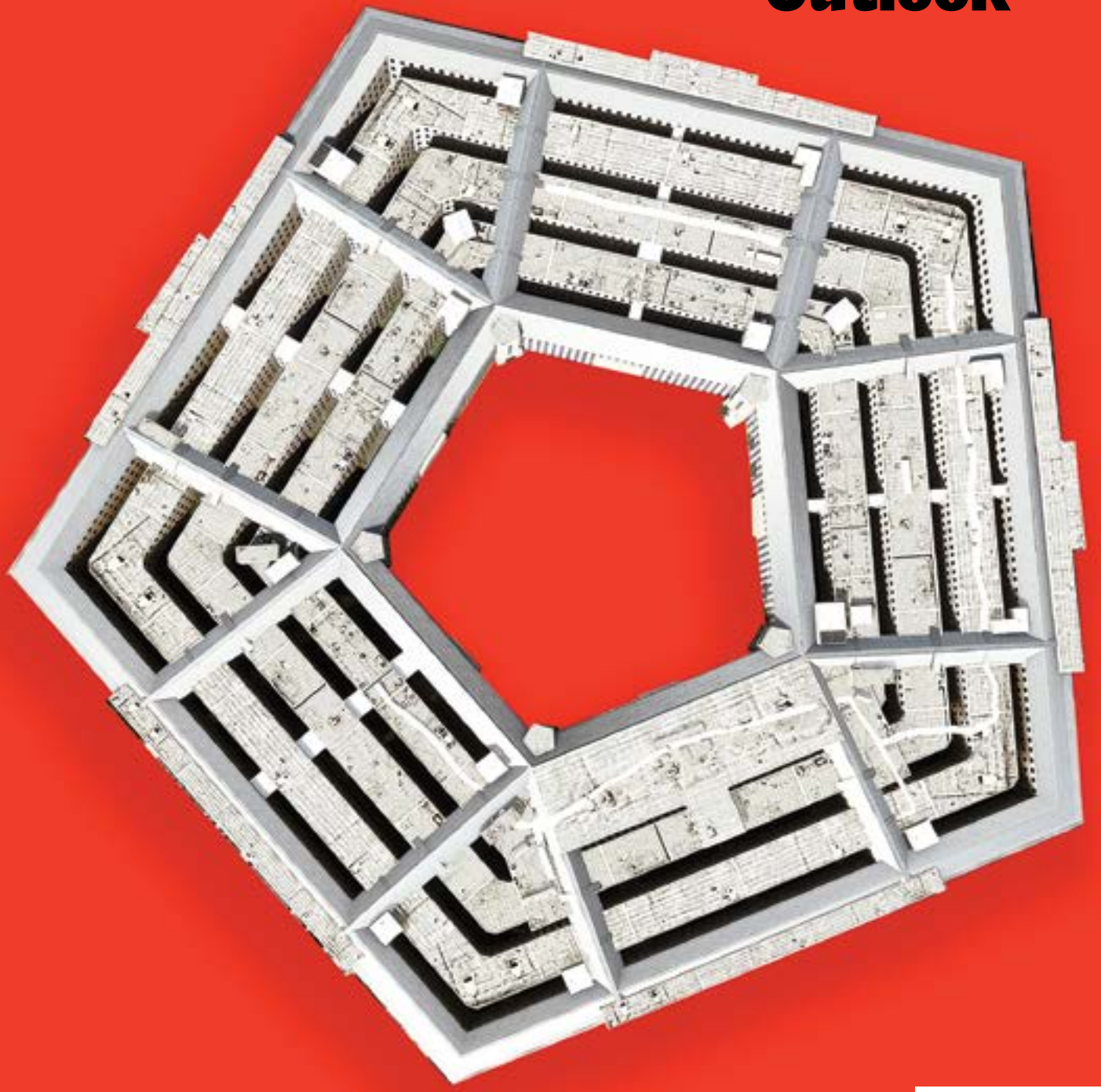
NDIA

# National DEFENSE

## Defense Industrial Base Vitality Outlook



SPECIAL REPORT

# Introduction to Vital Signs 2021

*By Hawk Carlisle*

The National Defense Industrial Association is proud to release its second annual report on the health and readiness of the defense industrial base, "Vital Signs 2021."

This year we again give a rating of a C with an overarching score of 74, slightly lower than that of 75 last year. Because this report is an indication of the environment defense contractors operate in vice a report on the companies themselves, this means that the environment remains challenging.

In this special report, you will get a preview of the scores and findings and articles that begin to decipher what that means going forward.

*Continues on page 4.*

# Table of Contents

# Get ready for CMMC with C3 Integrated Solutions

## The C3 CMMC Readiness Program

C3 Integrated Solutions specializes in securing our nation's Defense Industrial Base using Microsoft Government Cloud.

Our C3 CMMC Readiness Program leverages the Microsoft 365 GCC High, Azure Government, and industry leading partners to meet Cybersecurity Maturity Model Certification (CMMC) requirements in a methodical, incremental approach.

To get the most out of GCC High and understand your road to compliance, turn to C3 Integrated Solutions.

## Get started today

**To learn more about the C3 CMMC Readiness Program, visit c3isit.com/CMMC.**

Microsoft Partner
Microsoft
Gold Cloud Productivity
Gold Windows and Devices
Silver Enterprise Mobility Management
Silver Collaboration and Content
Silver Security

Inc. 5000

C3 INTEGRATED SOLUTIONS
connect, communicate, collaborate

(571) 384-7950 | info@c3isit.com
1001 19th Street N | Suite 1200 | Arlington, VA 22209

## Introduction BY HAWK CARLISLE

Later this month, the National Defense Industrial Association will release its second annual report on the health and readiness of the defense industrial base, "Vital Signs 2021."

This year we again give a rating of a C with an overarching score of 74, slightly lower than that of 75 last year. Because this report is an indication of the environment defense contractors operate in vice a report on the companies themselves, this means that the environment remains challenging. In this issue of *National Defense*, you will get a preview of the scores and findings and articles that begin to decipher what that means going forward.

"Vital Signs" is a data-driven report drawing from the expansive data set provided by our data science partner, Govini, and by multiple other unclassified sets available on a yearly basis.

Because this year has been unique to say the least, many will look immediately to see what effect the COVID-19 public health crisis had on the industrial base and what long-term effects will result. But the nature of the data sets we use means that much of the report provides a lagging indicator of what is happening within the defense industrial base.

For one, to ensure we control for one-year anomalies and show real trends, all our scores are based on a three-year running average. Additionally, to get a complete and comparable data set across variables and measures, scores reflect data collected up to the end of the previous calendar year. This means that for "Vital Signs 2021," we capture the state of the industrial base up to, but not including, the onset of the COVID-19 crisis.

> "The silver lining of the COVID-19 crisis has been that companies and the Defense Department have an increasing understanding of the supply chain."

So, when reading the report, one needs to remember this is what the defense industrial base looked like going into the crisis, and all that has happened since will impact what the sector looks like post-pandemic. So, when we find that year-over-year we saw a halving of new entrants receiving Defense Department contracts — 12,000 in 2018 compared to 6,000 in 2019 — even before the pandemic hit, this is a worrying statistic.

There is one caveat to this report being a lagging indicator, and that is something that we have added to our report to capture some qualitative aspects of the health and readiness of the industrial base we couldn't through available databases. We have begun an annual survey that asks two sets of questions.

One set is questions we will ask each year to include questions related to their work with the Defense Department, business confidence and outlook. With the questions asked each year, we will be able to do trend analysis over time. The other is a set of questions that will change annually focused on unique aspects affecting the defense industrial base that year. For this year, those questions focused on defense contractors' experiences surrounding the COVID-19 crisis and their resulting expectations.

Interestingly, the results of this study give us some leading indicators of what we have noted anecdotally happening within the base. On average, the smaller the contractor, the more challenging the COVID-19 crisis is to the company. Also, across the board over 70 percent say the crisis has had a moderate to large negative effect on their company's business. Regarding business recovery, over 50 percent believe it will take a minimum of six months to return to normal while an additional 13 percent believe the sector will never fully recover.

We enter the next policy cycle with a new Congress, a new administration, and new leadership in the Pentagon. It is these headwinds, coupled with predicted flat budgets, increased regulatory burdens like those focused on industrial security with the implementation of the Cybersecurity Maturity Model Certification and Section 889 Part B of the fiscal year 2019 National Defense Authorization Act, and an increasingly capable threat that these leaders must take into account when crafting the legislation and rules affecting the industry.

Some good has come out of 2020. The silver lining of the COVID-19 crisis has been that companies and the Defense Department have an increasing understanding of the supply chain. With supply chains already identified as vulnerable by the Executive Order 13806 Report, the collective headwinds have demonstrated that supply chain visibility and resiliency are vital going forward and worthy of increased attention and investments.

The health and readiness of the defense industrial base have been and will remain key to our military's continued advantages across all warfighting domains. For the sector to remain vibrant, it has to be one where well-run companies thrive no matter where they sit in the supply chain and innovative new and nontraditional companies see opportunity.

That combination is key to producing the best of the best for our warfighters; providing interoperable capabilities to our friends, allies and partners overseas; and having a surge capacity in the event of a national emergency.

So, as you read through this issue of *National Defense*, take the time to look at both the lagging and leading indicators measured in this year's Vital Signs report and consider what it means to have a healthy, ready industrial base.

Also, consider what it takes in terms of deliberate policy and investments to restore its health following the COVID-19 crises and reinvigorate the sector as one of both opportunity and meaningful impact to the nation's security. ND

**Retired Air Force Gen. Hawk Carlisle is president and CEO of the National Defense Industrial Association.**

# VITAL SIGNS

## Second Annual Study Reveals 'C' Average for Defense Industrial Base

**BY WESLEY HALLMAN AND NICK JONES**

In 2018, the Defense Department released "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States," a report focused on the production risks to critical defense industrial supply chains.

The report starkly framed the health of the U.S. defense industrial base as key to the readiness of the nation to confront near-term threats and compete in an age of great power competition.

Despite the report's high-resolution snapshot of the DIB's "unprecedented set of challenges," the report did not provide a publicly available summary measurement of the health and readiness of the defense industrial base or a simple way of tracking it over time.

To fill this gap, the National Defense Industrial Association in 2020 completed "Vital Signs 2020," which provided an unclassified summary of the health and readiness of the defense industrial base that was accessible to both the public and the defense policy community. "Vital Signs 2021" is the second installment.

In order to provide a comprehensive assessment, our procedure involved standardizing and integrating different elements that impact the performance of the defense industrial base and the overall business environment.

Like "Vital Signs 2020," this report's final grade for the health and readiness of the defense industrial base was a "C." This year's score was 74, slightly lower than last year's 75.

While passing, the "C" grade reflects a business environment that is characterized by contrasting areas of concern and confidence. It also reflects the state in which the defense industrial base entered the COVID-19 pandemic, which dramatically disrupted the daily lives of every American and the flow of U.S. commerce.

Continued deterioration in industrial security and the availability of skilled labor and materials emerged from the analysis as areas of clear concern. Favorable conditions for competition in the defense contracting market and a rising demand for defense goods and services reflected growth in the U.S. defense budget and increased overseas sales.

NDIA intends Vital Signs 2021 to contribute to the debate about national defense acquisition strategy by offering a common set of indicators — "vital signs" — of the defense industrial base partners that give the men and women in uniform an advantage in all warfare domains.

In order to complete this year's Vital Signs, we conducted a months-long study of data related to eight different dimensions that shape the performance capabilities of defense contractors: competition; cost production input; 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 publicly available longitudinal statistical indicators, converted each of them into an index score on a scale of 0 to 100, and evaluated three years of scores for each indicator — a running three-year average to control for single-year anomalies. A score of 100 equates to a baseline associated with

the Carter-Reagan buildup of 1979-1986 or, if corresponding data is not available, a more recent peak value.

With the exception of our Vital Signs 2021 member survey, which was fielded in August 2020, our datasets are lagging indicators collected before the nationwide lockdowns that occurred in March 2020 at the beginning of the COVID-19 pandemic. These lagging indicators provide insights into how the defense industrial base entered the pandemic which may give future policymakers a baseline to evaluate the defense industrial base's ability to cope with disruptions due to a national crisis.

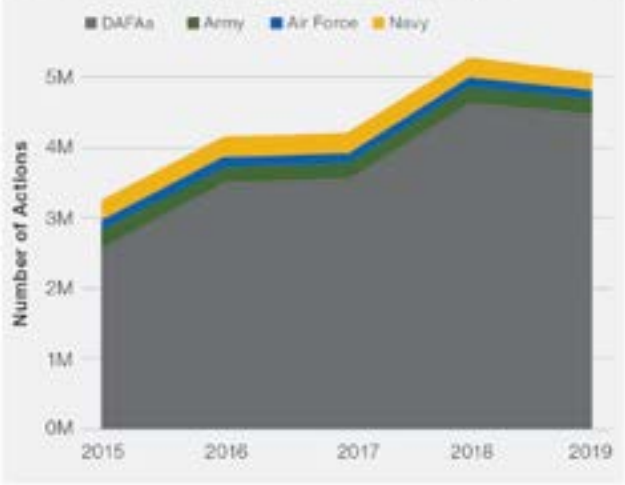
Vital Signs 2021 reveals a defense industrial base that entered the COVID-19 pandemic in a weakened state. As noted, with the exception of data from our August 2020 Vital Signs 2021 member survey, most data were published before the disruptions caused by the nationwide COVID-19 lockdowns and the concomitant overseas actions impacting certain supply chains.

The final "grades" are based solely on data from before the COVID-19 pandemic. Six conditions earned composite scores lower than 80, and four earned scores lower than 70, which we consider failing grades — the same as last year's report. These scores suggest that the defense industrial base is continuing to face multiple challenges to its ability to thrive.

Industrial security scored the lowest among the eight dimensions with a 56 for 2020. Industrial security has gained prominence as massive data breaches and brazen acts of economic espionage by state and nonstate actors plagued defense contractors in recent years.

To assess industrial security conditions, we analyzed indicators of threats to information security and to intellectual property rights. The score incorporates MITRE's annual average of the threat severity of the new cyber vulnerabilities, which improved slightly from the 2018 score of 17 to a similarly dismal score of

**DoD Contract Actions, Including Modifications, FY15 – FY19**




Source: Govini (2020)

**DoD Contract Awards, FY15 – FY19**


Source: Govini (2020)

**DoD Competitive Awards: Average Offers Received Per Award, By Category Management Group, FY15 – FY19**


Source: Govini (2020)

18, in 2020.

In contrast, threats to IP rights scored 100 out of 100 for 2019 as the number of new FBI cases into IP rights violations steadily declined since reaching an all-time high in 2011. Defense industry production inputs also scored poorly in 2020 with a score of 68, a steady score since 2018. Major production inputs include skilled labor, intermediate goods and services, and raw materials used to manufacture or develop end-products and services for defense consumption.

Our estimate of the size of the defense industry workforce, currently about 1.1 million people, falls substantially below its mid-1980s peak size of 3.2 million. The indicators for security clearance processing also contributed to the low overall score for production inputs as backlogs have improved but continue to persist.

The competitive environment and the state of demand for defense goods and services were areas of confidence. Over the past few years, the Defense Department has averaged about 701,000 prime contracts a year and had over $394 billion in prime contract obligations in 2019, according to an analysis conducted by our research partner Govini.

Analysis of the top 100 publicly traded defense contract recipients produced a competition score of 91 for 2020. Several high scoring indicators drove the strength of market competition conditions, including 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 in the defense industrial base. Additionally, the DIB earned a score of 77 for profitability for 2020, based on a new methodology for this edition of the report.

Demand for defense goods and services received a score of 93 for 2020, which is a 16-point increase over 2018. The high score for demand is a result of the recent increase in contract obligations issued by the department. Total contract obligations grew from $329 billion in fiscal year 2017, to $394 billion in 2019, a 20 percent increase. Foreign military sales also grew by nearly 20 percent over the same time period.

Other takeaways: Innovation conditions within the defense industrial base received a score of 71 for 2020, two points down from its 2018 score.

Notably, the U.S. share of global investment in research and development was only 28 percent, down from a peak of 38 percent in 2001. In early 2020, before the pandemic took hold, the percentage of Americans that thought the United States was spending "too little" on national defense was nearly half as many as in 2018, the largest two-year drop since 1983, which may indicate a decrease in the American public's appetite for major increases in military spending.

Acquisition reform and budget stability, two of NDIA's strategic priorities, continue to be top of mind for the defense industrial base. In the survey, when asked what the most important thing the government can do to help the defense industrial base, respondents said that streamlining the acquisition process (35 percent) and budget stability (nearly 32 percent) were the most important.

Defense Dept. photo

When asked what conditions would limit their firm's willingness or ability to devote larger amounts of productive capacity to military production, 48 percent of respondents said uncertain prospects of continuing volumes of business was a moderate deterrent and 41.5 percent of respondents said that the burden of government paperwork was a moderate deterrent. Both findings underscore the continued importance of reforming the acquisition process and the need for budget stability.

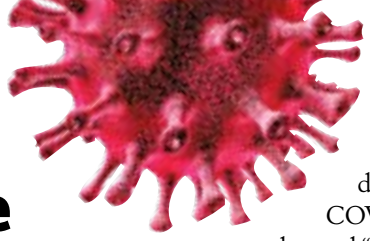
The capacity of the defense industrial base to grow its output and fulfill a surge in military demand stands as a key test of its health and readiness. Productive capacity and surge readiness earned a score of 66 for 2020, a 15-point decrease from 2019. Declines in output efficiency contributed to the declining trend. Productive capacity is baselined against the defense buildup that began under the Carter administration and accelerated through the Reagan administration. The Carter-Reagan Era buildup involved a 31 percent surge in Defense Department expenditures.

The health and readiness of the DIB poses a challenge to the acquisition community. With the growing expectation for the defense industrial base to meet the challenges faced during an era of great power competition, Vital Signs 2021 highlights several hurdles that the base must overcome coming out of the COVID-19 pandemic. The overall health grade of "C" suggests a satisfactory ability to meet current industrial requirements.

Our full report will release to the public at the end of January. We hope that Vital Signs 2021 will drive policy debates in the coming legislative policy cycle and inform the discussions and actions that lead to an improved grade for Vital Signs 2022 and beyond. **ND**

**Wesley Hallman is vice president of strategy and policy, and Nick Jones director of regulatory policy at NDIA.**

# Future Uncertain For Industrial Base As Pandemic Spreads



**BY CONNIE LEE**

While the United States continues to deal with challenges posed by the COVID-19 pandemic, it is still too early to know how the health of the defense industry will fare in the long run, according to analysts.

"The magnitude of the virus … it's really unknown, a lot of this just has to do with when the virus is going to go away, ... how quickly [a vaccine] can be deployed," Nick Jones, the National Defense Industrial Association's director of regulatory policy, said in an interview. "COVID-19 is going to continue to be an issue until the virus is at very low levels, which may be who knows how long," he added.

Jones' comments echo sentiments expressed by Ellen Lord, the Pentagon's undersecretary of defense for acquisition and sustainment. During a virtual *Defense News* conference in September, Lord said many of the effects of COVID-19 may be yet to come.

"All the reports that have come out in large part don't reflect the hits that were taken by business," she said. "There have been mixed reports in terms of revenue and profitability. I would contend that most of the effects of COVID haven't yet been seen, because most companies gave their employees time off — they stretched out production, paid a lot of people for working 100 percent when, perhaps, they were only getting 50 percent of the hours in, and so forth."

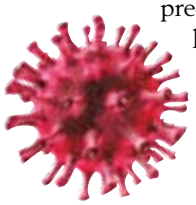
In November, Lord said she did not expect to see additional company closures despite an apparent rise in infections. The United States passed 4 million COVID-19 cases that month, according to the Centers for Disease Control and Prevention.

Another large wave of the virus is underway, and forecasts from the CDC anticipated 690,000 to 1.7 million new cases during the last week of December.

Lord said she is concerned that the COVID-19 case-count is still increasing in industry.

"I'm optimistic that although cases are going up, industry is going to continue to be very resilient. And we will continue to add pretty impressive productivity rates," she noted during the American Institute of Aeronautics and Astronautics' ASCEND conference.

At the beginning of the pandemic, about 700 defense companies were shut down to mitigate the spread of the virus. However, that number is now down to one, Lord said. Enough precautions have been taken to potentially avoid large-scale closures again, she said.



Industry has taken steps to space out manufacturing lines to find ways to comply with all the CDC regulations and "those have really prevented severe cases and the need to shut down," she said.

Lord said she is unsure if members of the defense industry will receive priority when a COVID-19 vaccine is released. The sector was deemed "essential infrastructure" in the early days of the pandemic, which enabled companies and employees to avoid some of the lockdown restrictions faced by "non-essential" businesses.

"I don't have the answer to that," she said. "That's being sorted out right now in the White House."

As of press time, the Food and Drug Administration was weighing whether to approve emergency use of newly developed vaccines. They were expected to start being distributed to high priority individuals such as front-line health care workers and other vulnerable segments of the population by the end of December.

The defense acquisition workforce is continuing to adjust to pandemic restrictions. Employees who must work in sensitive compartmented information facilities are doing so in shifts, and the Defense Acquisition University has transitioned completely to online courses, Lord said in December.

"I'm incredibly proud of what was done and how quickly we found that everyone adapted to being efficient," she said. "I hope we do not backtrack in terms of efficiencies when we get to whatever our stable situation is."

As the United States continues to navigate through the pandemic, the defense industry appears to be an economic "safe haven" for companies that operate in both the defense and commercial space, said Robbie Van Steenburg, regulatory associate at NDIA.

"That's one area where things, at least temporarily, there hasn't been a whole lot of negative general economic pressure," he said. The defense industry is doing OK for now, he added. In quarterly earnings calls, the defense divisions of their businesses tend to be doing better right now than the non-defense side, he said.

However, it is difficult to predict if this state of affairs is here to say, Van Steenburg noted.

"I don't know if this is temporary or not," he said. "The fact that the defense industry has had so few closures — due to COVID and the recession and everything — I think that's a pretty good way to sort of look and say, 'OK, things could be worse in the defense industry.'"

Defense may also be an area where companies can thrive while other sectors such as commercial aviation continue to flounder, he said.

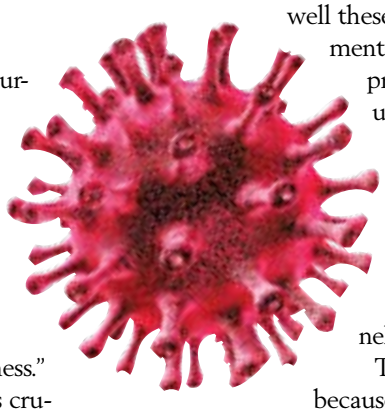
However, Kevin Fahey, assistant secretary of defense for acquisition, noted the defense industry does experience effects from the decline in commercial aviation. The Pentagon has had to find alternative means for transporting equipment, resulting in higher costs, he noted.

"A lot of people don't realize that travel restrictions … have a major impact because much of our industry is tied to the commercial airlines [and] most of our transport of equipment is commercial," he said at NDIA's Joint Armaments, Robotics, and Munitions Digital Experience conference in November.

The Defense Department is also hoping that Congress will have an appropriation to go along with Section 3610, which is a part of the Coronavirus Aid, Relief, and Economic Security Act passed in March 2020. The section authorizes agencies to reimburse contractors for paid leave taken during the pandemic. As of press time, Congress had not yet appropriated those funds.

"As of today, we don't have an appropriation to pay those costs," Fahey said.

The DoD needs money for 3610 "and other COVID costs" as well, he noted, which assists in purchasing safety items such as personal protective equipment. Fahey said he suspects that some of the smaller subcontractors may be concealing financial hardships from the pandemic in fear that the primes may look for alternative companies.



"If we don't get those costs, we will be seeing impacts for years to come," he said. "It could force some contractors and small businesses out of business."

Additionally, keeping the industrial base afloat is crucial to ensuring that companies do not turn to competitors such as China for investments, he said.

"Foreign investment caused by COVID has us scared," he said. "Most of our industry would rather have money from the United States and Canada. But if they can't survive without money, what are they going to do?"

Meanwhile, companies facing economic downturns are laying off employees. In October, Boeing announced that it will reduce its workforce to 130,000 by the end of 2021. The company reported a $466 million net loss during the third quarter of 2020. This was due both to the grounding of the 737 MAX aircraft and COVID-19 complications, according to the aerospace giant.

"There's no doubt that this moment is among the most difficult in our more than 100-year history," Dave Calhoun, Boeing's president and CEO, said in the company's third quarter earnings call. However, "through it all, I remain confident in Boeing's long-term future," he added.

Conversely, Lockheed Martin, which relies more heavily on defense contracts, had a third quarter net sales of $16.5 billion. In 2019 the company had a net sales of $15.2 billion in the third quarter. The company has been accelerating cash payments to its supplier base to help alleviate COVID-19 complications.

"Since March, we have accelerated payments to more than 8,300 suppliers, including more than 5,000 small businesses across all 50 states, the District of Columbia, Puerto Rico and 39 nations," the company said in a September statement.

General Dynamics — another firm that leans heavily on government contracts — reported net earnings of $834 million in the third quarter.

Jones noted that some defense contractors are uneasy about their future. Earlier this year, NDIA conducted a survey to gain feedback on COVID-19 impacts from the defense industry. As of September, 52 percent of about 1,100 respondents thought that it would take six months or longer for their businesses to return to normal, he said. Twelve percent said they did not think they would ever return to normal.

"I would say it's pretty unstable," he said. "You have a lot of companies, especially small suppliers, that are dependent on not only their defense contracts, but [commercial] aerospace."

New regulations such as the Cybersecurity Maturity Model Certification requirements may be a factor in determining how well these companies recover, he added. These requirements are part of the Defense Department's push to protect industrial base networks and controlled unclassified information from cyber attacks.

"We're concerned about that," Jones said. "But I think the Defense Department has done a great job working with associations and industry to respond to COVID-19, through the CARES Act, through accelerated progress payments and really keeping communication channels open between the government and industry."

The pandemic had a silver lining for the Pentagon because it spotlighted some of the challenges facing the Defense Department such as supply chain issues, Lord noted. It reinforced what the Pentagon had discussed in a 2018 report to assess the strength of the industrial base — that there was too much dependency on offshore companies, she said.

"We therefore were able to move out and make some investments in industrial capacity and throughput," she said. "When the pandemic rolled around and everyone realized how vulnerable we were as a nation without the [personal protective equipment] and the pharmaceuticals that we needed, where we depended on offshore sources. That heightened everybody's awareness of how that spread through the defense industry as well."

Cyber is another area of concern, Van Steenburg said. NDIA found that over the last year, the number of reported cyber vulnerabilities within companies has gone up, although the severity of those vulnerabilities has decreased, he said.

"It could be more people working online [or] it could just be we're better at catching them," he said. "It could be that more people are reporting them to the government when they find them. … I just know that, at least in terms of what the government … [is] pointing out, is that they're saying we're seeing a lot more vulnerabilities."

The Pentagon is also continuing to take steps to keep industry afloat using provisions in the CARES Act.

In December, it announced eight Defense Production Act Title III actions that fall under the legislation. Bender CCP, NCA Solutions, Bernard Cap and Aurora Industries, IDEAL Fastener Corp. and Boeing received funding. DPA Title III allows the government to provide resources to support defense initiatives and bolster critical nodes in the supply chain. The agreements were for $1.5 million, $2.3 million, $3 million, $5.1 million and $63 million, respectively.

"These actions will help retain critical workforce capabilities throughout disruptions caused by COVID-19 and restore some jobs lost due to the pandemic," the announcement stated. **ND**

iStock illustration

# Vital Signs Report Reflects Some Sobering News

As we await the publication of "Vital Signs 2021," I am reminded of President George Washington's First Annual Address to Congress almost 231 years ago this month.

In his address, Washington advised the 1st Congress "that they should promote such manufactories, [that] tend[s] to render them independent on others for essential, particularly for military supplies." Over the last 10 months, the COVID-19 pandemic has forced Americans to pay attention to the supply chains that support their everyday lives. For businesses and policymakers too, the pandemic has placed a renewed focus on the resiliency of U.S. industry and the defense industrial base.

In service to "promoting" the industrial base, "Vital Signs 2021: The Health and Readiness of the Defense Industrial Base," the National Defense Industrial Association's second annual edition, is designed to measure the status of the defense industry's health through eight conditions which describe the business environment that defense firms must cope with.

Like the four traditional vital sign conditions that physicians use to assess the status of their patients' life-sustaining functions — temperature, pulse, respiratory rate and blood pressure — we believe that the following eight conditions are essential to a well-functioning defense industrial base: competition, production inputs, demand, innovation, industrial security, supply chain, political and regulatory environment, and productive capacity and surge readiness.

Unlike the traditional medical vital signs, our condition scores and overall grade are not measured in real time but reflect the state of the defense industrial base before the COVID-19 pandemic began. These lagging indicators earned the environment in which we ask the defense industrial base to operate in, a "C" grade for health and readiness — a passing grade. We expect that next year's grade will capture how the environment changed because of the challenges of the pandemic, the economy and the ongoing social reckoning.

In the past few years, there have been several very well-done assessments produced by other defense-related trade associations, national security think-tanks and universities. Those assessments tended to evaluate the nation's ability to operate in contested environments, the impacts of specific policies, or simply illuminated facts and figures on the state of the industry. "Vital Signs" is unique amongst those reports because it is the only unclassified annual assessment specifically focused on measuring the health of the defense industrial base in a way that is accessible to NDIA's members, the American public and policymakers.

"Vital Signs 2021" does not make specific policy recommendations, it does not look at the performance of specific defense industry segments such as ships, autonomous systems, vertical lift, etc., and it does not attempt to make financial forecasts of markets or specific programs.

NDIA members contributed greatly to "Vital Signs 2021," through a survey that was fielded in August. We used the survey's results throughout the report and they are a valuable leading indicator in a report that relies heavily on data produced before the pandemic. We had over 1,100 responses to the survey, from all parts of the defense industrial base, which helped us to understand the initial impact of COVID-19, the business sentiment of the defense industrial base, and the capacity of the DIB to surge their operations.

Like NDIA's numerous engagements on the Cybersecurity Maturity Model Certification, Section 889 of the 2019 NDAA, and other issues, the survey was able to provide members a voice at the table that will positively impact future policymaking cycles. Of the many survey findings, we were surprised to learn that nearly 12 percent of the total survey respondents thought that their business would never return to the level it was at in 2019. This is sobering news.

We are grateful for our continued partnership with the data science company Govini, which allowed us to derive insights from the reams of publicly available information related to Defense Department contracts. Through Govini's proprietary tradecraft, we were able to learn that the average annual amount

> "Lagging indicators earned the environment in which we ask the defense industrial base to operate in, a 'C' grade ..."

of DoD innovation investments that used other transaction authorities rose by nearly 300 percent from 2015-2019, and that foreign military sales obligations increased 74 percent over the same time period.

We learned that the defense industrial base is becoming more competitive in some ways, with an increase in the average number of offers received for full and open competition increasing to 7.68 in 2019, from 4.58 in 2015. Defense services like transportation remain highly fragmented, with 14 offers per award, while professional services received less than two offers per award.

We are also grateful for our summer and academic year cohorts of junior fellows. This year, we were fortunate to have an outstanding group of fellows that mostly joined us remotely, from some of the best policy and law schools in the country.

The fellows fought through the pandemic induced challenges of uncertain class schedules, remote learning, and even a few hurricanes, to contribute to the research and writing of "Vital Signs 2021." Their grit shows us that the future of defense policymaking will be in good hands. ND

**Nick Jones is director of regulatory policy at NDIA.**

iStock illustration

# Defense Industry Could See Another Wave of Mergers, Acquisitions

iStock illustration

**BY JON HARPER**

The defense industry could be on the cusp of further consolidation as contractors look to bolster their business portfolios and access to innovation through mergers and acquisitions, analysts say.

M&A has been a long-term trend since the end of the Cold War and the 1993 "Last Supper" when then-Deputy Defense Secretary William Perry encouraged consolidation among contractors to achieve efficiencies in an era of significantly reduced military expenditures.

"Merger activity in the defense industry increased dramatically," noted a study by the Center for Strategic and International Studies, with the number of major prime contractors dropping from 50 to just six between 1993 and 2000.

While military budgets ramped up again in the decade after the 9/11 attacks, spending constraints stemming from the Budget Control Act of 2011, as well as the drawdowns in Iraq and Afghanistan during the Obama administration, had a major impact on industry, according to the CSIS study published in 2019 titled, "Evaluating Consolidation and the Threat of Monopolies within Industrial Sectors."

"Across categories and vendor sizes, the analysis found that the number of vendors receiving prime contracts from the Department of Defense dropped in all by 17,000, or nearly 20 percent over the drawdown period," the study said. Sectors experiencing major reductions in contact obligations for products and services included ships, aircraft, land vehicles, space systems, and missiles and ordnance.

In 2015, then-Undersecretary of Defense for Acquisition, Technology and Logistics Frank Kendall voiced concerns about the state of affairs.

"The trend toward fewer and larger prime contractors has the potential to affect innovation, limit the supply base, pose entry barriers to small, medium and large businesses, and ultimately reduce competition — resulting in higher prices to be paid by the American taxpayer," he warned.

There have been a number of high profile mergers and acquisitions in recent years including the combinations of General Dynamics and CSRA, Northrop Grumman and Orbital ATK, L-3 Technologies and Harris Corp., Lockheed Martin and Sikorsky, and Raytheon and United Technologies Corp.

Analysts say another wave of consolidation could be on the horizon. Many observers expect a decline in defense spending as the nation grapples with the economic fallout from the COVID-19 pandemic and exploding federal budget deficits.

"We forecast a range of scenarios, with the best case being essentially a flat budget, and the worst being a steep decline. If the worst case occurs, it's likely that new programs will be postponed, R&D cut for all but the most strategic efforts, and current procurements will slip," analysts with the Boston Consulting Group wrote in a recent report titled, "Building Beachheads in the U.S. Defense Market Through M&A."

The report added: "Such downturns have historically been periods of consolidation in the industry, a chance for stronger companies to buy firms in financial distress and either establish a beachhead in the U.S. or expand their presence."

A number of factors could drive mergers and acquisitions.

"Intense competition for fewer programs and contract awards … coupled with possible re-emergence of [lowest-price technically acceptable] contracts, may expedite consolidation in some of the more fragmented and under-capitalized segments," according to a report by advisory firm KPMG titled, "After the Shock: Implications for M&A in the Aerospace and Defense Market."

This could prompt companies to pursue both vertical and horizontal integration strategies, it noted.

In another study titled, "2020 Aerospace and Defense Industry Outlook: A Midyear Update," consulting firm Deloitte not-

ed that larger contractors may use acquisitions to gain access to new and advanced technologies. M&A activity could be shaped by demand growth in areas such as: command, control, communications, computers, intelligence, surveillance and reconnaissance, unmanned and autonomous vehicles and hypersonics.

During a quarterly earnings call in October, Lockheed Martin indicated it is on the hunt for opportunities.

"We're going to invest in R&D to sustain our technological leadership … but we're also going to seek acquisition and joint venture opportunities to deepen our capabilities and … add technological firepower to our existing company," said Lockheed president and CEO James Taiclet. "We plan to be active."

The company recently bought a company called i3 that gave Lockheed novel capability for hypersonic glide bodies, he noted. That is "something we wanted to bring in-house and again accelerate our own potential for developing that piece of the technology that's so absolutely critical."

Liquidity challenges and the prevalence of distressed assets could create a buyer's market for companies pursuing acquisitions, the KPMG report said.

M&A isn't just an option for the major primes, the Boston Consulting Group noted, suggesting other firms should pursue opportunities to become "conduits of innovation" for the large players.

To achieve that, contractors may need to acquire subunits from other companies, then couple their know-how with cutting edge capabilities.

Deloitte predicted that consolidation by parts family — components, aero structures, electronics and interiors — will also continue as firms focus on gaining economies of scale.

The Boston Consulting Group said: "Recent developments in the U.S. defense industry have placed it on the cusp of the next consolidation wave. Companies looking to make inroads have no time to waste. They need to lay their plans now to capitalize on opportunities."

What would be the consequences of further consolidation?

Basic economic theory would suggest that it would reduce competition and potentially lead to higher prices for goods and services for the Pentagon and taxpayers, said Greg Sanders, deputy director of the Defense-Industrial Initiatives Group at CSIS.

Primes have pushed back on the idea that larger defense contractors inherently undermine competition or inhibit innovation.

"What the companies will argue is that by bringing things together, they are able to rationalize, eke out efficiencies, get economies of scale, etc.," Sanders said. "Probably their best argument for that sort of thing might be that … there are better products they can provide, they are bringing different expertise."

There are a number of tools available to the Defense Department and other agencies to prevent unwanted consolidation and mitigate its effects.

One is regulatory scrutiny of proposed mergers and acquisitions. The Justice Department's Antitrust Division and the Federal Trade Commission lead the U.S. government's antitrust reviews, and the Pentagon provides input when deals involve the defense industry.

"The overriding goal of the agencies in enforcing the antitrust laws is to maintain competition going forward for the products and services purchased by DoD," the Justice Department and FTC said in a joint statement in 2016. "Competition ensures that DoD has a variety of sourcing alternatives and the most innovative technology to protect American soldiers, sailors, Marines and air crews, all at the lowest cost for the American taxpayer."

They assess whether a sufficient number of both prime and subcontractors will remain after a deal is consummated to ensure that future procurement competition is robust.

As part of its reviews, the agencies also consider procompetitive aspects of a proposed transaction, including economies of scale, decreased production costs and enhanced R&D capabilities.

"However, if a transaction threatens to harm innovation, reduce the number of competitive options needed by DoD, or otherwise lessen competition — and therefore has the potential to adversely affect our national security — the agencies will not hesitate to take appropriate enforcement action, including a suit to block the transaction," the statement added.

President Donald Trump has expressed concerns about combinations in the defense industry.

At the annual Defense News Conference in September, Undersecretary of Defense for Acquisition and Sustainment Ellen Lord was asked if she also had concerns.

"I actually put a process in place early on when we are notified of M&A deals that we go out very formally to all the services and agencies and ask for objective evidence as to whether or not these mergers or acquisitions will constrain competition in any way," she said.

"We've worked very, very closely with either FTC or DoJ on those deals to make sure there are divestitures, if needed," she added. "We watch very carefully. And at this point we think we've made some smart divestitures on some of those. And we like competition. It's our friend."

Another path the Pentagon could pursue to fend off consolidation is to award contracts to multiple offerors to build a particular type of system, "taking a bit of quantity from each" rather than conducting "big winner-take-all" competitions, Sanders said.

Requiring open systems architectures is another way to encourage competition when it comes time for technology upgrades, he noted.

Additionally, the Pentagon could utilize cost-based contracting in an effort to keep prices down.

Under that construct, "DoD gets access to a lot of cost and accounting data and will take a very close look, and you end up with a bit more of a utility model than a commercial competi-

iStock illustration

tion model," Sanders explained.

To add more players to the marketplace, the Defense Department can try to do business with nontraditional contractors and commercial firms. The military is already making a big push to tap into commercial tech and expand the use of other transaction authority agreements to speed prototyping and fielding of new capabilities. Most of those agreements are with nontraditional companies.

However, that could potentially lead to unintended consequences.

"Traditional defense technology developers may feel compelled to acquire or partner with emerging nontraditional suppliers, given nontraditional firms' current dominance in the prototyping marketplace," analyst Rhys McCormick wrote in a CSIS report titled, "Defense Acquisition Trends 2020."

If traditional players are unable to increase their market share in the next generation of defense systems, their revenue base will start to erode, he said. "This raises the potential for a substantial round of industry consolidation in the next five to 10 years."

However, Sanders doesn't anticipate consolidation on a scale seen in the 1990s after the Last Supper for several reasons. One is the expectation that U.S. defense spending will remain more robust than it was after the threat posed by the Soviet Union disappeared.

"The Cold War had ended. There was a definite sense that we were just in a different strategic state, whereas [today] there's a … very big bipartisan concern with Chinese activities," he said. "Even if you disagree about the amount of defense spending needed, we're not going from a period of higher tension to a lower one."

The amount of consolidation that has already occurred also means there are now fewer opportunities for contractors to merge, and analysts predict that proposed combinations of large companies would face intense regulatory scrutiny.

Some elements of the Democratic Party are less friendly toward big business. Sanders said the incoming Biden administration will likely be more wary of M&A than the previous one.

"We haven't seen that much detail on Biden antitrust policy," he said, "but I think that probably this administration would be a little more skeptical … on how much they want to encourage consolidation." ND

**Viewpoint** BY JOHN C. JOHNSON

# Forecasting the New Administration's Impact on Defense

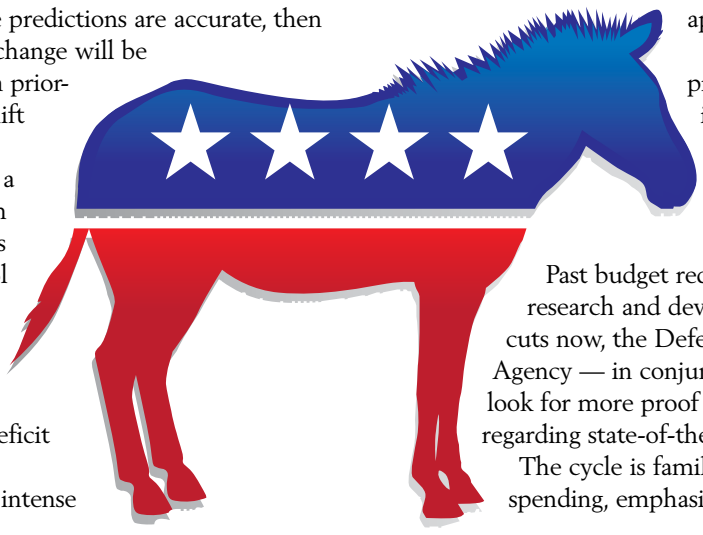
■ With each administration change the specter of uncertainty raises its head: Will the defense budget stay the course? Or, as a discretionary pool of money — approximately 50 percent — will the budget be tapped to plus-up social programs or serve to reduce budget deficits? Or perhaps both? This shift in administration is no different from those of the past, with the principal exception being the stark contrasts in political philosophy of the two candidates. This has fostered greater budgetary anxiety.

"Inside the Beltway" experts have predicted, with mounds of justification, a slight dip to a slight rise in defense allocations — bottom line, a flat budget. If these predictions are accurate, then the impact of the administration change will be minor, with shifts only in program priorities. But planning for a seismic shift may be more prudent.

The Obama administration left a significant fiscal deficit, along with dangerously low military readiness in the wake of the Budget Control Act. Then along came the unexpected pandemic, which necessitated trillions of dollars in economic relief packages that have driven the nation's budget deficit to breathtaking levels.

These factors, plus the push by intense elements within the Democratic Party to expand unemployment benefits, fund health care for all, eliminate college debt, and so forth, put additional pressure on the new Biden administration and the subsequent budget.

Consequently, one must now take an earnest look at the possibility of a deeper defense cut than both the military and industry desire. Another general election is years away, and politicians are more inclined to cut now, with increases reserved for election years to secure votes. Although sequestration is not envisioned, a little budgetary paranoia may be appropriate.



When budgets are reduced, production and force levels in military and industry headcount are impacted. Defense cuts result in increased unemployment, which would further aggravate an economy struggling with COVID-19.

Past budget reductions witnessed a shift to research and development in defense. With budget cuts now, the Defense Advanced Research Projects Agency — in conjunction with the services — will look for more proof of concept, 6.2 and 6.3 initiatives, regarding state-of-the-art technology.

The cycle is familiar to many: reduce defense spending, emphasize R&D; then increase defense

iStock illustrations

spending, attend to production. Foreshadowing this cycle is always the threat, and the threat dampens the severity of this budgetary cycle. For example, the dissolution of the Soviet Union caused a pause in Moscow's defense spending that Russian President Vladimir Putin is still striving to overcome, whereas China has not lost its stride or momentum in military growth.

In a Nov. 2 *Washington Post* article, Northrop Grumman CEO Kathy Warden said, "Defense spending is largely threat driven and today's threat environment warrants a strong defense." This comment is accurate, and echoed by other leaders in the national security community.

However, the Neville Chamberlains of the new administration may downplay any foreboding threat and thus advocate for defense budgetary cuts, looking instead to alliances, agreements, appeasement, and soft power projection through international aid programs. Some reductions because of the deficit and/or philosophical differences in government spending should be anticipated.

All that being said, defense companies do look and plan for various scenarios. After all, the severity of the threat and the appropriate force structure in response to the threat are open to a rather subjective interpretation.

The impacts on the defense community of a defense budget reduction are numerous, including but not limited to the following direct effects.

Any service program not in existence prior to the Trump administration will be subject to close review and re-justification.

The number of aircraft to be purchased will be reduced, lot buys pushed out, recapitalization delayed, satellite constellations deferred, ship keel-laying slowed — all likely impacted by budgetary pressure and/or shifts in defense prioritization.

Development activity such as in hypersonic weapons, autonomous combat vehicles, artificial intelligence, and other state-of-the-art technology pursuits will be hampered.

Legacy programs will be retired while new acquisitions with lesser effect on service requirements will be canceled — and this may become the norm.

In the next several months, there will be considerable dialogue regarding the defense budget and its impact on military readiness, established programs, and the defense industry, but we will see little if any comments on and concerns about the indirect effects of the new administration's policy changes on the defense industry. Indirect impacts can have a more lasting negative effect on the industry.

An immediate concern is with foreign military sales (FMS). In many cases, these sales help compensate for fluctuations in the U.S. defense budget; if they are eliminated or reduced, industry suffers. FMS business activity flows for years beyond the budget cycles generated by a new administration.

According to State Department figures, the United States sold $175 billion in weapons to foreign partners and allies in fiscal year 2020, which was a combination of FMS and direct commercial sales.

Current sales and forecast sales in the approval cycle will come under scrutiny. Expect the new administration to focus more on foreign policy versus domestic manufacturing, and nations to demonstrate considerably more concern for human rights infringement, which will impact FMS approvals.

Meanwhile, "Buy America," another indirect policy decision, will negatively affect overseas sales. Many governments stipulate a percentage of manufacturing be accomplished by their own domestic companies. Although Buy America is well intentioned, it would most assuredly harm overseas sales opportunities.

Subcontractors and suppliers might appreciate the focus on Buy America but might not be able to realize its benefits. COVID-19 restrictions imposed by state and local governments have severely impacted many companies. Furthermore, employees who have become ill have caused small companies, with limited employee depth in certain technical disciplines, to halt production. Illness, policy restrictions, and the enduring negative effects of businesses forced to close from prior sequestration are all severely straining the defense industry. Even if the military budget stays intact, the supply chain will continue to suffer from the smallest budgetary tremors.

Finally, to fully understand the possible environment resulting from a new administration, we must consider tertiary effects.

For example, the new administration has not wavered from its stated position of increasing corporate taxes. This will affect employee headcount and internal R&D activity. The subsequent risk is lower technology readiness levels for articles in development.

Government contracting offices will seek more fixed-price contracts to ensure they remain within budgetary constraints; accordingly, industry will have to propose at higher dollar amounts to reduce the possibility of write-offs and to reserve funds for higher risk mitigation tasks.

Also, the recently formed Space Force may be pressured to justify its existence. Many believe it adds layers of unnecessary bureaucracy with a relatively small force structure.

In the final analysis, industry should expect some overall reduction in the defense budget in order for the government to fulfill social programs while addressing the deficit. FMS may not be sufficient to offset U.S. defense spending reductions, and a corporate tax increase would flow into the equation with its own set of negative ramifications.

Finally, the supply chain, which has suffered the brunt of sequestration, the pandemic — through policy and illness — and tax increases, will feel directly and indirectly any shift from the new administration.

Many in the new government understand the implications well and will work diligently to balance the impacts on defense and thus the economy; however, the White House will feel some obligation to appease those progressive elements within the Democratic party. **ND**

**Retired Air Force Col. John C. Johnson is a former vice president and general manager of Northrop Grumman. He can be reached at jjohn4236@yahoo.com.**

# Enthusiasm Growing at Pentagon for OTAs

**BY JON HARPER**

The Pentagon is using special contracting mechanisms to try to promote innovation and bring nontraditional partners into the acquisition fold.

The use of one of them — other transaction authority agreements — has skyrocketed in recent years. Meanwhile, spending on the more established Small Business Innovation Research program has remained flat, according to data presented in the National Defense Industrial Association's "Vital Signs 2021" report.


Other transaction authority agreements, or OTAs, are intended to cut through bureaucratic red tape and speed prototyping and delivery of new capabilities to the military. They have become an increasingly popular tool for acquisition officials since the 2016 National Defense Authorization Act encouraged their use.

OTA obligations rose from $4.4 billion in 2018 to $7.7 billion in 2019, the last year for which final numbers are available, according to a recent study by the Center for Strategic and International Studies tilted, "Defense Acquisition Trends 2020." That represents a 75 percent bump.

Between 2015 and 2019, the average annual amount of Pentagon innovation investment that used other transaction authorities rose by nearly 300 percent, according to the Vital Signs report on the health of the defense industrial base, which incorporated data provided by big data analytics firm Govini.

Analysts at Bloomberg Government said OTA growth continued to ramp up in fiscal year 2020, even though final numbers are not yet available.

"Our data is showing $14.8 billion for DoD and $16.3 billion [for the U.S. government] overall for FY 2020, so the total has gone up over 100 percent over FY 2019 and we're still waiting on the last month or so of data for DoD," Robert Levinson, senior defense analyst at Bloomberg Government, said in an email in December. "The enthusiasm for OTAs continues."

Most of the Pentagon's OTAs go to firms operating through consortia such as the National Armaments Consortium. More than 80 percent of the NAC's members are nontraditional companies. The consortium recently had to revamp its operations because the growing caseload was taxing its system.

"That just became a bow wave and it really wasn't tenable," NAC Executive Director Charlie Zisette told *National Defense*. "We knew we had to work closely with the Department of Defense and do … a process reset and take a look at how can we streamline this" to meet the growing demand.

The Army remains the leader in OTA usage among the Defense Department, but the other components saw "significant upticks" in recent years, according to the CSIS study.

Army OTA obligations increased from $3.07 billion in fiscal year 2018 to $4.95 billion in 2019, a 61 percent bump. Air Force obligations grew by 190 percent, going from $540 million to $1.56 billion. The Navy, which had "marginal" OTA obligations in previous years, saw a surge in 2019, from $30 million the previous year to $170 million, a 431 percent increase, according to the report.

In 2019, the Army accounted for 67 percent, the Air Force 21 percent, the Defense Advanced Research Projects Agency 6 percent, and the Navy 2 percent of defense OTA obligations, respectively, the study said.

"The Army is ahead of the other services because it had a head start," CSIS analyst Rhys McCormick, the author of the report, said in an interview. Army Contracting Command out of Picatinny Arsenal in New Jersey has been the Army's OTA "center of excellence" since well before the 2016 NDAA was passed, he noted. "When they started ramping up, the Army already had that institutional knowledge."

"The Army will continue to maintain its lead, but I think the other services are going to catch up," he added.

But will OTA spending continue to ramp up as fast as it has been recently?

"I definitely don't think the [current] growth rate is sustainable … but I think we're going to continue to see growth in OTAs in the coming years," McCormick said. "It just won't be at that crazy rate that we saw" after the 2016 NDAA was passed.

Usage of other transaction authority agreements could come under more intense scrutiny as they become more popular.

"There are definitely some concerns about transparency when it comes to OTAs" in terms of who they are going to, the level of competition and other data, McCormick said. "You could see some small pushes from Congress there where they are requiring greater transparency."

There is also the possibility of a high-profile program going off the rails, he noted.

"There is definitely a big risk that you have a major system fail during those OTAs," he said.

The Army recently had to reset its Optionally Manned Fighting Vehicle modernization initiative, which is leveraging other transaction authority. While the move garnered headlines, it didn't generate much political fallout.

"They caught it early enough and the problems weren't an OTA problem, they were a requirements problem," McCormick noted. "But I think there are some programs in the works that, if they fail, could lead to some serious curtailment of OTA authorities."

The Army's future vertical lift programs are an example, he noted. The service is leveraging other transaction authority agreements for its future armed reconnaissance aircraft, or FARA, and future long-range assault aircraft, or FLRAA, projects.

"The Army is in a good place, but developing any major weapons system is a major challenge," McCormick said. "The

iStock photo

Army is full-steam-ahead on OTAs on those two efforts. So there is a significant risk there."

While Congress wants the military to move faster in acquiring next-generation systems, that doesn't mean they are seeking to jettison the traditional procurement process. If lawmakers decide that the Defense Department is using other transaction authority excessively or inappropriately, they could compel the Pentagon to dial it back, McCormick said.

"OTAs are great, but you have to be careful about using them where they make sense, or you do risk losing this authority or having it severely curtailed," he said.

To bring nontraditional players and small businesses into the defense innovation ecosystem, the Pentagon is also leveraging the federal government's Small Business Innovation Research (SBIR) program and Small Business Technology Transfer (STTR) program.

The SBIR program was established by Congress in the 1980s to strengthen the role of innovative small businesses in federally funded R&D. The most significant difference between SBIR and its sister program STTR is that STTR requires a small business to have a research partner consisting of a university, federally funded research-and-development center, or another qualified nonprofit research institution.

The Defense Department accounts for about half of all U.S. government SBIR funding — $1.8 billion out of a total of approximately $3.7 billion in 2019, according to the Small Business Administration. Spending in this area has remained relatively flat in recent years, according to the Vital Signs 2021 report and other data.

Solicitations are released three times per year for SBIR and contain a number of technical topics that describe areas of interest and needs. Small businesses are invited to submit proposals dealing with one or more of the topics.

"Through the Navy's SBIR program, small businesses of 500 employees or less have the opportunity to address naval needs in more than 30 science-and-technology areas," according to a description on the Navy small business office website. "The SBIR program provides the fleet with the innovative advances in technology developed by small firms that have the courage, drive and flexibility to assume risks, develop niches, and generally compete in areas less attractive to larger firms."

One difference between SBIR and OTAs is that the former are limited to small businesses, whereas even the largest defense primes are eligible to receive OTA funding.

SBIR contracts also have price ceilings that don't apply to OTAs. SBIR deals involving the Defense Department are generally worth up to $50,000 for phase 1 awards and $750,000 for phase 2 awards, whereas some OTAs have been worth hundreds of millions of dollars for big-ticket projects like hypersonic weapons development.

Helping companies commercialize their products is another key aim of the SBIR program that doesn't necessarily apply to OTAs.

Defense officials have touted the broader economic benefits of SBIR/STTR investments.

A study conducted by TechLink in collaboration with the business research division of the Leeds School of Business at the University of Colorado in Boulder, tried to quantify the programs' overall contribution to the nation's economy and defense mission. It examined the economic outcomes from phase 2 contracts initiated in fiscal years 1995 to 2012, with the impacts measured up to 2018.

During that time period, the department invested $14.4 billion in small business R&D funding provided via 16,959 phase 2 contracts, according to the report titled, "National Economic Impacts from the DoD SBIR/STTR Program, 1995-2018."

More than half of those contracts — 58 percent — resulted in sales of new products and services based on the innovations developed under those deals, the study said.

Additional findings from the report include: $121 billion in total sales of new products and services; $28 billion in sales of new products to the U.S. military; $347 billion in total economic impact nationwide; and 1.5 million jobs supported with average compensation of about $73,000.

However, because the SBIR program doesn't fund phase 3 work, many participating companies haven't been able to cross the so-called "Valley of Death" between technology development and production deals because they weren't working with a program office.

"It wasn't connected to the big acquisition system — the market that we represent — and that created a Valley of Death," Assistant Secretary of the Air Force for Acquisition, Technology and Logistics Will Roper noted in September during a talk promoting AFVentures, the investment arm of the service's AFWERX initiative that is focused on fostering innovation.

"Unfortunately, the option that was only left to many companies hitting the end of the SBIR pipeline was to be acquired by a prime, and then ultimately that technology would be charged back to us, but probably with a little higher rate than we would have gotten from a small business," he added. *(For more on defense industry consolidation, see story on page 30)*

The Air Force aims to address that problem by providing additional sources of funding to help small businesses involved in innovative research bridge that gap, he noted.

Many analysts expect defense spending to decline in coming years, which could potentially take a bite out of the SBIR program.

"I definitely think that is a possibility," McCormick said of a downturn in funding. "We've seen in the past that SBIR has fallen as defense budgets have fallen."

However, McCormick said continued growth in OTA spending wouldn't necessarily divert resources from SBIR accounts.

"I don't think they should necessarily be competing for dollars," he said. "They both have similar types of [innovation] missions, but they also have distinct differences." **ND**

Army photo

# Nothing Seems to Stop Relentless Hackers Exfiltrating Trade Secrets


**BY YASMIN TADJDEH**

The news shocked the cybersecurity world: FireEye, a leading security company with 9,600 customers across 103 countries, had been hacked.

The perpetrator was not your run-of-the-mill hacker on his laptop, but a "highly sophisticated threat actor, one whose discipline, operational security and techniques lead us to believe it was a state-sponsored attack," said CEO Kevin Mandia.

The attack was led by a nation with top-tier offensive capabilities, he said in a blog post in early December announcing the breach. The attack was consistent with a nation-state cyber espionage effort, with the hacker primarily seeking information related to certain government customers.

While Mandia did not call out a specific country, experts were quick to suggest it was conducted by Russia.

The country is one of the leading perpetrators of cyber espionage alongside China. Both nations are listed as great power competitors by the 2018 U.S. National Defense Strategy.

The FireEye attack is indicative of a growing trend: cyber espionage has become an increasingly pervasive threat and is on the rise.

For the U.S. defense industrial base, companies are increasingly worried about adversaries attempting to siphon off critical information and glean insights into Defense Department weapon designs.

Contractors are bolstering their defenses, and the Pentagon is implementing new regulations through its Cybersecurity Maturity Model Certification, or CMMC, to help. But experts say that the defense industrial base remains vulnerable to attack.

In the National Defense Industrial Association's annual report "Vital Signs 2021," which grades the health of the defense industry, industrial security scored the lowest among eight different dimensions that shape the performance capabilities of defense contractors. It received a score of 56 out of 100 for 2020.

"Industrial security has gained prominence as massive data breaches and brazen acts of economic espionage by state and nonstate actors plagued defense contractors in recent years," said Wesley Hallman, NDIA vice president of strategy and policy and Nick Jones, NDIA director of regulatory policy, in a summary of the document.

According to a recent report by the Center for Strategic and International Studies and security firm McAfee, the "burden" of global cybercrime has reached more than $1 trillion dollars — with more than $945 billion in monetary loss and global spending on cybersecurity expected to exceed $145 billion in 2020.

The report — "The Hidden Costs of Cybercrime" — is in its fourth iteration. Since the 2018 version was released, the cost of cybercrimes has increased by more than 50 percent.

IP theft can represent a significant loss to agencies and companies and pose a national security risk, noted the report, which was released in December. It can be even harder to fight against when attackers are backed by a resourceful nation-state.

The defense industrial base is made up of more than 300,000 companies and only a small percentage are large, multi-billion-dollar firms, said Armando Seay, director and co-founder of the Maryland Innovation and Security Institute.

Those large "companies are pretty resilient. They're not impervious — no one is — but they have the dollars to invest substantially in cyber resilience," he said. But most of the firms that make up the DIB are small- and medium-sized businesses that average 50 employees or less.

Smaller firms are more vulnerable, he noted.

"They're interested in making that widget. That's what they do," Seay said. "They're not computer people, they're not internet folks."

And adversaries are taking note, he added. "When it comes to weapon systems, when it comes to software, satellites, space, data, the adversary is crawling all over the supply chain."

According to a RAND Corp. report, "Unclassified and Secure: A Defense Industrial Base Cyber Protection Program for Unclassified Defense Networks," cyber attacks designed to steal IP from U.S. companies are on the upswing.

The Pentagon's approach to thwarting attacks is based on the Defense Acquisition Regulation Supplement (DFARS) 252.204-7012 and National Institute of Standards and Technology (NIST) Special Publication 800-171. However, it "appears to be inadequate," the report said.

The document — which was released in 2020 — said that as of July 2019, no defense industrial base firm had been able to fully implement the cybersecurity controls specified in NIST SP 800-171 and that some medium-sized firms will not have the resources to comply with it.

Further, it noted that DFARS 252.204-7012 assumes that controlled unclassified information, or CUI, "flows down from the prime contractors, with primes responsible for denying a subtractor access to CUI if the subcontractor does not comply with regulation.

"However, many subcontractors are in business because of their trade secrets. CUI exists at all levels of the supply chain," the study noted.

CUI on unclassified defense industrial base networks are vulnerable to theft by foreign actors. "The persistent attacks and hemorrhaging of critical information and technology from unclassified networks, coupled with associated significant financial losses, erodes the U.S. DIB and threatens U.S. military advantage over the long term," the report said.

Even the Pentagon's much talked about CMMC effort — which requires the defense industry to better protect CUI — is not sufficient, RAND said.

iStock illustration

"Our cost analysis indicates that most small DIB firms may not be able to afford the cyber defenses that could be mandated by the CMMC, and many medium-sized DIB firms may face the same challenges, especially if held to the highest compliance levels of the CMMC."

Additionally, the cybersecurity architectures of small firms are likely to be "deficient" in several areas including authentication, network defenses, vulnerability scanning, software patching, and security information and event management, the report said.

RAND recommended the Defense Department establish what it called a DIB Cyber Protection Program, or DCP2, that would improve the monitoring and real-time health of industry networks, bolster cybersecurity, and offer data and legal protections.

"The DCP2 would be a voluntary program under which DoD would provide [cybersecurity tools] to DIB firms either free of charge or at significantly reduced licensing costs," the report said. "In turn, the DIB firms would agree to provide sanitized data … to a security operations center — either one run by DoD or a trusted third-party SOC — devoted exclusively to defending the DIB."

This security center would provide dynamic intelligence, security alerts and recommendations to defense contractors to identify and remediate advanced persistent threat incursions.

China is the leading actor behind global cyber espionage, according to the CSIS report.

"Economic espionage to benefit national industry has long been a hallmark of China's economic policy," the report said. "China accounts for roughly 80 percent of all economic espionage cases in the U.S., and it has cost the U.S. economy around half a trillion to a trillion dollars of damage."

Doug Howard, CEO of Pondurance, an Indiana-based cybersecurity company, said China is the adversary that gets the most press and attention.

Beijing takes a "shotgun" approach to its cyberespionage tactics, he said.

China's thinking is: "I'm going to go after everything, and I'll never worry about them seeing me. I'm just going to try to get in, and I'm going to break in, because … the hygiene of [the] security is pretty weak," Howard said.

Maiya Clark, a research assistant at the Heritage Foundation's Center for National Defense, said China's interests are widespread. It is looking for information on capabilities such as autonomous vehicles, semiconductors, cloud computing, aviation, space and maritime technology.

To determine what Beijing is after, officials need only take a look at the country's "Made in China 2025" strategy, said a report by the Harvard Kennedy School's Belfer Center for Science and International Affairs titled, "Confronting China's Effort to Steal Defense Information."

"The industries identified in this strategy either directly or indirectly impact the United States' ability to wage — or defend against — military action against its adversaries," said author Jeffrey Jones in the May 2020 report.

The report estimated that $300 billion per year is lost due to Chinese cyber espionage activities.

"The sheer magnitude of the value of the theft is alarming; however, the Chinese government is compounding the severity of the problem by releasing the results of this corporate theft to leading Chinese companies so that they can accelerate their research-and-development efforts without having to spend any money or devote the massive amounts of time and resources necessary to arrive at the information on their own," it said.

Russia takes a stealthier and more sophisticated approach to its cyber attacks compared to China, Howard said.

"They will take years and years and years to compromise something," he said. "Their dwell time is extremely high relative to … somebody like China."

Moscow is looking for assets such as code from the U.S. defense industrial infrastructure, he said. It also focuses on broad compromises of organizations, targeting network and security providers, he noted weeks before the FireEye breach was announced.

Those companies "would be high value targets because if they can compromise a security technology that is broadly deployed, you can imagine the havoc that that would attain," he said. "That's not an easy thing to do. You're not just going to hack into the average security company and steal their code. But if you were successful, and if you spent two years or three years doing that and had great success, you can imagine the havoc that would happen."

Cyber attacks are also coming from the Korean Peninsula and the Middle East, but China and Russia remain the most pressing concerns, Howard noted.

Meanwhile, the U.S. government is taking note. At the Pentagon's Joint Artificial Intelligence Center, officials are reminded every day that the AI space is a competitive environment and that adversaries are interested in stealing its work, said Marine Corps Lt. Gen. Michael Groen, director of the organization.

"We are wide awake to the threat posed by foreign actors especially who have a proven track record of stealing intellectual property from wherever they can get their hands," he said. "We're going to try to provide an effective defense to ensure that doesn't happen."

The organization has developed a number of cybersecurity tools that can help industry better detect threats in their networks, he noted during a briefing with reporters in November.

"We have to be able to ascertain our data," he said. "We have to know its provenance. We have to know that the networks that we pass that data on are sound and secure."

What can contractors do to help stem the hemorrhaging of critical information? They should always assume that they are being targeted, said Richard Chitamitre, a federal sales engineer at Corelight, a network security company based in San Francisco.

"You should always assume that you are compromised and that adversaries are hiding in plain sight and pretending to look like normal traffic," he said. "The moment that they start to take data it's … usually going to be a bit too late because by the time you find out and you've installed the security camera, they've already walked out the door." ND

# Hypersonics Illustrate Supply Chain Vulnerabilities

Hypersonics — the science behind missiles that travel in excess of Mach 5 and can quickly change trajectory mid-flight — illustrate the challenges faced by U.S. companies working on emerging technologies.

Contractors engaged in these areas must be vigilant about their supply chain vulnerabilities. They also need to be aware of the regulatory risks posed by foreign investment, including review and potential intervention by the Committee on Foreign Investment in the United States (CFIUS).

Because hypersonic weapons are an emerging critical technology vital to future warfighting capabilities, nation-states are aggressively pursuing them. Several countries, including U.S. allies and competitors, are independently developing hypersonic technologies.

This competition has led some to fear a coming arms race. Notably, both China and Russia have been touting their growing hypersonic capabilities. The U.S. government worries that these countries may take advantage of "a lull in U.S. modernization" to improve their capabilities in this area, including through surreptitious means.

The international market for hypersonic technology is expected to grow at a compound annual rate of over 7 percent over the next five years.

The increase in demand for hypersonic technology components does not come only from abroad. According to a May 2020 article in *Design and Development Today*, as recently as 2017 the Pentagon spent about $800 million on hypersonic weapons programs, rising to $3.4 billion in 2020. The administration's 2021 budget request seeks $3.6 billion.

While most investment in hypersonic technology is defense-related, venture capital investment has exceeded $300 million over the past five years, including support for commercial ventures.

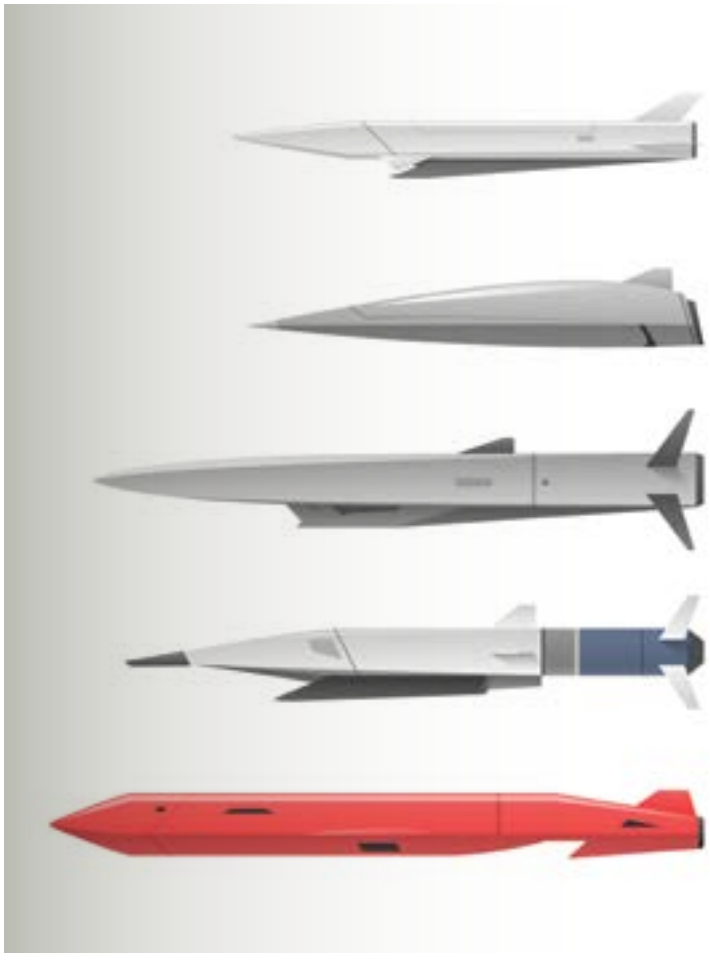
Despite the market demand, smaller suppliers of defense technology are struggling to keep up as their supply chains are impacted by the COVID-19 pandemic and an increasingly tense U.S.-China trade war. Large industrial providers and small research-and-development operations alike have had to face stay-at-home orders, travel restrictions and delivery delays. This issue has been especially acute for hypersonics. Many of the companies involved in this technology tend to be smaller, and those conducting R&D work could be more vulnerable to the economic effects of the pandemic and trade restrictions.

The effects of the pandemic and trade conflict with China come on the heels of increasing U.S. government restrictions on the use of Chinese products, based on concerns that China could infiltrate the U.S. defense industry by embedding its technology in weapon systems. As a result, the Pentagon is increasingly focused on the origin of components used in weapons systems.

Many defense contracting supply chains are global and have deep roots in China. Defense officials have highlighted the need to ensure that foreign nations cannot cut off U.S. companies' access to vital materials or buy their way into the defense-industrial base.

As part of this effort, agencies have increased their scrutiny of the supply chain to include even small companies developing components that could be incorporated into hypersonic technologies.

A recent analysis of the hypersonic supply chain conducted by big data analytics firm Govini noted that "the risk of supply chain infiltration by foreign adversaries to hypersonic technology exists at deeper levels than are typically visible" by the Defense Department and prime contractors. The report noted that the average exposure to Chinese suppliers in tiers 3 to 5 of the supply chain, where visibility of component origin is decreased, reached 11 percent, and indicated that contractors



iStock photo

likely share suppliers at lower levels of their chain, thereby increasing the risk of foreign influence.

Undersecretary of Defense for Acquisition and Sustainment Ellen Lord recently highlighted the Pentagon's challenges, stating, "Our biggest sustainment concerns with hypersonics are ensuring that subcomponents have a resilient supply chain with secure microelectronic components and that the … military services have a strategy for spares and repairables that provide sufficient annual quantities to ensure predictability for suppliers and readiness for the warfighter."

To address these vulnerabilities, the Defense Department has rewritten acquisition policies to focus on "creative compliance," including providing the Adaptive Acquisition Framework to deliver technology more quickly and help acquisition professionals design strategies to minimize risk. It has implemented rules restricting the use of some Chinese equipment and is increasing cybersecurity requirements. Pending legislation incentivizes companies to source materials domestically.

On the foreign investment side, CFIUS has long scrutinized foreign acquisitions of U.S. companies that present national security concerns. In February 2020, new regulations expanded the committee's authority to cover noncontrolling transactions involving foreign investors. Parties are now required to submit a declaration to CFIUS for review of a transaction if the U.S. business must obtain a U.S. regulatory authorization to export its critical technology to the foreign party involved in the transaction.

In 2018, the Department of Commerce identified hypersonics as a category of emerging technology subject to export controls. Emerging technology also serves as part of the definition of critical technologies for CFIUS purposes.

Additionally, CFIUS regulatory changes in October require companies to file mandatory declarations in certain cases if a foreign investor could acquire control of a U.S. business that produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies for which a U.S. regulatory authorization would be required for export.

As a result, foreign investment in companies working with hypersonic technology could be subject to mandatory CFIUS declarations. U.S. companies involved in hypersonic-related technology must be proactive about mitigating potential concerns. Manufacturers and suppliers should seek counsel to conduct proper due diligence and CFIUS analysis ahead of any potential foreign investment transactions, especially those involving Chinese or Russian investment.

Similarly, foreign investors in such companies should conduct sufficient due diligence, including confirming export control classifications, to determine whether their target companies are creating or using critical technologies.

Even if a mandatory declaration is not required for components throughout the supply chain, due to the heightened national security concerns around protecting hypersonic technology, impacted companies and investors should consider filing a notice with CFIUS to obtain a safe harbor ruling that it does not object to the transaction.

Parties choosing not to file for review remain vulnerable to future unilateral review, as there is no limit on when the committee can review a transaction. Obtaining a safe harbor ensures that the committee will not later review the filing and impose penalties, force the foreign party to divest from the U.S. business, or require the parties to adhere to conditions mitigating specific national security concerns.

One of the few topics that both Democrats and Republicans agree on is an urgent need to stop the flow of critical technologies to adversarial foreign powers and any diminishing role of U.S. military global technological superiority.

Although the term national security is undefined in CFIUS and related legislation, and evolves to address a changing threat environment, U.S. policymakers from both parties have been very clear that executive and legislative efforts must remain focused on stopping and eliminating foreign party access to emerging technology and technical data.

Thus, the incoming Biden administration likely will maintain the same policy stance on addressing national security supply chain vulnerabilities as well as CFIUS investigations and enforcement. In addition, we may see even more regulatory controls monitoring supply chains to ensure that foreign component products cannot affect the supply chain of emerging technologies and other defense and military items.

These regulatory controls may require additional due diligence of the supply chains for military and defense items and their components. Companies should monitor these issues and ensure that product development, supply system management and regulatory lawyers work together to plan a strategy to account for these challenges.

Due to disruptions caused by the COVID-19 pandemic, trade conflicts and growing U.S. national security restrictions, companies involved in emerging technologies should examine whether vulnerabilities exist within their supply chains, and, if so, what alternatives may be available. Companies should also perform thorough due diligence on all foreign investment to best understand CFIUS risk.

This due diligence should include screening processes to identify foreign beneficial ownership or investors, and classification reviews of the technology or product to determine whether the company's technology is considered an emerging technology, is export controlled, and/or requires an export license.

Be sure that counsel can identify any national security implications, conduct export classification reviews, raise alternative supply chain opportunities, explore applicable exemptions and craft deal documents to position the company to successfully complete transactions while facing CFIUS and other national security obligations. Developing the due diligence processes to fully identify supply chain vulnerabilities, technology classification and foreign investment risks can be time-consuming, but would go a long way toward mitigating supply chain and CFIUS risk. **ND**

**Abbey Baker is counsel, Christian Contardo an associate and Doreen Edelman chair of the law office of Lowenstein Sandler's global trade and policy practice.**

**Viewpoint** BY SHAWN FETTEROLF AND IRENE LAU

# Nation Should Invest in Electronics Critical Infrastructure

The National Defense Industrial Association's relatively new Electronics Division has a clear interest in the CHIPS for America Act and the American Foundries Act, which are currently before Congress.

The division has been closely following the proposed legislation, and recently hosted a webinar on this topic with staff from Capitol Hill. As a division, we felt it was important to improve members' understanding and visibility into these activities.

Since the inception of the industry in the 1960s, electronics technology has remained strategic for the Defense Department and has become an increasingly important part of the domestic economy.

In fact, the government helped to create new technologies and dominated the early market with the Very High Speed Integrated Circuits program.

The primary goal at the start of the VHSIC program was to reduce the time lag from the introduction of a microelectronic technology into the commercial market until the technology was first applied in deterrent and warfighting systems.

Today, however, commercial demand dominates the market by a large margin, with defense electronics being less than 1 percent, but remaining essential to national security.

To initially ensure access, in 1990 the government invested in its own fabrication line at the National Security Agency. As commercial adoption of electronics skyrocketed and technology refreshes became more complex and expensive, the government needed to change its approach. Starting in 2003, the Trusted Foundry program was initiated to ensure continued access to commercially available technologies, ultimately leading to a network of certified trusted suppliers.

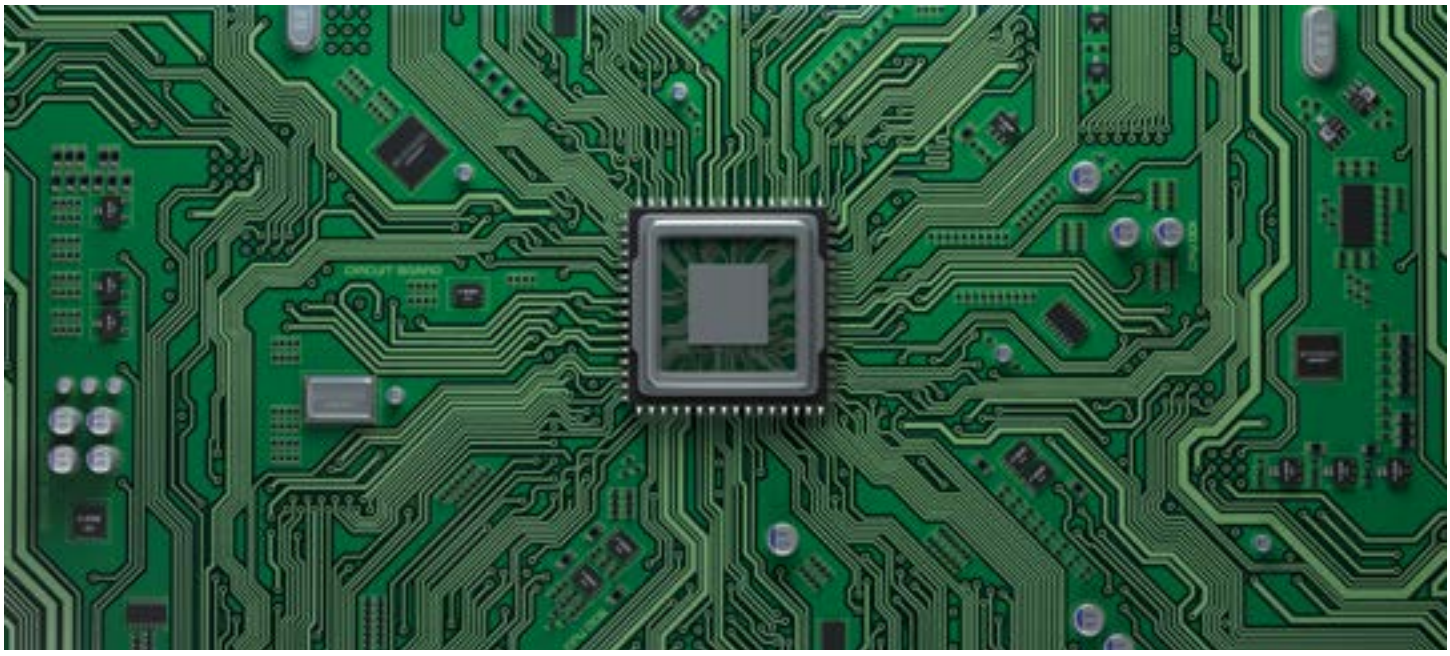
However, industry changes and challenges have led to a question: how can government and industry guarantee and secure a microelectronics supply chain able to meet critical national needs, across all technologies, and at pace? This is particularly important in today's globalized environment, with aggressive adversarial investments in technology leadership — both in fabrication and application.

The microelectronics supply chain is complicated, and includes many steps such as fabrication, testing and packaging. In parallel, industry seeks to adopt emerging technologies like heterogeneously integrated packaging to differentiate their offerings and capabilities.

Continued offshoring of these capabilities has exposed gaps and limitations within the defense industrial base. Events impacting the supply chain such as the coronavirus pandemic have further highlighted some detrimental impacts of offshoring. Further, there is a need to develop the workforce to support these technologies domestically.

As some domestic leading-edge technology companies have adopted a "fabless" model focusing on design and architectural innovation, the knowledge base required to innovate in manufacturing is not always available at the levels required. Additionally, hiring efforts can be hindered by clearances and U.S. citizenship requirements.

Design and architectural innovation also have limitations as



iStock photo

the workforce required for exquisite, custom designed parts is similarly limited. This has led to the commercial design intellectual property and services markets of today.

Today's advanced custom designs often utilize high percentages of commercially available design IP and services in order to accelerate the time to market. Similarly, another path to mitigate these issues is through the use of programmable hardware such as field programmable gate arrays. This is a technology prevalent in government platforms, also requiring a highly skilled, yet sometimes unavailable, workforce.

For both of these approaches, there is a tight coupling between manufacturing and design. This allows for optimization of a platform given the available technology options, impacting gate arrays and custom designed solutions as well as the design IP used in both. Therefore, system differentiating technologies rely upon manufacturing and architecture optimization regardless of platform.

Government systems typically incorporate both commercial off the shelf, as well as custom components to achieve system goals. This enables a balance between affordability and capabilities as well as potential accelerated adoption of "lead-ahead" technologies. Accomplishing this requires investment to transition lead-ahead technologies to industry and government, and to have the workforce to implement those technologies in or near the facilities architecting and manufacturing them.

Considering security of production and the supply chain, physical location may provide a level of inherent trust or assurance. However, mission critical functions also require system level security to address vulnerabilities.

As vulnerabilities span software and hardware, mitigations must ensure adequate protection of mission critical functionality. As a result, security requirements vary by platform, and based on intended mission criticality must consider: confidentiality to ensure bad actors are not able to accelerate compromising mission critical functions; integrity to ensure mission functionality achieves only what was intended; and availability to protect component supply in times of geopolitical unrest, natural disaster or pandemic.

There should be a national strategy for achieving guaranteed secure access to microelectronics components. In this globalized industry, it is unrealistic to expect an entirely domestic supply chain for every interesting technology given that volume sales are required for scale in manufacturing.

However, we need to reverse the trend of offshoring critical capabilities and start to rebuild those where we no longer have domestic capacity.

The current pandemic has laid bare that relying on fragile supply chains is unwise, and several actions are needed.

First, the industry needs incentives to re-shore key elements of the supply chain.

There should also be public-private partnerships to share risks and accelerate availability. And partnerships with allies are required to ensure uninterrupted, secure supply chains.

An advisory council — including government, academia and industry — focusing on how to support new technologies and their transition to commercial markets is also required. This council should develop a strategic long-term plan across mission critical needs and domestically available technology nodes, as well as forecast needed capacity for legacy to state-of-the-art technologies. This needs to occur concurrently with obsolescence and sustainment strategies.

An accurate, objective, accessible and supported end-to-end risk framework is also needed. The council should establish, maintain and evolve such a framework and include: a comprehensive attack surface risk assessment; an accurate mitigation versus risks analysis method; and a method to identify additional mitigation requirements for acceptance.

Advanced node technologies are an important subset of need. However, newer nodes may not accommodate needed specialized processes or technologies. Such investment across the full spectrum of technologies — emerging, state-of-the-art, state-of-the-practice and legacy — is critical to accommodate diverse national needs.

This requires reforms in acquisition and sustainment focusing on security and modernization. Rather than locking in today's technology for decades, refreshing capabilities more frequently needs to be enabled.

This includes simplifying acquisition practices and establishing public-private partnerships to accelerate access to critical technologies. Innovation in commercial markets is driven by commercial companies unwilling to tolerate current government acquisition processes or restrictions. Reducing this burden will provide more direct access to innovative solutions.

To enable modernization, procurement methods should aggregate demand across the entire government enterprise rather than program by program. Procurement methods must also adapt to commercial business practices and include long-term technology and capacity forecasting. This will better align government programs with commercial technology shifts, enabling early insight and faster adoption of technology advancements.

To secure the supply chain and guarantee access, clearly defined "tiers of trust" need to be established to guide program security requirements.

Further, government programs need to be better aligned with critical industries including infrastructure, artificial intelligence and consumer electronics.

Through such alignment, opportunities of scale can be realized for industry and government using common approaches to security. These tiers must be consistent with protection levels relevant to system end use in order to optimize adoption. Commercial industry will balance security against production costs to optimize the market.

Together, initiatives like the CHIPS for America Act and the American Foundries Act must support world class domestic commercial technology. They must balance cost, quality and a secure supply chain, to extend domestic advantage and secure the electronics supply chain as critical infrastructure. ND

**Irene Lau is chair and Shawn Fetterolf vice chair of NDIA's Electronics Division. NDIA committee and division leaders Mike Fritze, Nikhil Shenoy, Ezra Hall and Jim Will also contributed to this article.**