of mine resistant, ambush-protected vehicles to transport troops around the battlefield.

Production increased from 82 trucks per month in June 2007, to 1,300 a month in December of that year, Clark said.

"That was a pretty massive surge that we managed successfully," she said. "We had multiple manufacturers involved with that effort and ended up producing around 24,000 vehicles."

However, other platforms wouldn't be as easy to churn out, Cancian noted.

"If we were in a great power conflict with heavy attrition, we would surge all of the tank production that we could, but of course that's not going to be able to replace most" of the losses, he said.



Technologies that are also produced in the civilian sector will be less of a problem to replace such as small arms, trucks and some types of communication systems, he said. "It's those areas that are uniquely military where there's no civilian analogue that will be most vulnerable."

Munitions production is another area for concern. Advanced air-, ground- and sea-launched weapons are a key component of the military's operating concepts.

In the Trump administration's fiscal year 2020 budget request, the Defense Department proposed buying several critical munitions at maximum production rates, Blume noted.

"If we are maxing our production capacity in peace time for critical munitions, what does that say for our ability to produce those munitions in a moment where we could be expending many, many, many of them very, very rapidly?" Blume asked.

Cancian said the United States can't count on replicating the production successes it accomplished during the last great power conflict when civilian industry was converted to military manufacturing.

"In World War II we had several years to get ready before we actually got involved in the fighting. And even once we got involved in the fighting, we had several years before we went toe-to-toe with the main forces of our opponents," he said. "During that time it was our allies for the most part who were holding the line, and we won't have that luxury in a future conflict."

The U.S. economy has also changed significantly since the 1930s and 1940s, and is now much more oriented toward services than manufacturing, he noted.

Blume said defense equipment is also more specialized in the 21st century.

"In World War II you had major industrial conglomerates like Ford producing war materiel. They were making tanks and there was a lot of … industrial capacity in the United States that could be thrown towards the war effort," she said. "The composition of the defense industrial base is not the same today. You tend to have more highly specialized defense companies … and there just aren't that many of them."

Cancian said China and Russia would also face challenges replacing equipment and growing their forces during a war with the United States. But they might not be in as tough a spot.

"The Chinese have, I think, a much larger military industrial base and they're producing more weapons than the United States," he said. "So they might have an advantage there."

Russia, meanwhile, might have larger quantities of older equipment in storage that it could draw from, he added.

However, there are a number of steps that the U.S. government can take now to ameliorate the surge problem, analysts say.

One is to ensure that the Defense Department has sustained and consistent funding. Budget instability, including a series of continuing resolutions and threats of government shutdowns in recent years, have hurt the industrial base and driven away suppliers, Clark noted.

Multi-year contracts would also help to establish predictable funding, she said.

"Without that reliability, these companies end up shutting their doors, they end up consolidating and our capacity to meet current and potentially larger future needs is compromised," Clark said.

While sole-source risk can occur at the prime level, it more often manifests itself at the sub-tier, the 13806 Report noted.

Clark said: "There's just a lot of different examples where these little companies are very adversely affected by the unpredictability of DoD funding. It may look like a little company, but it can have drastic results for U.S. national security."

Cancian said it would be prudent to identify and address the most severe bottlenecks in industry so that production in wartime could be increased as much as possible. Targeted investments could have an outsized impact on the ability to surge.

Clark noted that the government could provide funding to selected industries that are in jeopardy under authorities provid-

HUNTINGTON INGALLS

ed in the Defense Production Act.

For planning purposes, the Pentagon should determine what surge production capabilities would be needed in a global war with China or Russia, and where the shortfalls are, Clark said.

"You need to know … which holes need to be plugged first," she said. "The information that we have that would lead us to draw conclusions about our surge capacity would lead us to say we're not all that prepared, but actually the degree to which we are prepared or unprepared is hard to know without more information."

Tom Spoehr, director of Heritage's Center for National Defense, said more government visibility into industry's resourcing needs would also be helpful. Using contracting to elicit that information would be one option.

"If we're contracting for a hundred planes a year, the contractor … [could be required to] advise the government what resources are required to get to 200 a year or something like that," he said. "Right now that's not part of it, and so everybody's kind of flying blind on this topic."

The Pentagon will need to give companies financial incentives if it wants them to boost their production capacity, he noted. Firms are focused on maximizing shareholder value and profit, and maintaining extra facilities is generally looked upon as wasteful in that context.

"Companies will not typically maintain one iota of additional capacity more than what they've been contracted or can foreseeably need in the next couple of years," he said.

Blume said new manufacturing techniques could enhance industry's capabilities.

Assistant Secretary of the Air Force for Acquisition, Technology and Logistics Will Roper is pushing a new Digital Century Series concept that calls for using digital design and engineering to improve the way aircraft are produced, she noted.

"If he's right and there is a way to build airplanes, for example, without a lot of heavy, highly specialized tooling or skilled labor, that has significant implications for … the ability to restart or expand production capacity faster," Blume said.

The Defense Department can invest and push for industry to embrace the kinds of technologies that will make it easier to surge, she added.

"It's not as though the only solution to this problem is just building more factories and letting them sit unproductive," Blume said. "You can design weapons systems in a way such that they can be built more quickly and more easily using technologies like digital [engineering], etc."

Cancian said if the balloon goes up and the U.S. military finds itself in a shooting war with China or Russia, it might have to buy foreign systems or take older, less capable systems out of storage to help replace equipment losses. It would also need to improvise with whatever industry could put together quickly.

Meanwhile, Pentagon officials are well aware of many challenges the nation would face trying to execute a wartime surge.

"I have a lot of concerns," Assistant Secretary of Defense for Acquisition Kevin Fahey told reporters recently. "But the other thing I'd tell you is industry never ceases to amaze … when you end up with a requirement that is funded, how quickly they can ramp up."

Fahey noted that he played a role in the effort to surge mine resistant, ambush-protected vehicle production. However, the MRAP was basically just "a really big truck," he said. Other types of equipment surges would be more difficult.

For example, "we already have bottlenecks given what we've got at the shipyards," he said. "If you wanted to ramp our production [that] would be harder to do." It wouldn't be impossible, but it would "probably take a little bit of time," he added.

The Trump administration is trying to tackle the issues that were highlighted in the 13806 Report, including surge capacity and supply chain vulnerabilities, he said.

"We did a great job of actually for the first time … not only identifying what we believe our problems were in the industrial base, but what were we going to do about it," he said. "We have a lot of executive orders to actually work on some of these major problems." **ND**

ARMY

COMMENTARY

Signs of Progress on Industrial Base Issues

BY JENS PEDERSON-GILES AND KEVIN MERRICK

For decades, defense policymakers have focused attention on the U.S. manufacturing sector as an area of strategic concern for the United States. Issues such as production outsourcing, skilled personnel deficits, insufficient investment in new technologies and equipment and worrisome supply chain resiliency have plagued the manufacturing sector in recent years, encouraging doubts about its ability to meet the military's need for secure and reliable industrial supply.

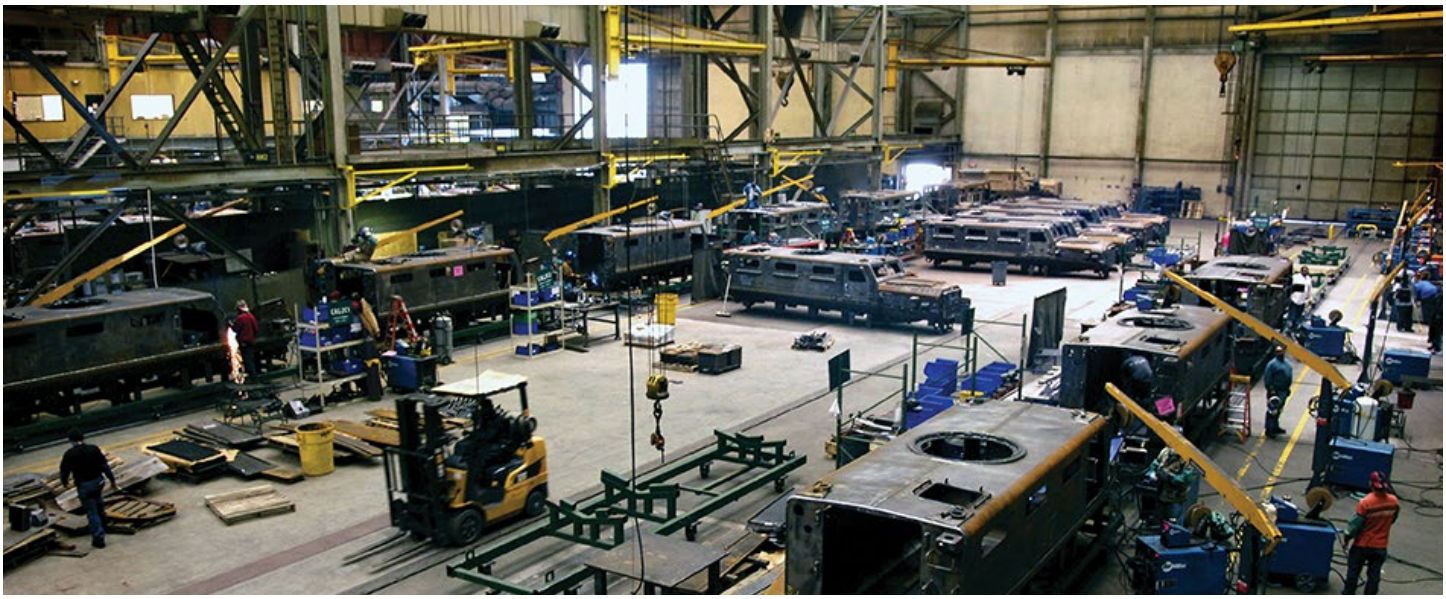
An interagency task force assessment of the state of the defense industrial base, initiated by President Donald Trump's Executive Order 13806, identified multiple systemic risks and recommended policy initiatives to address them. Recent actions by the Trump administration have been promising, but strengthening America's industrial vulnerabilities will be a long process, requiring patience and dedication by policymakers and the contracting community.

Released in September 2018, the interagency task force report titled, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," established an important benchmark for understanding the risks to the defense industrial base's performance. The report identified macro focuses and risk archetypes shaping the industrial base — including uncertainty of government spending, sole source manufacturing and diminishing STEM skills — and specified roughly 300 impacts felt across 16 sectors in a classified appendix.

To address the risks and negative trends raised by the report, the agencies involved provided a lengthy list of recommendations including expanding direct investment in the industrial base, growing workforce development efforts and improving research efforts into next generation technologies.

The Trump administration has taken perhaps its most aggressive policy action to enhance domestic sourcing of rare earth materials. Many advanced defense technologies rely on rare earth materials as ingredients in critical high-performance components. In July 2019, Trump signed five presidential determinations designating light rare earth elements, heavy rare earth elements, rare earth metals and alloys — neodymium iron boron rare earth sintered material permanent magnets, and samarium cobalt rare earth permanent magnets — as critical to national defense under Section 303 of the Defense Production Act of 1950. This act gives the president broad economic policy authorities to create, maintain, expand or restore domestic industrial base capabilities for the purpose of national defense.

Trump also signed similar orders this year regarding small unmanned aerial systems, naval sonobuoys and critical chemicals for missiles and munitions. The Section 303 orders target some of the deficiencies identified in E.O. 13806 report caused



DEFENSE DEPT.

by sole source or foreign source production.

In another initiative to reduce reliance on foreign made goods, the Pentagon has begun a partnership with domestic textile manufacturers to produce "smart fabrics" for use in military uniforms. Working through the Advanced Functional Fabrics of America nonprofit, the Defense Department has funded a collaborative research venture between the Massachusetts Institute of Technology, Drexel University and Apex Mills. Together this group has created a factory where they can rapidly design and create prototype smart fabrics which can communicate health information from its wearers and test the feasibility of producing durable outfits with these capabilities on a larger scale.

Financing partnerships to help build innovative and economically viable domestic sources for next-generation uniforms will mitigate the current risks presented by the military's reliance on single source and foreign source textile providers.

The administration also has used public-private partnerships to expand domestic sourcing of cold-rolled aluminum. The E.O. 13806 report identified cold-rolled aluminum — which serves as an essential ingredient in the armor for military ground vehicles, ships and aircraft — as an area of sourcing risk. The Defense Department leveraged the Cornerstone Initiative, a public-private "consortium of consortiums," to invest $9.5 million into Constellium's West Virginia plant to increase the production quality and amount of cold-rolled aluminum.

The department's industrial base analysis and sustainment program started the Cornerstone Initiative in early 2018 using an other transaction authority agreement funding vehicle. While Cornerstone formed before the 13806 report was published, it stands as a model to emulate in responding to other risk areas mentioned in the report.

The administration has also acted to address risks to the availability of skilled workers. In June 2019, the Department of Labor announced the creation of a new rule which would expand access to industry-recognized apprenticeship programs. This rule would allow educational institutions and industry groups to be authorized as "standards recognition entities," making them eligible to develop and approve the apprenticeships. Additionally, Labor has pledged $183.8 million dollars in grant money to support universities and industry groups working to build or expand their own apprenticeship programs.

Shortages in skilled domestic laborers is one of the macro-level problems identified by the report, and industrial apprenticeships have a proven record of growing the size and quality of the manufacturing workforce.

In a little over a year since the release of the report, the Trump administration has achieved some early successes in addressing the vulnerabilities it identified. Despite the reasons for cautious optimism, there remains significant work to be done to fully implement the recommendations. Restoring and advancing U.S. manufacturing will require years of effort. **ND**

Jens Pederson-Giles and Kevin Merrick are NDIA junior fellows.

DEFENSE DEPT.

VIEWPOINT

Defense Production Act Must Remain Committed To National Security

BY EMMA WATKINS

The Defense Production Act lies at a unique nexus between private industry and federal investment for the purposes of national security. In many respects, the act is well suited to address key vulnerabilities in the industrial base. However, it currently wades into waters beyond the scope of national security. The act must maintain a narrow focus on national defense and avoid intervention in areas that do not fall within a strict concept of national security.

Glaring weaknesses in the current defense industrial base are highlighted in the Trump administration's recent report, "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States." This report points to the severity of the issues and demonstrates the weakening of the U.S. strategic advantage when it comes to the industrial base. Commissioned by Executive Order 13806, the report lays out five macro forces currently undermining the strength of the industrial base, to include the "decline of U.S. manufacturing base capabilities and capacity" and "industrial policies of competitor nations." Each of these macro-level forces are driving risk in the domestic industrial base, and therefore to national security, and can be at least partially addressed by ensuring that the Defense Production Act upholds a strict understanding of national defense.

In its current form, the act can be used for a number of things not pertinent to national defense. These non-defense related efforts detract from the value of the authority and potentially misdirect defense funding.

The definition of national defense, according to the act, permits the use of its authorities to be used to support domestic preparedness for emergencies and recovery from natural disasters. Conflating humanitarian disasters with national security issues and implying that they merit similar government responses hinders the free market's ability to act where it can be of best use. Moreover, use of the act's funding for these kind of emergencies hinders the military rebuilding that is necessary for the U.S. to remain strong on the world stage by detouring resources away from its intended target.

Following the destructive 2017 natural disaster season, the Federal Emergency Management Agency invoked Title I of the DPA — which authorizes the prioritization of defense programs, contracts and orders and the allocation of resources accordingly — to provide food and water assistance and restore power grids. This action was rooted in the notion that the act could be used as an all-purpose tool in times of crisis, when in reality, the word "crisis" appears nowhere in the act's language. The Defense Production Act was not structured to be a rescue tool in times of humanitarian need. Rather, it is best employed to support the industrial base to support national defense.

DEFENSE DEPT.

Additionally, the Defense Production Act can and has been used to stimulate domestic energy production for commercial uses, an overstep currently allowed by the law. According to the 2013 Annual Industrial Capabilities report to Congress, in fiscal year 2013, the U.S. government contributed $3.61 million of the act's funding to a project that aimed to "establish a domestic, large-scale, commercial, feedstock flexible, manufacturing capacity" of bio-synthetic paraffinic kerosene. The report described the reasoning behind this program, which stressed the importance of energy diversification for the purposes of "energy security and environmental stewardship." While this may be a worthwhile goal, this investment was not relevant to national security to the degree that it justified government investment with dollars appropriated for national defense.

Another example of an inappropriate use of Title III funding was the Obama administration's 2012 initiative to advance the production of biofuel. Similar to the aforementioned project, the administration touted the need for energy security and environmental consciousness in its announcement of the initiative. In total, the Advanced Drop-In Biofuel Production Project — as it was titled in the 2014 Annual Industrial Capabilities report — was allotted a whopping $230.5 million of Title III funding. This project was marketed to support naval operations by providing a diverse production of domestic energy. However, President Barack Obama's use of the Defense Production Act to further this non-defense project diverted defense funding away from the defense industrial base. The overly broad definition of national defense allowed Obama to advance an environmental agenda by packaging it as a national security issue.

The issue of exploiting the Defense Production Act for non-defense reasons transcends administrations as reports surfaced in mid-2018 that the Trump administration was considering invoking the act to keep domestic coal mines online. A White House memo claimed that "federal action is necessary to stop the further premature retirements of fuel-secure generation capacity." While President Donald Trump ultimately did not follow through with his proposal, this move represents how easy it is to misuse the powers of the act in order to promote a non-defense related agenda. The Defense Production Act should not be used to further any form of a "Buy American" agenda; that is not the goal of the act. Rather, its authorities are there to step in where there is a domestic capacity shortfall for a national security requirement.

These inappropriate uses of the Defense Production Act do not mitigate its utility, but rather should be curbed in order to protect its utilization for defense-related programs. In fact, the act has indeed seen success over the years. Recent investments enhancing the strength and resiliency of essential sectors such as microelectronics and the space industrial base highlight its productiveness.

Title I has been successfully employed to prioritize contracts for "ballistic material used in body armor both [for] the Army and Marine Corps" to ensure a timely delivery, as mentioned in a 2008 report by the U.S. Government Accountability Office. During an increase in production of mine-resistant ambush protected vehicles, the Defense Department used Title I authorities to help prevent a shortage of armor plates. The act's priorities and allocations authorities can be of particular use during production surges and when additional capabilities are necessary for deterrence.

An example of how Title III can properly support the defense industrial base is the Steel Plate Production Project. Beginning in fiscal year 2014, $17.6 million of Title III funding was given to this project, discussed in the 2014 Annual Industrial Capabilities report, in order to compensate for the lack of "widespread commercial application" for Navy-grade steel plates. The project summary notes the lack of return on investment for the domestic industry to establish the capacity to produce these steel plates. The Defense Production Act was able to step in to support this industry, thereby reducing the threat of delays in its production line. Because weapons systems feature such intricate supply chains, it is critical that they are protected against sudden breakages and able to continue their course.

The Executive Order 13806 report provides target areas for potential Defense Production Act attention based on research-based analysis of the industrial base. The report identifies industries currently plagued by single sources, fragile suppliers, foreign dependency and other such risks. To date, 14 presidential determinations have been issued that focus on addressing strategic industrial base risks identified in the report. These determinations have indicated that materials such as sonobuoys, lithium seawater batteries, and critical chemicals for missiles and munitions are in need of Title III project funding to help mitigate the risks in those industries.

Title III projects should have clear ties to identified shortfalls of domestic capacity, such as those identified in the Executive Order 13806 report. Infusion of federal investment into the private sector on behalf of the Defense Production Act must be accompanied by a narrow focus and a fact-based analysis of how it will contribute to national defense.

The Defense Production Act has proven to be a successful tool to support national security by eliminating vulnerabilities in the defense industrial base. These vulnerabilities — whether they be single sources, fragile suppliers, material shortages or foreign dependency — have the potential to be detrimental to military operations and objectives. It is important that we recognize both the strengths and the weaknesses of the DPA in order to improve its effectiveness. This act was never intended to influence areas of the private sector with a purely commercial base. Rather, it was intended to support national defense industry partners.

The time to pay attention to the gaps in the domestic industrial base is not after the need becomes acute enough that proper weapons systems are not being delivered to the warfighter. There is no better time than the present to take proactive steps to enhance the effectiveness of the Defense Production Act and ensure its goals are being met. The industrial base is fundamental to U.S. military strength. The nation cannot afford to let it erode. **ND**

Emma Watkins is a research assistant at the Heritage Foundation.