

BACKGROUNDER

No. 3598 | APRIL 1, 2021 CENTER FOR NATIONAL DEFENSE

Understanding and Protecting Vital U.S. Defense Supply Chains

Maiya Clark

KEY TAKEAWAYS

In an armed conflict, robust and resilient defense supply chains are vital to sustaining American forces and ensuring the U.S. can successfully engage its enemies.

Supply chains for the U.S. defense sector are not as secure as they should be, with many businesses moving supply chains overseas, sometimes to unfriendly countries.

Congress and the Administration must work together to secure U.S. defense supply chains and ensure they are ready to protect and serve the nation's interests. he United States has entered a new era of great-power competition with China. As the country makes this shift, policymakers are forced to reevaluate some lingering assumptions that drove defense policy during the Cold War, the country's last period of sustained great-power competition. The competition with the Soviet Union was a competition between two spheres that rarely overlapped: The United States had very little commerce with the Soviet Union, and the global economy was essentially divided into East and West, with much more trade within each sphere than between the two.

The competition we face with China today is very different. In the globalized economy, the United States and China are deeply invested in each other's economies and highly interdependent as a result. The U.S. defense sector is no exception to this, as large

This paper, in its entirety, can be found at http://report.heritage.org/bg3598

The Heritage Foundation | 214 Massachusetts Avenue, NE | Washington, DC 20002 | (202) 546-4400 | heritage.org

Nothing written here is to be construed as necessarily reflecting the views of The Heritage Foundation or as an attempt to aid or hinder the passage of any bill before Congress.

multinational defense contractors and their suppliers seek to drive down costs by moving their supply chains overseas, sometimes to countries with whom the United States shares no special security arrangements.

Dependence on Overseas Suppliers. Two notable occurrences highlighted the risk that results from dependence on overseas suppliers. First, when former President Donald Trump banned Turkey from participation in the F-35 Joint Strike Fighter program due to Turkey's military ties to Russia, the Department of Defense (DOD) quickly realized that the F-35 program was dependent on single-source suppliers located in Turkey.¹ As a result, F-35 components must still be purchased from Turkey until 2022—despite security concerns. Had the DOD completely stopped buying from Turkey in December 2020 as planned, it would have cost the F-35 program \$1 billion.²

The COVID-19 pandemic also highlighted risks of foreign dependency. During government-mandated shutdowns, some countries (such as Mexico) did not permit defense-related companies to continue producing items necessary to U.S. defense programs.³ They did not consider factory workers "essential" as did the U.S. Many countries turned inward to focus on their own needs during this global emergency.

The resulting delays to U.S. defense programs reminded policymakers that overseas supply chains create risks that may not be tolerable in a defense context. In an armed conflict, materiel is used and must be replaced: Munitions are consumed, ships and fighter jets are damaged, and uniforms and boots wear out. Robust and resilient supply chains for these items and their hundreds of thousands of constituent parts are required to win wars.

Based on these concerns, policymakers have in turn accelerated their efforts to better secure defense supply chains.

"Re-Shoring" Defense Production. Proposals in Congress to "re-shore" defense production were a prominent part of negotiations for the Fiscal Year (FY) 2021 National Defense Authorization Act (NDAA). There were proposals both for industry-specific measures (such as requiring that certain ship components be purchased from the National Technology and Industrial Base—a group consisting of Australia, Canada, the U.K., and the U.S.) and sweeping new Buy American requirements, like the NDAA amendment proposed by Congressman Donald Norcross (D–NJ).⁴ The Norcross Amendment, had it been incorporated into law (which, ultimately, it was not) would have required, by the end of FY 2021, a 25 percent increase in the percentage of components for major weapons programs that must be manufactured in the United States (from the current 50 percent to 75 percent), followed by a further 5 percent increase each year—until reaching 100 percent U.S.-manufactured components by FY 2026.⁵

While offered with the best of intentions, none of these proposed policies attack the root causes of the issue. Many industry-specific measures are proposed in a piecemeal fashion that fails to recognize that the problems of individual sectors are part of a larger issue of vulnerable defense supply chains. Meanwhile, more sweeping proposals, like the Norcross Amendment, are overly broad and could be perceived as protectionist in nature.

Nor is foreign production the only vulnerability in defense supply chains. The report resulting from former President Trump's Executive Order 13806, entitled "Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States,"⁶ found other weaknesses in defense supply chains: single and sole-source suppliers of defense products, eroding U.S.based infrastructure, fragile businesses and markets, and gaps in domestic human capital.⁷ A particular defense supply chain may contain only one of these vulnerabilities, but it most likely suffers from a combination.

Now President Biden is continuing the efforts of Executive Order 13806 with his own "Executive Order on America's Supply Chains," which calls for additional studies of defense supply chains.⁸ Congress has also taken up the issue and aims to complement these efforts with a new "Defense Critical Supply Chain Task Force."⁹ The bipartisan task force, established by the House Armed Services Committee, aims to focus on issues of foreign dependency.¹⁰

A Comprehensive Approach

Responding to one defense supply chain vulnerability but not others will be ineffective. The United States therefore needs a comprehensive approach toward securing its defense supply chains.

Three elements are necessary to strengthen defense supply chains:

- 1. Greater visibility into defense supply chains;
- 2. A system for objectively assessing and rating supply chain strength, risks, and issues; and
- 3. An understanding and a method for selecting the policy tools best suited to address the particular supply chain vulnerability(s).

Visibility: How Well Does Government Understand Defense Supply Chains?

In order to address defense supply chain vulnerabilities, policymakers and defense officials must first have a clear view of them. This requires supply chain visibility: the ability of the customer (the DOD in this case) and the prime contractor to clearly "see" into the lowest tiers of the supply chain. This involves a full understanding of the supply chain; for example, in the case of the Army's Stryker armored combat vehicle, from the vehicle itself, to the bottom tiers, to the companies making the bolt that connects the alternator assembly to the engine powering the Stryker.

Does this information currently exist? If so, where is it? Can it be found in a central place? After all, the DOD—as well as the services that fall within it—is the main contracting agency procuring the items whose supply chains are of direct concern and require protection. One would expect the Department of Defense, as the customer, to possess centralized supply chain information.

But this is not the case. In addition to the Office of the Secretary of Defense, each of the services, and program offices within the services, typically hold limited degrees of information on the defense supply chains that support their materiel programs. This information is not centrally maintained.

Program Offices. As the organization with the predominant responsibility to ensure effective defense systems are delivered to the warfighter, one might expect DOD program offices to maintain detailed visibility into the supply chains of their programs. However, most services and program offices do not have anything approaching complete information on their programs' supply chains.

This is because program offices in the Department of Defense, as a whole, have moved away from supply chain management. Collecting and monitoring supply chain information is a time- and cost-intensive undertaking, and—under pressure to save time and money—it appeared to be a function that the government did not need to perform.

Instead, supply chain management is a responsibility normally included in the government's contracts with prime contractors; in the government's eyes, prime contractors are responsible for ensuring the resilience and knowledge of the supply chain of the end product.¹¹ See, for example, the Army's recent Request for Proposals (RFP)¹² for the Optionally Manned Fighting Vehicle Program: It includes a clause requiring the prime contractor to report to the program office any "unresolved risks and issues" to the program, following a specific template.¹³ Further DOD guidance indicates that supply chain–related issues would fall under the "risk" category.¹⁴ Program offices might get information from prime contractors on supply chain issues that reach the threshold of an unresolved or unresolvable risk to the program—but would otherwise have no real indication of the health of the supply chain. Program offices are therefore currently not the best primary source for detailed defense supply chain information.

Prime Contractors. The prime contractor is ultimately responsible for the product it sells to the government. For their own sakes, prime contractors take special care to ensure they have reliable suppliers and subcontractors. However, defense products are often highly complex, with many tiers of subcontractors involved in making components of the final product. As a result, a prime contractor may know who builds the cooling system for its submarine, but it does not necessarily know who makes the wiring that makes the component that makes the subsystem that is part of the cooling system for the submarine.

Therefore, while prime contractors are expected to manage their supply chains and are responsible to the contracting government agency if a supply chain issue causes a delay or system failure, prime contractors often follow the government's example and include supply chain management in their contracts with their first-tier subcontractors. Those subcontractors follow suit in their contracts with second-tier subcontractors, and so on down the chain. As a result, prime contractors usually only understand their supply chains down through the first few tiers; beyond that, they trust their subcontractors to manage their subcontractors, and so on.

DOD Assessments Directorate. The DOD does not rely solely on program offices for information on supply chains. While industrial base issues declined in importance in the early 2000s, by 2011 (with the resurgence of Russia and the rise of China), department leadership and Congress slowly came to rediscover the importance of resilient supply chains, and responded by creating the Office of Manufacturing and Industrial Base Policy in the FY 2011 NDAA.¹⁵ Now called the Office of Industrial Policy, the office performs multiple functions to support the defense industrial base, and falls under the umbrella of the Under Secretary of Defense for Acquisition and Sustainment. The FY 2021 NDAA further recognized the importance of emerging industrial base issues by elevating the head of that office to an assistant-secretary-level position requiring Senate confirmation—the Assistant Secretary of Defense for Industrial Base Policy.¹⁶ The Assessments Directorate, underneath the Office of Industrial Policy, has the main responsibility to monitor and evaluate defense supply chains. The Assessments Directorate is organized by sector (such as aircraft, missiles and munitions, and electronics), not by program, and a technical expert leads each sector. These technical experts often have years of experience working in their particular sectors, understand the industry, and have extensive professional networks in the field.

The Assessments Directorate endeavors to do what one might expect: assess the health of the industrial base for specific sectors and monitor vulnerabilities. It communicates its findings to Congress and the public each year through the annual Industrial Capabilities Report to Congress. The most recent report, for FY 2020, is 181 pages long and includes a COVID-19 response highlight, a defense industry outlook, assessments of each sector, assessments of the industrial base for critical emerging technologies, and a summary of supporting policy authorities.¹⁷

Visibility Gaps Remain. However, even the Assessments Directorate does not maintain comprehensive and continuous visibility into defense supply chains. Its methods are more diagnostic and rely on data collected in the course of its technical experts' research and the research of other entities within the DOD. Thus, while defense supply chain data exist, those data are limited and not centrally managed or stored. The Department of Defense has very limited supply chain visibility, which hinders its efforts to measure those supply chains' fragility or to respond in ways to strengthen supply chains.

Two issues inhibit the DOD's efforts to improve supply chain visibility.

- Companies do not want to share any more information than is required about their suppliers. Such information is proprietary and, in some cases, its continued secrecy provides a company a competitive advantage. Voluntary efforts by the DOD to collect supplier data usually leave large holes, as companies can simply refuse to participate. This occurred in the Trump Administration's efforts to complete its Executive Order 13806 report. While that order produced an informative report, it did not rest on comprehensive knowledge about defense supply chains. Indeed, previous voluntary efforts to collect such data from the defense industry resulted in only a 50 percent response rate.¹⁸
- The President can, if he chooses, use the Defense Production Act (DPA)¹⁹ to compel companies to share relevant supplier information, and the Obama Administration attempted to do just that in its

Sector-by-Sector, Tier-by-Tier (S2T2) industrial base assessment effort in 2014.²⁰ However, merely collecting and processing that data required a lot of time and resources, and while it gave a more complete picture of defense supply chains, that picture was just a snapshot in time. As suppliers and supplier relationships changed (as they do almost every day), the results of the S2T2 effort quickly became obsolete.

These two issues—the cost of collecting supply chain data and the challenge of accurately capturing business relationships that are constantly changing—add to the problem of companies' hesitation to share proprietary data, making supply chain visibility a continuing challenge for the DOD. These same issues are likely to plague President Biden's efforts to improve defense supply chain visibility with the reporting required in his latest "Executive Order on America's Supply Chains."

However, technological advances may provide a solution to some of these issues. Digital tools are available to manage incredibly large data sets securely and in real time. There are a wide variety of tools to create secure modes of communication between the DOD, contractors, and subcontractors. For example, blockchain technology, which underpins Bitcoin and other cryptocurrencies, is now being applied in many other sectors, such as health care data storage and supply chain management.

While current applications of blockchain to supply chain management are limited in scale (especially compared to the scale of the DOD's supply chains), this technology could provide a way to securely store and organize these data.²¹ It would also make the data easily updatable, which would reduce costs and solve the obsolescence issue. However, an application of blockchain in the defense realm would probably require a centralized network of computers, rather than a network of decentralized servers as are used in the case of Bitcoin. It is unclear how this would impact the other potential benefits of blockchain. Blockchain is just one example of digital technologies that can be leveraged to map and monitor defense supply chains.

And once this massive database is created and maintained, artificial intelligence (AI) could be applied to process supply chain data, to identify patterns, and to generate a response. AI could be used to detect supply chain weaknesses, for example, by screening data to find single- and sole-source suppliers. Or it could be used to process country-of-origin data for components and determine whether those components meet domestic-sourcing requirements. AI is another technology that makes perfect supply chain visibility more possible than it ever has been before.

Supply chain visibility is a huge hurdle the Department of Defense must overcome in order to accurately and continuously gauge the health of the defense industrial base and, ultimately, better secure the country's supply of defense items. Currently, there is little concerted effort within the DOD to obtain and maintain this information. But without this information, it will be impossible to accurately determine supply chain fragility or make policy that addresses these fragilities. Fortunately, emerging digital solutions for data-sharing and management mean that obtaining supply chain visibility is more feasible than ever before.

Determining and Comparing Supply Chain Fragility

Collecting data to create supply chain visibility is both crucial and challenging. However, it is only the first piece of the problem. Once those data are collected, they need to be analyzed to determine the health of the supply chain, to compare the health and security of different suppliers and supply chains and, ultimately, to triage and prioritize areas of highest risk for action.

Defense supply chain analysis should capture variables in three categories:

- 1. The item's relative importance to national security;
- 2. The health of the industry and organizations that produce the item (which includes producing the item at the required capacity/rate and whether the supplier is a single/sole source); and
- 3. The place where the item is produced—domestically, abroad in an allied or friendly country, or abroad in a competitor or potential competitor state.

With this information for supply chains across different sectors or programs in hand, policymakers could compare the urgency of supply chain vulnerabilities and make informed choices about policy choices and solutions, including the best use of limited funds allocated to support U.S. defense industrial base needs.

Fragility and Criticality. The Department of Defense—specifically the Assessments Directorate—currently uses a methodology that captures these variables, called "fragility and criticality." Fragility and criticality essentially correspond to probability and consequence, a common framework used to

evaluate risk, in which "probability" refers to the likelihood of an event, and "consequence" describes the event's possible impact level.²² But in the case of fragility and criticality, the assessment factors are tailored to industrial base risks.

Fragility describes the likelihood of disruption. It is measured at both the micro and macro levels. On the micro, provider/individual business level, fragility is determined using the metrics of the company's financial outlook, as well as the breakdown of its business between government and the private sector (a company that relies solely on the DOD for business is considered more fragile than a company with significant commercial, as well as government, business). Fragility is also measured at the macro, market level: The metrics used here are the number of firms in a given sector and the level of dependence on foreign suppliers in that sector. These metrics together capture both the economic health of businesses and sectors producing defense items, and the location of production—either domestically or overseas.

Criticality measures how difficult it would be to recover from disruption in a certain industry. There are six metrics for criticality:

- 1. Facility and equipment requirements,
- 2. Skilled labor requirements,
- 3. Defense design requirements,
- 4. Defense uniqueness,
- 5. Reconstitution time, and
- 6. Availability of alternatives.

Navy shipbuilding, for example, requires complex and specific facilities; highly skilled labor, of which there is a shortage; intricate defense designs; and defense-unique end products (meaning there is no commercially available alternative). These variables help to capture the health of the sectors producing defense items.

Significantly, the fragility-and-criticality methodology is currently used to assess the health of particular defense sectors and subsectors, rather than production capacity for individual items or components in defense supply chains. However, if more granular supply chain data were available,

TABLE 1

The Fragility and Criticality Methodology

FRAGILITY		CRITICALITY
Micro Forces	Macro Forces	
Company's financial outlook	 Number of firms in a given sector Foreign dependency 	 Facility and equipment requirements Skilled labor requirements
• Breakdown of business between government and commercial		 Defense design requirements Defense uniqueness
		Reconstitution timeAvailability of alternatives

SOURCE: U.S. Department of Defense, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, "Annual Industrial Capabilities Report to Congress for 2014," p. 9, September 2016, https://www.businessdefense.gov/Portals/51/Documents/Resources/2014%20AIC%20RTC%2010-03-16%20-%20Public%20Unclassified.pdf (accessed March 8, 2021).

BG3598 Theritage.org

the methodology could be adapted to measure fragility and criticality at that greater level of detail. As mentioned earlier, AI could be leveraged to process supply chain data in order to help assess the fragility and criticality of particular items.

Importance to National Security. The fragility-and-criticality methodology, however, does not provide a measure of an item's importance to national security. In theory, all defense items are important to national security; the government made that determination when it chose to buy the item or the weapons system that requires the item as a component. However, some items are more important than others: A component of the F-35 jet fighter ought to rank above the laces for Army boots, for example.

While the Assessments Directorate may not be able to determine which items are of greatest importance to the national defense, senior leadership can. Senior leadership in the DOD would make these determinations based on the National Security Strategy and the National Defense Strategy currently in place, while also giving consideration to current events and demands placed on the armed forces. Thus, while this prioritization does not fit into the fragility-and-criticality methodology, it must be a factor in determining where to intervene to protect defense supply chains. With that aside, the fragility-and-criticality methodology essentially captures the necessary variables to evaluate and compare supply chains' health and relative need for intervention. Its usefulness depends on the quantity and quality of supply chain data obtained through visibility efforts previously discussed.

Policy Tools to Strengthen Defense Supply Chains: Are They Enough?

Once supply chains are visible, have been evaluated, and are assessed to require some sort of mitigation, policy tools can be applied to remedy shortfalls. Some already exist and others are yet to be implemented. These tools typically fall into two categories: incentives and restrictions.

Defense Production Act. Title III of the Defense Production Act allows the President of the United States to promote the defense industrial base with tailored economic incentives, often grants. Specifically, it grants authority to the President to "create, maintain, protect, expand, or restore domestic industrial base capabilities" using funds allocated specifically for that purpose.²³ These authorities have been used to incentivize businesses to enter the defense space or to expand their capabilities, and have served to create domestic production capabilities for items typically procured from overseas and to strengthen the fragile domestic supply base. Examples include organic light-emitting diode displays; small, unmanned aircraft systems (drones); and mobile communications receivers.²⁴

However, DPA Title III funding is typically limited, with an annual appropriation averaging \$62.4 million per year, a tiny drop of water in the sea of the defense budget. (Though it is important to note that in FY 2020, the fund received an additional \$1 billion to help respond to the COVID-19 pandemic.)²⁵ Title III is an effective response to supply chain vulnerabilities that require a surgically precise solution, but at its current level of funding, it can only cover so many projects per year. In an era in which dependence on Chinese products cuts across nearly every sector, Title III grants will not be sufficient to secure our defense supply chains.

Industrial Base Analysis and Sustainment. Similar to DPA Title III, the Industrial Base Analysis and Sustainment (IBAS) program sets aside funds to strengthen the domestic defense industrial base. The program was created in 2013 and is notably being used for efforts to develop a domestic rare-earths industry. It faces the similar issue of having a limited pool of funds—roughly \$10 million to \$30 million per year, though with an increase to over \$50 million in FY 2019, and \$104 million in FY 2020—and has a list

of many projects that could use those funds.²⁶ IBAS can help address specific supply chain vulnerabilities, but, like Title III, it can only resolve so many issues at its current level of funding.

Trusted Capital Marketplace. The Trusted Capital Marketplace was created in 2019 by the Trump Administration to foster connections between vetted venture capital firms and non-traditional defense contractors.²⁷ Unlike Title III and IBAS, which rely on the distribution of government funds, Trusted Capital Marketplace connects defense-related technology companies, particularly start-ups, with funding in the private sector.

The goal is to foster domestic innovation in defense technologies, while also ensuring that investment in those technologies comes from trustworthy sources rather than, for example, Chinese-backed venture capital funds.²⁸ In the context of supply chain concerns, this keeps these start-ups future defense suppliers—as American companies, backed with American capital, and it accomplishes this through fostering relationships, rather than through restrictive government mandates or government spending.

Tax Incentives. Federal and state tax incentives exist to promote domestic defense manufacturing. Some of these are targeted to specific industries, like those passed into law in the FY 2021 NDAA. Title XCIX of the NDAA, which was based on proposed legislation entitled The Creating Helpful Incentives to Produce Semiconductors (CHIPS) Act, creates new incentives, including grant programs and tax credits, to boost semiconductor manufacturing capacity in the United States.²⁹

Defense industry manufacturing also benefits, or has the potential to benefit, from broader tax incentives to encourage domestic manufacturing. For example, the Domestic Production Activities Deduction, in effect from 2004 until 2017, gave a tax deduction to domestic manufacturers and certain other domestic business activities.³⁰ States have many such incentives to encourage businesses to set up within their state lines, though the decentralization of such incentives mean they are less relevant to defense policymakers at the national level.³¹

Targeted incentives, like those enacted to boost domestic semiconductor manufacturing, are the most useful in protecting defense supply chains, as these can be enacted to directly respond to areas of greatest vulnerability.

Multiyear Procurement and Block Buy Contracting. To support supply chains from the sector level, rather than more targeted interventions for individual items, multiyear procurement (MYP) and block buy contracting (BBC) can be appropriate and money-saving tools. In traditional annual defense contracting, the DOD uses a separate contract (or multiple contracts) for each year's procurement of a given kind of item. This gives the DOD and Congress the flexibility to change the quantity of the item to be procured. But that same flexibility creates uncertainty that can wreak havoc on supply chains for the item—as the prime contractor and all tiers of its supply chain have to adjust their production schedules and planned capital investments each year based on the DOD's or Congress's changed plans.

MYP and BBC can bypass some of this uncertainty by allowing the DOD to use a single contract for two or more years' worth of procurement of a given kind of item. There are restrictions on the use of these types of contracts, including a requirement for congressional approval for each use.³² When the prime contractor has the certainty of a contract extending multiple years into the future, it can operate more efficiently, as can all tiers of its supply chain.

Sourcing Restrictions: Buy American Act and Others. There are multiple legal requirements that require the Department of Defense to buy domestically produced items. The Buy American Act of 1933 is the chief domestic sourcing restriction currently impacting U.S. defense acquisition.³³ It requires that all end products purchased by the U.S. government be manufactured domestically and be made "substantially" of domestic parts, which is interpreted to mean at least 50 percent of the end product's components must be U.S.-made, subject to certain exceptions.³⁴

The Buy American Act was a protectionist response to the Great Depression, meant to preserve American jobs during a time of high unemployment; it was not designed with securing defense supply chains in mind.³⁵ Today, however, these restrictions play a role in preserving defense industries that might otherwise have followed their commercial counterparts overseas.

Other domestic sourcing restrictions include the Berry Amendment, which requires some categories of items purchased by the DOD to be 100 percent domestic in origin.³⁶ Domestic sourcing restrictions are sometimes included as amendments in the National Defense Authorization Act; for example, the FY 2021 NDAA includes a requirement that certain satellite components be purchased from countries in the National Technology and Industrial Base (e.g., Australia, Canada, the U.K., and the U.S.).³⁷

One of the shortcomings in this approach is that these domestic procurement restrictions can be provoked by a congressional delegation seeking to protect a certain company—not as a result of a deliberate approach to protect defense supply chains. Another is that there is a cost, sometimes significant, for systems to incorporate components from a new source. There are design, testing, and qualification activities required to ensure the systems still perform as required. These costs are not accounted for in Pentagon program budgets. **Restriction: Prohibitions on Specific Foreign Sourcing.** Beyond requirements that certain items be sourced in part or in whole from domestic producers, there are more specific prohibitions on DOD acquisitions. These are sometimes the result of congressional legislation and sometimes the product of DOD-created regulations. But whatever their source, they are recorded in the Federal Acquisition Regulation (FAR) and the Defense FAR Supplement. For example, FAR § 52.204 prohibits federal government acquisition of Chinese telecommunications equipment or services; DFARS § 225.770 bans U.S. government purchases of certain items from Communist Chinese military companies; and DFARS § 225.771 prohibits DOD contracting or subcontracting with firms owned or controlled by governments that are state sponsors of terrorism.³⁸ These prohibitions provide a more targeted regulation to protect defense supply chains from reliance on competitor states.

Restrictions on Foreign Investment: The Committee on Foreign Investment in the United States. The Committee on Foreign Investment in the United States (CFIUS) reviews foreign investment in U.S. companies and real estate in order to ensure those transactions do not pose a risk to national security.³⁹ The interagency committee was created by President Gerald Ford in 1975, and its authorities were expanded with the Foreign Investment Risk Review Modernization Act of 2018.⁴⁰ These authorities prevent foreign companies from acquiring key defense-related technologies or firms that make defense components—all of which is designed to solve supply chain problems before they start.

The Merits of the Available Policy Tools

These incentives and restrictions serve different purposes: Title III and IBAS use government funds to directly stimulate key defense industries; the Trusted Capital Marketplace and CFIUS ensure that defense-related technologies remain in the United States, and not in the hands of U.S. adversaries; and the Buy American Act and other domestic content restrictions endeavor to keep government business in domestic defense industries. This combination of targeted investment, protection from adversarial foreign capital, and maintenance of the domestic defense industry, taken together, do a lot to ensure the security of our defense supply chains.

However, there are gaps in the current policy tools, involving areas of concern that these tools do not adequately address. This is unsurprising, as the tools that exist today were created in different eras to address different defense industry issues and other economic concerns. A consensus must be reached in the defense community on our degree of comfort with overseas supply chains in allied, partner, and competitor countries. Once that consensus is achieved that, for example, an item supplied from Belgium, Canada, France, or India is an acceptable risk, but an item primarily supplied by China is not, the U.S. needs to have the nuanced policy tools to allow the first scenario while prohibiting the second. A blunt tool, such as sweeping Buy American rules, causes a degree of disruption to the defense industrial base—and economic harm to our allies—that outweighs the benefits to our supply chain security, while specific prohibitions, like a ban on Chinese telecommunications equipment, are time-consuming and inflexible.

It is important to note that other countries, allies and competitors alike, incentivize their domestic industries with subsidies via direct government investment, tax breaks, loan programs, and other avenues. China is an obvious example of this: Its Made in China 2025 plan calls for large government subsidies and other incentives to meet higher targets for domestic manufacturing in strategic sectors like robotics and power equipment.⁴¹ These measures are not mentioned as a model the United States should follow. Rather, it is important that policymakers understand the global economic context in which U.S. defense supply chains operate.

The current policy tools listed and potential future policy tools described are only as effective as the supply chain data and assessments used to direct these tools' use. Without greater supply chain visibility and better assessments of supply chain strength, the use of these authorities will be scattered and less effective. With this in mind, the following recommendations are offered for consideration.

Recommendations

Congress should:

• Form a bipartisan expert commission charged to develop policy designed to create a system to maintain defense supply chain visibility; evaluate and compare supply chain strength; and properly address supply chain vulnerabilities. The issues surrounding defense supply chains are incredibly complex and have not been discussed in one conversation. And while the new Defense Critical Supply Chain Task Force will doubtless be helpful in initiating that conversation, a commission comprised of experts in defense acquisition and supply chain management must complement this effort in order to guide more comprehensive, effective solutions to defense supply chain vulnerabilities.

The commission's first order of business should be to create a plan for increasing the DOD's supply chain visibility. In doing this, the commission should explore potential applications of data management technology to defense supply chain information management. Some of the key issues with collecting defense supply chain data—namely, the expense and the rapid obsolescence of the data—could potentially be resolved with blockchain technology or other digital data management solutions. Their use in defense supply chain visibility should be explored.

• **Increase DPA Title III funding** and focus investments to the most fragile and critical areas. A limited pool of funds constrains the number of targeted interventions that can be made to support defense supply chains. Title III funding should increase, and its use should be focused on sectors found to be most vulnerable using the fragility-and-criticality framework.

The executive branch should take the following actions:

- The DOD should use the current tools at its disposal to increase supply chain visibility. In order to address threats to defense supply chains, the DOD must have visibility into those supply chains. And while current tools and resources would not allow for total supply chain visibility into every tier of every defense program's supply chain, there are things the DOD can do now to get a better sense of the challenges such an effort would face. The Office of Industrial Policy should initiate a pilot project with a program of its choosing—perhaps the Army's Joint Light Tactical Vehicle, the Navy's Virginia-class submarine, or the Air Force's MQ-9 Reaper drone—aiming to achieve full supply chain visibility for that program within a certain timeline. This would provide valuable insights for broader efforts toward defense supply chain visibility across the Department of Defense.
- The DOD should use the fragility-and-criticality framework as one of the tools to determine defense supply chain priorities. Congress should also base its legislation on the DOD's comprehensive findings. The Department of Defense already has a framework of criteria to evaluate the health of, and risk to, defense supply chains. The executive branch and Congress should have this framework in mind when legislating or making policy about defense supply chains.

The President should create a policy authority in which the DOD can make and enforce determinations on countries of origin for specific defense suppliers. The Department of Defense needs a precise tool that allows them to make case-by-case determinations on the acceptability of security risks inherent in overseas supply chains for defense products. Domestic content restrictions such as the Buy American Act are tools too blunt to address such a nuanced issue, when one product might be supplied by multiple allied and partner countries, but another might be concentrated in one foreign country or even in an adversarial foreign country. If certain industries or specific supply sources should be re-shored, there should be a policy tool to make this doable and enforceable, without forcing lower-risk supply chains to re-shore as well.

Conclusion

Defense supply chains involve networks of extremely diverse firms, belonging to a variety of sectors, which provide millions of components to eventually produce defense items. As a country, we need to better appreciate the vast scope of our defense supply networks, the range and seriousness of the threats these supply chains face, and the new tools government will need to mitigate these threats—without exceeding its proper role in our free-market democracy. Congress and the executive branch must work together to secure our defense supply chains.

Maiya Clark is Research Assistant in the Center for National Defense, of the Kathryn and Shelby Cullom Davis Institute for National Security and Foreign Policy, at The Heritage Foundation.

Endnotes

- Specifically, Turkey's procurement of the Russian S-400 air defense system—which is incompatible with NATO systems and would threaten the secrecy of the F-35's stealth technology—led the U.S. to suspend Turkey from the F-35 program. For more information, see "Turkey: Background and U.S. Relations," Congressional Research Service *Report for Congress*, November 9, 2020, p. 27, https://crsreports.congress.gov/product/pdf/R/R41368 # Toc55812485 (accessed March 9, 2021).
- 2. Richard Sisk, "U.S. to Keep Buying F-35 Parts from Turkey, Despite Purchase Ban," October 1, 2020, https://www.military.com/daily-news/2020/10/01 /us-keep-buying-f-35-parts-turkey-despite-purchase-ban.html (accessed March 9, 2021).
- Joe Gould, "COVID Closed Mexican Factories That Supply U.S. Defense Industry. The Pentagon Wants Them Opened," *Defense News*, April 21, 2020, https://www.defensenews.com/2020/04/21/covid-closed-mexican-factories-that-supply-us-defense-industry-the-pentagon-wants-them-opened/ (accessed March 9, 2021).
- 4. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, Title VIII, § 823, H.R. 6395, 117th Cong., 1st Sess., https://rules .house.gov/sites/democrats.rules.house.gov/files/BILLS-116HR6395-RCP116-57.pdf (accessed March 9, 2021).
- 5. Carrie Healey, "Norcross Ensures Enhanced 'Buy American' Provisions in NDAA," U.S. House of Representatives, July 2, 2020, https://norcross.house .gov/media-center/press-releases/rcross-ensures-enhanced-buy-american-provisions-ndaa (accessed March 9, 2021).
- Donald Trump, "Presidential Executive Order on Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency in the United States," July 21, 2017, https://trumpwhitehouse.archives.gov/presidential-actions/presidential-executive-order-assessing -strengthening-manufacturing-defense-industrial-base-supply-chain-resiliency-united-states/ (accessed March 9, 2021).
- For more on defense supply chain vulnerabilities, see U.S. Department of Defense, Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States, Interagency Task Force in Fulfillment of Executive Order 13806, https://media .defense.gov/2018/Oct/05/2002048904/-1/-1/1/ASSESSING-AND-STRENGTHENING-THE-MANUFACTURING-AND%20DEFENSE-INDUSTRIAL-BASE -AND-SUPPLY-CHAIN-RESILIENCY.PDF (accessed March 9, 2021).
- 8. Joseph Biden, "Executive Order on America's Supply Chains," February 24, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions /2021/02/24/executive-order-on-americas-supply-chains/ (accessed March 11, 2021).
- 9. News release, "House Armed Services Committee Stands Up Acquisition Task Force," Armed Services Committee, U.S. House of Representatives, March 4, 2021, https://armedservices.house.gov/2021/3/house-armed-services-committee-stands-up-acquisition-task-force (accessed March 11, 2021).
- Justin Doubleday, "After 'Searing' COVID Shortfalls, House Lawmakers Eye Foreign Dependencies in Defense Supply Chain," *Inside Defense*, March 10, 2021, https://insidedefense.com/daily-news/after-searing-covid-shortfalls-house-lawmakers-eye-foreign-dependencies-defense-supply (accessed March 11, 2021).
- 11. Remarks by Christine Michienzi, Chief Technology Officer, Office of Industrial Policy, U.S. Department of Defense at George Mason University's Center for Government Contracting and Defense Acquisition University Conference: "Government Contracting in a Changed World," October 6, 2020, https:// business.gmu.edu/govcon/events/conference/ (accessed March 9, 2021).
- 12. The RFP is essentially a draft of the eventual program contract.
- 13. U.S. Department of the Army, "Request for Proposals (W56HZV-20-R-0142): Optionally Manned Fighting Vehicle," p. 21, § C.7.2.1, https://beta.sam.gov /api/prod/opps/v3/opportunities/resources/files/461e0175dbb744eaa360c5c95d5e8ff4/download?api_key=null&token= (accessed March 9, 2021).
- 14. U.S. Department of Defense, *Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisitions*, Office of the Deputy Assistant Secretary of Defense for Systems Engineering, January 2017, pp. 15–16, https://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue -and-Opportunity-Management-Guide-Jan-2017.pdf (accessed March 9, 2021).
- 15. Public Law No. 111–383, Title VIII, § 896, https://www.govinfo.gov/content/pkg/PLAW-111publ383/pdf/PLAW-111publ383.pdf (accessed March 9, 2021).
- 16. National Defense Authorization Act for Fiscal Year 2021, Title IX, § 903.
- 17. U.S. Department of Defense, *Fiscal Year 2020: Industrial Capabilities: Report to Congress*, January 2021, https://www.businessdefense.gov/Portals/51 /USA002573-20%20ICR_2020_Web.pdf?ver=o3D76uGwxcg0n0Yxvd5k-Q%3d%3d (accessed March 9, 2021).
- 18. Marjorie Censer, "Pentagon Official: New Defense Industrial Base Review 'Won't Just Be a One-Time Exercise," *Inside Defense*, January 22, 2018, https://insidedefense.com/daily-news/pentagon-official-new-defense-industrial-base-review-wont-just-be-one-time-exercise (accessed March 9, 2021).
- 19. Defense Production Act of 1950, Public Law No. 81-774.
- 20. Author conversations with Andrew Hunter, Director, Defense-Industrial Initiatives Group and Senior Fellow, International Security Program, Center for Strategic and International Studies, and John G. McGinn, Executive Director, Center for Government Contracting, George Mason University.
- 21. Knut Alicke, "Blockchain Technology for Supply Chains—A Must or a Maybe?" McKinsey & Company, September 12, 2017, https://www.mckinsey.com /business-functions/operations/our-insights/blockchain-technology-for-supply-chainsa-must-or-a-maybe (accessed March 9, 2021).

- U.S. Department of Defense, Annual Industrial Capabilities Report to Congress for 2014, September 2016, p. 9, https://www.businessdefense.gov /Portals/51/Documents/Resources/2014%20AIC%20RTC%2010-03-16%20-%20Public%20Unclassified.pdf?ver=2017-04-18-072624-770 (accessed March 9, 2021).
- 23. U.S. Department of Defense, "Defense Production Act Title III: Overview," Office of the Under Secretary of Defense for Acquisition and Sustainment, https://www.businessdefense.gov/DPA-Title-III/Overview/ (accessed March 9, 2021).
- 24. White House, "How President Trump Uses the Defense Production Act to Protect America from the China Virus," Office of Trade and Manufacturing Policy, August 2020, p. 17.
- "The Defense Production Act of 1950: History, Authorities, and Considerations for Congress," Congressional Research Service *Report for Congress*, updated March 2, 2020, https://crsreports.congress.gov/product/pdf/R/R43767 (accessed March 9, 2020), and CARES Act, H.R. 748, 116th Cong., 2nd Sess., p. 240, https://www.congress.gov/116/bills/hr748/BILLS-116hr748enr.pdf (accessed March 9, 2021).
- 26. U.S. Department of Homeland Security, *Final Report: Economic Security Subcommittee*, Advisory Council, November 2020, p. 17, https://www.dhs.gov/sites/default/files/publications/final_economic_security_subcommittee_report_1.pdf (accessed March 9, 2021), and U.S. Department of Defense, *Department of Defense Fiscal Year (FY) 2021 Budget Estimates*, February 2020, https://comptroller.defense.gov/Portals/45/Documents/defbudget /fy2021/budget_justification/pdfs/03_RDT_and_E/RDTE_Vol3_OSD_RDTE_PB21_Justification_Book.pdf (accessed March 9, 2021).
- 27. Maiya Clark, "How Pentagon's 'Trusted Capital' Program Can Secure Financing for Defense Industrial Base," Heritage Foundation *Commentary*, November 27, 2019, https://www.heritage.org/defense/commentary/how-pentagons-trusted-capital-program-can-secure-financing-defense -industrial.
- 28. U.S. Department of Homeland Security, *Final Report: Economic Security Subcommittee*, Advisory Council, November 2020, p. 17–18, https://www.dhs .gov/sites/default/files/publications/final_economic_security_subcommittee_report_1.pdf (accessed March 9, 2021).
- 29. National Defense Authorization Act for FY 2021, Title XCIX.
- 30. Public Law No. 115–97, § 13305(a), repealed § 199, https://irc.bloombergtax.com/public/uscode/doc/irc/section_199 (accessed March 9, 2021).
- 31. Kevin Potter, "Credits & Incentives Talk with Deloitte, Credits and Incentives for the Aerospace and Defense Industry," Deloitte, November/December 2016, https://www2.deloitte.com/us/en/pages/tax/articles/credits-and-incentives-for-the-aerospace-and-defense-industry.html (accessed March 9, 2021).
- 32. "Multiyear Procurement (MYP) and Block Buy Contracting in Defense Acquisition: Background and Issues for Congress," Congressional Research Service *Report for Congress*, December 22, 2020, https://fas.org/sgp/crs/natsec/R41909.pdf (accessed March 9, 2021).
- 33. Buy American Act of 1933, Public Law No. 72-428.
- 34. Kate M. Manuel et al., "Domestic Content Restrictions: The Buy American Act and Complementary Provisions of Federal Law," Congressional Research Service *Report for Congress*, https://fas.org/sgp/crs/misc/R43354.pdf (accessed March 9, 2021). The Buy American Act should not be confused with Buy America laws, which govern domestic content restrictions for the construction of state and municipal transportation systems and are usually not relevant in the defense acquisition context.
- 35. U.S. Government Accountability Office, *Buying American Act, Actions Needed to Improve Exception and Waiver Reporting and Selected Agency Guidance*, GAO–19–17, December 2018, p. 3, https://www.gao.gov/assets/700/696086.pdf (accessed March 9, 2021).
- 36. "Defense Primer: The Berry and Kissell Amendments," Congressional Research Service *Report for Congress*, January 13, 2021, https://crsreports .congress.gov/product/pdf/IF/IF10609 (accessed March 9, 2021).
- 37. "National Defense Authorization Act for Fiscal Year 2021," Title XCIX, § 1603, and "Defense Primer: The National Technology and Industrial Base," Congressional Research Service *Report for Congress*, updated February 2, 2021, https://fas.org/sgp/crs/natsec/IF11311.pdf (accessed March 9, 2021).
- Federal Regulations Acquisitions System, "52.204–25: Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment," https://www.acquisition.gov/far/52.204-25 (accessed March 9, 2021), and Defense Federal Regulations Acquisitions System, "Subpart 225.7: Prohibited Sources," https://www.acq.osd.mil/dpap/dars/dfars/html/current/225_7.htm (accessed March 9, 2021).
- 39. U.S. Department of the Treasury, "The Committee on Foreign Investment in the United States (CFIUS)," https://home.treasury.gov/policy-issues /international/the-committee-on-foreign-investment-in-the-united-states-cfius (accessed March 9, 2021).
- 40. "The Committee on Foreign Investment in the United States (CFIUS)," Congressional Research Service *Report for Congress*, February 14, 2020, p. 1, https://fas.org/sgp/crs/natsec/RL33388.pdf (accessed March 9, 2021).
- 41. U.S. Department of Defense, *Military and Security Developments Involving the People's Republic of China 2020*, Office of the Secretary of Defense, p. 15, https://media.defense.gov/2020/Sep/01/2002488689/-1/-1/1/2020-DOD-CHINA-MILITARY-POWER-REPORT-FINAL.PDF (accessed March 9, 2021).