

April 2021

A DPA for the 21st Century

Securing America's AI National Security
Innovation Base

CSET Policy Brief



AUTHOR
James E. Baker

Preamble

Some commentators say the field of artificial intelligence is ungovernable. It covers many fields and capabilities, they note, and involves a breadth of private and academic actors, many working in secrecy to protect intellectual property and profit potentials. But it is an overstatement to call AI ungovernable. Several existing laws and executive orders give various agencies and elected officials tools to regulate the national security development of AI, as does the Constitution. Policymakers should become familiar with these tools, examine their strengths and shortcomings, and become involved in efforts to modify and improve the AI governance architecture. As with other “ungovernable” areas, like nonproliferation, where there are also myriad actors and challenges, we can design an effective governance architecture if we are purposeful about doing so. This paper considers one of the most important potential tools in this effort, the Defense Production Act (DPA); however, it would be a more effective tool if updated and used to its full effect.

AI development depends on hardware, data, talent, algorithms, and computational capacity.¹ Thus, any law that can (1) help ensure an adequate supply of these assets and in appropriate form; and (2) prioritize the use of these assets to achieve national security policy objectives is an important national security tool. That is not to say the DPA’s full authority should be used at this time. Extraordinary tools, such as the DPA’s allocation authority, might more appropriately be used at a moment of emergency, for example, in time of conflict or should another nation achieve an AI breakout creating decisive security advantage. Thus, at this time, the most important function a debate about the use of the DPA for AI purposes can serve is to shape and condition expectations and understandings about the role such authorities should, or could, play, as well as to identify essential legislative gaps so that we do not learn of these gaps (and are not hesitant to use the authority we have) when the authority is needed. However, in less dramatic manner, the DPA’s other authorities might well be used, or more fully used at this time to shore up America’s AI supply line, as illustrated with the examples below.

While obscure to the public, the DPA got a burst of national attention in early 2020 when the coronavirus pandemic began overwhelming U.S. hospitals, first in New York City and then elsewhere. In the absence of federal leadership, in March 2020 national security specialists familiar with the DPA urged its full use to mobilize the nation's capacity to provide medical equipment and personal protective equipment (PPE) to address COVID-19. In April 2020, as the spreading virus was depleting national supplies of ventilators and PPE for health workers, President Donald Trump generated headlines by invoking the DPA, ostensibly to compel businesses to manufacture such equipment. A second order authorized the Secretary of Health and Human Services and the Director of the Federal Emergency Management Agency to "use any and all authority available" under the DPA to acquire N95 respirator masks from 3M. By mid-July, however, CNN noted that "the Trump administration has made only sparing use of its authorities [under DPA], leaving front-line workers in dire need of supplies like masks, gowns and gloves."² The Trump Administration did eventually use the DPA during the second half of 2020 to prioritize contracts (eighteen times to channel raw materials to the manufacture of vaccines and therapeutics) and to incentivize the production of medical supplies like testing swabs; however, the DPA was never used to full effect, nor in a strategic and transparent manner.

In contrast, as a candidate for the White House, President Biden promised full use of the DPA to put the United States on a "war time" footing to meet COVID supply chain challenges. Since assuming office, the Biden Administration has used the DPA, and other laws, to address bottlenecks in the supply chain for components needed for vaccine manufacture and to prioritize supply contracts to allow Merck to assist in making Johnson & Johnson vaccines. In addition, the Biden Administration has used Title III financing authorities to incentivize the building of factories and supply lines for COVID tests and rubber plants for medical gloves.

What is significant here, is not just that the Biden Administration used the DPA to provide vaccine capacity to plug supply chain

gaps, it did so after the president-elect and then president conditioned industry for its use in this manner and directed the federal government to lean into the law. It also made “friendly” use of the DPA, identifying needs in consultation and partnership with industry, with a focus on the result rather than the means. These are lessons worth noting in the AI context going forward. With COVID, as with AI, the legal policy question is not whether and how to use the DPA to accomplish a task but how to use the full range of available law effectively, purposefully to meet the nation’s needs, and in a manner consistent with our values. With COVID, it turned out, the DPA was one of several laws that could be used to harness America’s industrial capacity to address the pandemic.

The government’s handling of the pandemic is a topic for another day. The point here is that the mere mention of the DPA’s potential clout reinforced the view, in some people’s eyes at least, that the law is a vehicle to “nationalize” industry, a “commandeering” authority, which empowers the government to take over and run the nation’s defense industries. This fed into an already existing narrative about government regulation and opposition from the Chamber of Commerce.

In fact, as this paper shows, the DPA contains many different authorities, some narrow and others potentially broad in scope. It is important for policymakers to understand that the DPA is not limited to military equipment and actions, and its powers are not solely addressed to, or limited to, “commandeering.” Rather, the law establishes a national mobilization capacity to bring the industrial might of the U.S. to bear on broader national security challenges, including technology challenges and public health challenges. Thus, the DPA is both a potential macro tool and a micro tool. Its application to artificial intelligence can be substantial.

Table of Contents

Preamble	1
The Defense Production Act	5
Title I: Prioritization and Allocation Authority	6
Title III: Production Incentives	8
Title VII: Tools to Build and Secure the National Security Innovation Base	9
Executive Order 13603	12
DPA Boundaries and Safeguards	15
Issues	17
1. Does the DPA Require Companies to Accept New Government Contracts?	17
2. Academia	18
3. Talent	19
4. Authority to Inquire and Survey—Industrial Base Assessments ...	20
5. The Scope of the DPA’s Allocation Authority	22
6. Liability	23
7. Does the DPA Provide “Notwithstanding” Authority?	24
8. Voluntary Agreements and Plans of Action	24
9. Federal Acquisition Regulations and Practice	26
10. Pricing	27
11. Transparency	27
12. Litigation	27
Conclusion	30
Acknowledgments	32
Reading List	33
Endnotes	34

The Defense Production Act

The DPA is a Cold War era statute (1950) that derives in turn from World War II era statutes intended to harness the industrial capacity of the United States for war. It is the principal executive authority to “shape defense preparedness programs and to take appropriate steps to maintain and enhance the domestic industrial base.” It was drafted with steel and tanks in mind. Yet it has been reauthorized over 50 times since 1950 and amended to include within its reach, not just the traditional defense industrial base, but also the nation’s critical infrastructures, like public health and critical technologies, as well as what is now referred to as the National Security Innovation Base. Bottom line: The DPA has broad scope and applies to the constellation of technologies known as AI.

The Act includes authority to prioritize existing government contracts, allocate resources, incentivize the manufacture of materials and products, and survey industry to determine which entities are producing, or can produce, needed materials, services, and goods. These authorities might be useful in a technological “arms race” involving emerging technologies. For example, the survey authority would be significant if key items are largely or exclusively produced overseas and the government needed to identify U.S. companies capable of producing the same goods, like extreme ultraviolet scanners, computer chips, and labeled data.

The DPA comes with an existing bureaucracy to enable its work — the Defense Priorities and Acquisitions System and Committee and Federal Priorities and Acquisitions System (FPAS). Thus, the DPA is well known to defense contractors and FEMA first responders, who rely on the DPA to prioritize contracts for disaster response in the case of FEMA, or to incentivize the production of defense articles for which there is not a generalized market, in the case of DOD. However, policymakers and lawyers new to the law may not be aware of its potential to reach across the government and may feel uncomfortable with its potential legal reach. The statute is written in places with extraordinary Cold War breadth, contributing to its reputation as a “commandeering” authority. When President George H.W. Bush signed the DPA’s reauthorization into law in

1992 he cautioned that “in peacetime” at least one of its provisions (Section 705 providing for industry assessments) “would intrude inappropriately in the lives of Americans who own and work in the Nation’s businesses.”³ As noted, this survey provision would be most relevant in the event key supplies are manufactured overseas and the government needs to identify new U.S. sources of supply. Title III, in turn, with its production incentives, including guaranteed purchasing authority, could then be used to generate a U.S. capacity. Consider, for example, the manufacture of lithographic equipment used to etch patterns on the film on top of the silicon wafers, which are part of the semiconductor chips that enable computer memory, communication, and computation. As the National Security Commission on AI has noted, a Dutch company is the only company in the world that produces Extreme Ultraviolet (EUV) lithographic scanners. Title III thus could be used to incentivize the establishment of a domestic manufacturing capability and to guarantee purchase of a market-appropriate number of scanners.

Since its enactment, the DPA has included a five-year sunset clause for most, but not all, of its provisions. The law’s 53 reauthorizations underscore the realistic opportunity to amend or adjust the DPA to address AI applications or ambiguities. Policymakers should do so in a purposeful manner, thinking forward to 21st century technologies like AI, rather than backward to Cold War era industrial needs and authorities.

The DPA originally had seven titles. Four have been repealed. Titles I, III, and VII still apply.

Title I: Prioritization and Allocation Authority

Title I authorizes the president to prioritize contracts and allocate materials, services, and facilities to promote the national defense.

“The President is authorized (1) to require that performance under contracts or orders (other than contracts of employment), which he deems necessary or appropriate to promote the national defense, shall take priority over performance under any other contract or order, and for the purpose of assuring such priority, to require

acceptance and performance of such contracts or orders by any persons he finds to be capable of their performance, and (2) to allocate materials, services, and facilities in such manner, upon such conditions, and to such extent as he shall deem necessary or appropriate to promote national defense.” (Emphasis added.).

Section (b) of Section 101 further provides that allocation authority “shall not be used to control the general distribution of any material in the civilian market unless the president finds” (1) that the material is a scarce and critical material essential to national defense; and (2) the requirements for national defense cannot otherwise be met. Section (b) is a limitation on the president’s authority. Both Presidents Trump and Biden made these determinations regarding resources needed to combat COVID. Sections 101(a) and (b) illustrate the DPA’s potential breadth. Consider the potential AI uses here. With companies increasingly turning to product specific chips, the government might prioritize the production and allocation of generic chip capacity to ensure an adequate national security supply. The government might also prioritize access to cloud computing resources generally, or in times of crisis, for government-generated needs. Section 101(c) provides distinct prioritization and allocation authority “in order to maximize domestic energy supplies.” This section, in contrast to the national defense authority in subsection (a), requires three presidential findings antecedent to its use. While this section of the law was used, as contemplated, to direct energy sales during the “California Energy Crisis” (2000-2001), one can imagine emergent scenarios where the government might need to ensure the availability and routing of energy supplies to server farms or for computational capacity, and might look to DPA authority to do so.

Application of Title I of the DPA involves five layers of law and regulation: The Constitution, the DPA, executive order, implementing regulations, and departmental and agency internal regulations. The system is implemented using the Defense Priorities and Allocations System (DPAS). In general, DPAS is administered by the Department of Commerce’s Bureau of Industry and Security. However, the president and Commerce have delegated many of the DPAS’ authorities to other agencies,

including DOD. Of course, the president's own direction takes legal precedence over agency direction.

Most commentary on the DPA is addressed to Title I's prioritization and allocation authority. This is true of the Annual DPAC Report to Congress as well. This makes sense. Title I is a frequently used provision of the DPA, including over 300,000 uses per year by DOD alone. It is also the authority most likely to be used in an emergency, for example, by FEMA during a hurricane. And, depending on whether and how the allocation authority is invoked, it is an area of potential dispute and litigation.

Title III: Production Incentives

Title III authorizes the provision of incentives through loan guarantees (Section 301), direct loans (302), purchase commitments and purchases (303(a)), and subsidy payments (303(c)) to provide industrial capacity in support of national defense and homeland security. The Title III program provides “the President broad authority to ensure the timely availability of essential domestic industrial resources to support national defense and homeland security requirements, through the use of highly tailored economic incentives.” Invocation of the program requires the President to make seven determinations, including: that the resource or technology is essential for national defense; that “industry cannot or will not provide needed capacity in a reasonable time without DPA Title III assistance;” and “Title III incentives are the most cost-effective, expedient, and practical alternative for meeting the need.” As noted earlier, this Title is an obvious tool to generate U.S. manufactured circuit foundry capacity reducing reliance on foreign suppliers of chips in Taiwan and South Korea, and single points of failure, like the EUV scanners produced in the Netherlands. Less obvious perhaps, would be the use of Title III to guarantee the purchase of distinct, labeled data for particularized Intelligence Community or DOD machine learning applications.

The law prohibits the President from delegating these determinations. The program is typically overseen by the Deputy Assistant Secretary of Defense for Industrial Base Policy, reporting

to the Under Secretary of Defense for Acquisition & Sustainment. The DOD executive agent for the program is the Air Force, specifically, the Title III Office at Wright-Patterson AFB. There were 28 publicly listed Title III projects in 2017, covering subjects such as thermal, solar, and lithium batteries; nanotechnology; and rocket motors. Considering the breadth of U.S. national security needs in the AI/Title III area one might well contemplate a greater National Security Council or Office of Science and Technology Policy presence in the Title III decision-making process.

Title VII: Tools to Build and Secure the National Security Innovation Base

Title VII of the DPA includes several provisions addressing operation of the law. Section 702 provides definitions of key terms. Section 706 grants federal district courts jurisdiction over civil and criminal proceedings for violations of the act or its regulations. The courts are empowered to enjoin or enforce provisions of the DPA. This provision reflects Congress' anticipation that use of the DPA might necessitate a judicial forum for dispute resolution as well as enforcement mechanism. However, in practice, outside of the CFIUS area, there is a surprising lack of litigation, with most of the lead substantive cases dating to the 1950s, following passage of the Act and initial efforts to implement its provisions.

Title VII also provides additional authorities to study, shape, and influence the defense industrial base. Section 722 provides the statutory underpinning of the Defense Industrial Base (DIB) system, which, in turn, is the statutory foundation for the DPAS, the Defense Production Act Committee (DPAC), and the DIB information system. With AI, three authorities might prove especially important.

Section 705 authorizes the government to conduct industry assessments, including if necessary, subpoena authority to access covered facilities and records. The person furnishing the information, or the president, may direct that information and data obtained in this manner receive "confidential treatment," unless the president determines that withholding the information is "contrary

to the interest of national defense.” This section has obvious application as the government considers where and how to increase computational capacity, store data, create data sets, and design algorithms. The Bureau of Industry and Security has not published an industrial base assessment of United States AI since 1994.

Section 710 of the Act could be used to address what the National Security Commission on Artificial Intelligence (NSCAI) refers to as “the human talent deficit,” described by the Commission as “the government’s most conspicuous AI deficit and the single greatest inhibitor to buying, building, and fielding of AI-enabled technologies for national security purposes.” This section authorizes the president to “employ persons of outstanding experience and ability without compensation” to “carry out the provisions of this chapter,” as well as to establish, train, and sustain a National Defense Executive Reserve (NDER). The NDER was active in the 1950s as a Cold War entity; however, it fell into disuse in subsequent decades. The Obama Administration re-established the NDER but with little apparent impact. Section 710 is an underutilized authority to attract talent to government service without a full-time commitment or the necessity for market-competitive salaries. Title I in turn might be used to prioritize and incentivize the creation of AI services such as academic programs to educate and train AI talent.

Title VII, Section 721, also serves as the statutory enabling authority for the Committee on Foreign Investment in the United States (CFIUS). President Ford established the committee in 1975 by executive order, and it was given statutory authority in 2007. The committee is the principal executive vehicle for regulating foreign control and investment in the United States that could impair national security. The committee is formally comprised of nine cabinet members and designated members of the president’s national security staff. However, in practice, the committee is run by staff, usually at the assistant secretary level, and includes formal and informal members, advisors, and as-needed agency representation. The Director of National Intelligence is required to

provide either a general threat assessment, or a thorough analysis of any threat, about each covered transaction.

Pursuant to Title VII, as amended by the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), the committee is required to review “any merger, acquisition, or takeover that is proposed or pending after August 23, 1988, by or with any foreign person that could result in foreign control of any United States business, including such a merger, acquisition, or takeover carried out through a joint venture.” Companies may affirmatively seek review by filing a notice with the committee and thus mitigate the risk of unilateral CFIUS review after a transaction is underway. The law requires CFIUS to safeguard confidential information provided by businesses during the review process. It also sets firm deadlines, measured in days, for government decisions and actions, so that companies are not adrift in bureaucratic limbo and can, if necessary, seek court review. During the period 2008-2015, the committee received on average 116 notices of transactions per year, with a high of 147 in 2014 and a low of 65 in 2009.⁴ During this same period, the committee conducted 333 investigations, with a high of 66 in 2015 and a low of 23 in 2008. The annual reports do not indicate the number or nature of mitigation steps taken in each case or generally; however, the reports indicate that 42 notices were withdrawn following notice and 62 during investigation. Since 1990, the president has blocked six transactions outright, all of which involved Chinese firms or investors in some manner. Most cases involved the acquisition of semiconductor or communications firms of obvious national security concern at the time, and now of AI interest as well.

FIRRMA expanded CFIUS jurisdiction to expressly include real estate transactions, critical infrastructure, critical technologies, and businesses that maintain or collect sensitive personnel data of U.S. citizens. It is too early to tell how the expanded authority of FIRRMA will change CFIUS practice, although an increase in use and litigation is likely. Moreover, CFIUS review is one area where policymakers will want to ensure AI policy is aligned with AI practice and appropriate AI expertise assigned to the Committee, considering not just matters of AI software and hardware but also

access and control of data and services like cloud storage and computing.

Executive Order 13603

Over the years, presidents have issued executive orders affecting the Defense Production Act. E.O. 13603 is particularly noteworthy.

The order, titled “National Defense Resources Preparedness,” was issued by President Obama on March 16, 2012. It delegates authority and addresses defense resource policies and programs under the DPA. (This is the most recent presidential executive order directed to the DIB, which remains in force as of early 2021.)

The order delegates the President’s authorities under Section 101(a) of DPA Title I to six cabinet secretaries with respect to six specific areas. However, exercise of this delegated authority “may be used only to support programs that have been determined in writing as necessary or appropriate to promote the national defense” as determined by the secretaries of Defense, Energy, and Homeland Security. Specifically:

“ . . . the authority delegated by Section 202 of this order may be used only to support programs that have been determined in writing as necessary or appropriate to promote the national defense:

- by the Secretary of Defense with respect to military production and construction, military assistance to foreign nations, military use of civil transportation, stockpiles managed by the Department of Defense, space, and directly related activities;
- by the Secretary of Energy with respect to energy production and construction, distribution, and use, and directly related activities; and
- by the Secretary of Homeland Security with respect to all other national defense programs, including civil defense and continuity of government.”

The Department of Commerce has delegated authority to four agencies to place priority-rated contracts and orders: Defense, Energy, DHS, and GSA. The Department of Commerce and these agencies can also place priority contracts for the use of other agencies. While the Department of Defense is the primary user of the system (applying the “critical to national defense” DO rating to about 300,000 contracts per year), the authority is used episodically by a range of agencies, and by DHS on a regular basis.

The government’s response to COVID illustrates the breadth and potential range of this authority. It is also illustrated with reference to the 2011 DPAC report showing how the authority has been used to address prior disasters and emergencies.

The “priorities authority has been used to support, for example, hurricane and flood preparedness and response activities; Homeland Security Technology Programs; emergency preparedness activities related to the 2009 H1N1 flu virus; the Greater New Orleans Hurricane and Storm Damage Risk Reduction System program (by the U.S. Army Corps of Engineers); the International Safeguards, Second Line of Defense, and Nuclear Counterterrorism Incident Response programs (by DOE’s National Nuclear Security Administration); the Geostationary Operational Environmental Satellite, R-Series Program (DOD’s NOAA); and the Terrorist Screening Center program (DOJ/FBI).”

DHS/FEMA guidance and reporting indicates that DHS primarily uses rated orders to ensure on-time performance of contracts and to address supply chain problems.

The Department of Defense uses two DPAS industrial priority ratings—DX and DO. As noted above, DO is used for orders “critical to national defense” and requires the approval of the Under Secretary of Defense for Acquisition & Sustainment. DX-rated orders are used for orders of the “highest national defense urgency” and must be approved by the Secretary or Deputy Secretary of Defense. DX-rated orders have equal priority and take precedence over DO orders. Likewise, DO orders have equal priority and take precedence over regular commercial contracts.

Where the statutory elements are otherwise met, DPA Title I authority may be invoked for foreign contracts and for the benefit of foreign nations. This was the case, for example, with the 2003 decision to provide DX prioritization to the supply of Precision Lightweight GPS Receivers to British military forces in Iraq. In addition, DPA Title I authority includes pass-through authority. If the prime contractor receives a DX-rated order, it can, in turn, require priority treatment from subcontractors working on the same-rated order.

Policy oversight is ordinarily provided by the DPAC, and its subordinate interagency working groups, although FEMA and the Department of Health and Human Services (HHS) have played a central role during the COVID-19 pandemic as have the Biden Administration COVID Coordinators. Much of the DPAC's work is conducted at the working group level on either an interagency basis or an as-needed agency basis. Under Section 722(b) of the DPA, the DPAC advises the president on the effective use of DPA authorities in support of national defense. Seventeen departments and agencies are members of the DPAC, which is chaired by the director of the Federal Emergency Management Agency (FEMA). Since 2011, the DPAC has issued an annual report on "government contingency planning for events that might require the use of the priorities and allocations authorities," which "provides recommendations for effective use of priorities and allocation authorities, and provides recommendations for improving information-sharing among federal departments and agencies relating to the use of priorities and allocations authorities."⁵ The report is currently submitted under the FEMA administrator's signature, as delegated by the secretary of DHS.

One COVID takeaway is that process should be tailored to need, and that good process leads to better results. It is hard to legislate good process, which depends on personality and leadership as well as structure. But with AI, the DPAC and FPAS may be places to start, supplemented by representation from key AI agencies and entities like National Institute for Standards and Technology, OSTP, and the NSC Directorate for National Security and Emerging Technology. Likewise, existing governmental structures such as

those emanating from E.O. 13859 “Maintaining American Leadership in Artificial Intelligence” (February 11, 2019) and succeeding executive orders should include legal and DPAC knowledge and representation.

DPA Boundaries and Safeguards

From the outset, commentators have recognized that the DPA provides the executive branch with broad authority to regulate portions of the economy in a manner potentially in tension with traditional free market principles. Early on, they wrote about the sanctity of contract. And as we have noted, the DPA has been referred to as a “commandeering” authority. The DPA does provide broad authority; but it is also a tailored mobilization tool. It can be used to prioritize contracts or potentially allocate the entirety of a scarce and essential resource. Its virtue as a national security tool in the AI field may be found in the authority to determine what is occurring in industry and academia, as well as to incentivize Title III research and production capacity where there are single points of failure or unwise reliance on foreign supply chains.

The DPA has several statutory and other protections against its overuse or abuse. These include:

1. As with the PATRIOT Act, certain DPA provisions expire if not reauthorized by Congress (generally every five years). Thus, wage and price control authority expired in 1953. The law is next up for reauthorization in 2025.
2. In any event, nothing in the DPA requires companies to accept contracts at other than fair market value; however, the parameters for setting fair market value in the context of emergencies is opaque and the experience with COVID suggests the need for deliberate inquiry, post-COVID, to determine whether legislative or regulatory boundaries are prudent to protect all sides of the DPA equation going forward.
3. The DPA provides for federal court jurisdiction arising under the Act to include enforcement authority, as well as

injunctive power, allowing businesses to seek expedited federal court review, and, if appropriate, injunctions against government overreach.

4. Some DPA provisions are non-delegable, so only the President can trigger them.
5. The Act requires an annual report from the Defense Production Act Committee, which heretofore has been timely and detailed, largely reporting on DOD use of the law. However, as discussed below, Congress should consider a requirement for further transparency and reporting in the case of pandemics and other emergency uses of the DPA.
6. Finally, as noted, information obtained under Section 705 of the Act, providing for industry surveys and assessments, receives confidential treatment, if requested or designated by the President (or his delegee), as do classified information or programs. Moreover, as a matter of regulatory practice, the government deems all survey information confidential.

Issues

The federal government's handling (and mishandling) of the coronavirus pandemic helped spotlight gaps and ambiguities in the DPA and its application. If the DPA is to play a purposeful role in government regulation and oversight of AI, it is important for policymakers to address these ambiguities and shortcomings (and others certain to arise). It is equally important that policymakers, in consultation with industry and academia, set expectations and understandings about how the law might be used. In doing so, they should address twelve issues.

1. Does the DPA Require Companies to Accept New Government Contracts?

Section 101 of the DPA clearly requires companies to prioritize existing contracts or contracts within existing programs. However, the law is less clear on whether the government can require companies to accept new contracts or new contracts for products the company does not ordinarily make, or in the language of the Commerce regulations, “for an item not supplied or for a service not performed.” [15 C.F.R. §700.13(c)(2) (2020).] One can parse the language found in Section 101 either way. Section 101(a)(1) requires “performance under contracts and orders.” The use of the word “under” implies the presence of an existing contract or order. However, language later in the section seems “to require acceptance and performance of such contracts and orders,” which, depending on how the word “under” is read, could mean either any new order or only those under existing contracts.

Government regulations implementing this section can be read either way as well. On the one hand, they state that companies are required to accept new contracts. On the other hand, they seem to exempt contracts for products “not supplied.” Government statements such as those found on the FEMA and DHS DPA websites seem to take the view that companies are required to accept new contracts, including for products they do not ordinarily make. Executive Order 13603 includes language that suggests the same, delegating in Section 201(a) “the authority of the President... to require acceptance and priority performance of contracts.” In

the context of COVID, these issues appear to have been resolved on a case-by-case basis. For example, GM and Ford, which do not ordinarily make medical devices like ventilators, partnered with companies that do. In the case of vaccine production, companies like Merck are licensed to produce the Johnson & Johnson vaccine.

Whether it is a good idea or not to require a company to make a medical product it does not ordinarily make, or any other such product or service, is a question for policymakers. Such a requirement would more fully engage the concerns expressed by the U.S. Chamber of Commerce about an actual commandeering authority and the nationalization of industry. However, if indeed acceptance of contracts for products a company does not ordinarily supply is intended to be required by the DPA, it ought to be clearly stated in the law, and issues of liability and risk should be more clearly addressed in that context. Legal and policy disputes cause delay. Litigation is also a poor substitute for purposeful policymaking, which increases the diversity of views considered and helps to condition expectations and understandings.

2. Academia

The operative authorities within the DPA apply to “persons.” The law’s general definition of “person” found in Section 702 is broad (“an individual, corporation, partnership, association, or any other organized group of persons”). However, the Department of Commerce regulations, required by the law and the president to implement Sections 101 and 705, expressly incorporate academic institutions within one sectional definition but not the other. One would expect a government grant or contract to cover such matters and the better legal view is that the general statutory definition is determinative. However, one can also imagine a scenario involving prioritization where the differences in regulatory language might prompt litigation over the prioritization of academic services and the nature of academic freedom, especially outside the context of existing grant or contract language. The more important point here is that clear regulatory language and the legislative process are two mechanisms with which to define and condition expectations going forward. With AI this is as important to do in academic context beyond Federally Funded Research and

Development Centers as it is with industry, so that issues are identified and addressed before moments of urgent need.

Imagine a breakout AI moment—call it a Sputnik moment if you want, although it will more likely be a China-1 moment named after China’s first satellite. The United States Government might feel compelled to respond as soon as possible in a like manner or in a defensive manner. This would not be the time to explore and litigate whether and how the government might mobilize academic and industry assets to provide AI services and prioritize AI contracts.

3. Talent

The DPA provides two authorities that may bear on recruiting critical expertise for government AI work, Section 703 and Section 710 discussed earlier. Section 703 provides agency heads waiver authority to hire persons outside the competitive civil service system and without regard to the general schedule (GS) pay scale. However, salaries are still capped at the GS-18 rate, now calculated at the Senior Level, which replaced the grades of GS-16 through GS-18. Senior Level paygrades are, in theory, designated for government employees with specialized expertise who are not otherwise performing management functions associated with the Senior Executive Service. Government pay scales are not competitive with the sort of NFL salaries that many AI innovators and engineers are receiving in the private sector. A first-year PhD in computer science can make as much as \$600,000 as a software engineer at a leading commercial technology firm. In contrast, a similarly situated PhD joining an FFRDC can expect to make one-third or less of that amount. Using this special 703 authority and the GS-18 rate, a government employee could, at best, make \$207,000—the highest possible level of ES-I (2019). Of course, an entry-level employee would not likely receive the benefit of a 703 waiver for this purpose. Although not addressed in the DPA, in other contexts, such as the Public Health Service and the military, the government possesses statutory authority to provide signing bonuses and incentive payments to recruit and retain expertise. Thus, it is possible for policymakers to construct

even greater incentives to attract AI talent than is currently contained in the DPA.

Recalling that the goal is not to use the DPA, but to provide a purposeful and effective AI architecture, the government, industry, and academia might more aggressively use the Intergovernmental Personnel Act (IPA) to bring industry and academic talent into government and expose government personnel to industry and academic AI labs and programs. Under the IPA, this can be done on a rotational basis and without additional cost, as IPA personnel receive pay and benefits from their parent organizations. However, effective use of this authority will require Congress to lift or waive statutory caps on the number of IPA personnel permitted.

4. Authority to Inquire and Survey—Industrial Base Assessments

Section 705 and corresponding CFR regulations provide authority for the government to obtain information “as may be necessary, or appropriate, in his [the President’s] discretion, to the enforcement and administration of this Act.” This provision is principally implemented through delegated authority by the Bureau of Industry and Security (BIS) at the Department of Commerce. The BIS conducts “industrial base assessments” “based on requests it receives from U.S. government agencies” “to enable the private sector and government agencies to monitor trends, benchmark industry performance, and raise awareness of diminishing manufacturing capabilities” as stated by the BIS website.⁶ The regulations state that information may be acquired from for-profit and non-profit organizations, as well as academic institutions and government agencies. Surveys are generally electronic and presented in a question-and-answer form and may require information about “employment, research and development, sources of supply, manufacturing processes, customers, business strategy, finances and other factors affecting the industry’s health and competitiveness,” such as data security practices. When the current regulation was circulated for public comment in 2015, BIS received just two comments in response. Links to completed industrial base assessments are found at the BIS website and include assessments of supply chains related to rare earth elements, C-17 aircraft, and topics like underwater acoustics and

satellite imagery. A critical technology assessment of U.S. artificial intelligence was conducted in 1994. The BIS does not indicate whether its posted list is exhaustive, or illustrative. Consistent with the President's constitutional authority over classified information and the confidentiality provisions of the DPA itself, the BIS could keep such studies confidential; however, the agency has not indicated if it has. As a distinct matter, in practice the BIS deems all information submitted in response to a survey as confidential and thus, one hopes as well, ensures a corresponding level of cybersecurity. Indeed, given the ongoing spate of successful cyberattacks on U.S. systems, Congress or the President might wish to prescribe cybersecurity requirements and standards for DPA practice.

Section 705 is clearly written and the authority it presents is strong. Section 705 could be used to collect information about AI research and development and to forecast milestones and pending breakout moments. Thus, depending on whether and how it is used, it could be as important an AI authority as Title I or the CFIUS provisions of the DPA. But its use in this manner will likely come with challenge and controversy, especially when directed beyond traditional defense industry actors to the AI commercial and social media sectors. More to the point, many AI companies are not part of the Cold War defense establishment. Neither is AI a defense function or weapon—it is a universal capacity. Thus, if the government is concerned about accurately charting the direction of AI R&D, it would be wise to test any limits and tensions in the law and its implementation now. If one believes the potential reach of the DPA goes too far, statutory amendment—not litigation—is the better course. Two issues warrant debate and resolution—now: (a) If the government is going to collect information from private companies, as it already does, are there additional safeguards and limitations on doing so that should be put in place? (b) To what extent, if at all, should the government use its authority to inquire into the activities of private companies engaged in AI research? COVID demonstrates that it is better to ask and answer these questions now than in the moment of need.

5. The Scope of the DPA's Allocation Authority

The allocation authority in the DPA is written with broad, if not breathtaking, language. As we have noted, Section 101(2) permits allocation “in such manner, upon such conditions, and to such an extent as he [the President] shall deem necessary or appropriate to promote the national defense.” This is the sort of language executive branch lawyers sneak into legislation when no one is watching.

At the same time, the executive branch appears not to have used this authority since the Korean War, except for the contingency designation of aircraft for the Civil Air Fleet. Thus, executive branch and industry actors have not had occasion to test what “manner,” “conditions,” and “extent” mean. Within the executive branch, key actors should seek the input of the Justice Department's Office of Legal Counsel on this matter. And Congress would do well to provide additional legislative guidance regarding the scope of the DPA's allocation authority. In a counterintuitive manner, the authority is so textually broad, Presidents and their advisors may be hesitant to use it. If not during the COVID-19 pandemic, one might ask, when would such an authority be used?

Of course, sometimes the availability of potential authority is sufficient leverage to achieve a result through consultation without invoking the law. It appears that the Biden Administration has achieved many, if not most, of the results it has sought for vaccine production and distribution using consultation and the exercise of “soft” allocation authority, i.e., the prioritizing of contracts to ensure necessary materials are allocated in accordance with government priorities and vaccine production needs, thus negating the need to invoke the expansive authority found in Section 101(a)(2). But if I were worried about the future allocation of electricity, cloud storage, and computational capacity in the context of a national security crisis, I would want a better understanding now as to the operating scope of this authority today (not in the political context of the Korean War during which it was passed) as well as an understanding of who or what entities would oppose such exercise of authority, and on what basis. Many concerns, I would imagine, could be addressed, and mitigated by understanding what the

government might have in mind rather than by debating abstractions. If the President is not prepared to invoke the authority in its present form, or industry and academia will resist its use, then it is now time to debate amendment to the law.

6. Liability

Section 707 of the DPA states: “No person shall be held liable for damages or penalties for any act or failure to act resulting directly or indirectly from compliance with a rule, regulation, or order issued pursuant to this Act, notwithstanding that any such rule, regulation, or order shall thereafter be declared by judicial or other competent authority to be invalid.”

A plain reading of this section indicates that it would protect companies from contractual liability for prioritizing a DPA contract over an existing commercial contract with a private party. It would also protect the contractor for relying in good faith on government direction and contracts pursuant to the DPA.

Liability, however, remains an issue in implementing the DPA. To start, the section does not extend to tort liability. The term tort is not mentioned, and were the section intended to preempt state tort law, courts would expect an express legislative statement in an area where federal law could not be said to already occupy the field. In addition, liability remains an issue where companies are requested to provide a product or service that they do not ordinarily make or that relies on new technology.

The public policy question is when, if at all, should companies receive tort liability protection for making products on an emergency or experimental basis. The question has been addressed in the context of pandemics in the form of the Public Readiness and Emergency Preparedness Act (PREP Act), which provides liability protection for pandemic medical countermeasures, 42 U.S.C. §§247d-6d & 6e. However, even with this law, which seemed clear in text and intent, there is indication some companies delayed entry into the market pending passage of the CARES Act, expressly stating that respiratory protective devices were covered countermeasures under the PREP Act (§3103). Policymakers

should consider now in what contexts liability protection may be sought in the context of national security applications of AI. This is not an argument for or against liability protection, but merely for clarity in the law, so that companies can make knowing and purposeful decisions, cognizant of risk, and production and delivery of a needed product or service is not delayed by an issue that was foreseen. For sure, industry actors are more likely to resist invocation of the DPA, or portions of the DPA, without liability protection or clarity; however, at the same time, AI presents such varied contexts across applications that general rules seem problematic. Legislative consideration of the question is prudent along with the identification of parameters.

7. Does the DPA Provide “Notwithstanding” Authority?

President Trump’s invocation of the DPA to leverage meat packing companies into staying open in April 2020 (if in fact that is what occurred) raises the question whether the DPA can override otherwise applicable health or safety laws or regulations. For example, would the “manner,” “condition,” and “extent,” language found in the allocation authority allow the President to bypass otherwise applicable OSHA, EPA, or CDC guidelines and regulations? Usually, when Congress provides “notwithstanding” authority it expressly does so by stating in the statute that the law operates “notwithstanding any other law.” However, the DPA is, in part, an emergency authority, and one can imagine the government taking the view that it overrides other law on that basis alone. The argument here is twofold. First, there should be purposeful and deliberate consideration of AI contexts where emergency needs may warrant regulatory or other exceptions. Second, if those potential exceptions are compelling, or potentially so, then the DPA needs additional clarity on this point.

8. Voluntary Agreements and Plans of Action

Section 708 of the DPA authorizes the President to “consult with representatives of industry, business, financing, agriculture, labor, and other interests in order to provide for the making by such persons, with the approval of the President, of voluntary agreements and plans of action.” This lengthy section has

numerous requirements, including the monitoring of any agreement by the Attorney General and the Chairman of the Federal Trade Commission to “assure . . . the protection and fostering of competition and the prevention of anticompetitive practices.” In contrast to some provisions of the DPA that are written with 1950s Cold War clarity and breadth, this section of the DPA has all the manifestations of having been written by a roomful of lawyers charged with making a law so confusing and unclear as to deter its use. Neither is there an apparent record of the provision’s use since 1950, which might offer the clarity of use.

Here too, COVID may serve to offer an important benchmark. On August 17, 2020, FEMA, using delegated authority from the president to DHS to FEMA, sponsored a “Voluntary Agreement for the Manufacture and Distribution of Critical Health Care Resources Necessary to respond to a Pandemic.” The Agreement is predicated on a finding by the FEMA Administrator that the Agreement is “necessary to help provide for the national defense” as well as a finding by the Attorney General, following consultation with the FTC, that the purpose of “the agreement may not reasonably be achieved through an agreement having less anticompetitive effect or without any voluntary agreement.” The agreement permits FEMA and industry actors to collectively coordinate and collaborate on the effective manufacture and distribution of PPE and vaccine, among other supplies, as implemented through individual plans of action. The Agreement and law provide “safe harbor” to participants from civil or criminal antitrust enforcement. The Section provides at least three safeguards: (1) Only activities approved by FEMA receive 708 protections; (2) Oversight by the Attorney General; and (3) A requirement to hold public meetings to implement the Agreement or plans of action, unless the Chair (the FEMA Administrator) exempts all or part of these meetings because they would require participants to disclose trade secrets or commercial or financial information that is privileged or confidential.” The Administrator of FEMA so far has done so.

In the absence of more transparent practice, it is not clear how Section 708 or this Voluntary COVID Agreement will align with

contemporary understandings and practices regarding antitrust rules and fair-trade practices. At the same time, the COVID-19 pandemic (and corresponding supply chain challenges for PPE and medical supplies) illustrate the need to have mechanisms to coordinate all of government, indeed all of country, responses to national security challenges. A breakout moment in AI, or perhaps another emerging technology like quantum computing, might necessitate a similar effort. National security specialists and legislators would be wise to study the design—and now implementation—of Section 708 to ensure that it reflects present legal values and will effectively function as an AI mobilization tool in practice, if needed.

9. Federal Acquisition Regulations and Practice

Although not expressly a DPA issue, one reason the DOD uses the DPA so frequently to help expedite and manage contracts is because the Federal Acquisition Regulations (the FAR) are otherwise outdated, cumbersome, and highly bureaucratic. The FAR deters interest in government contracts and deters corporate social responsibility to produce emergency supplies and services. If, indeed, the DPA is intended to be used in emergencies to incentivize contracting with the government for essential national security supplies, reform of the government contracting process generally would be a good place to start, to make government business a more attractive and viable option for more companies. This is especially urgent where the U.S. government is concerned about single source and foreign source supply chains. Small and innovative AI companies that are not dependent on government contracts may eschew working with the government, not just for the sort of policy reasons that caused Google employees to balk at working on DOD's Maven project but because it is too hard and complicated to do so. Government grants and contracts may come with so many requirements and reports that academics take their ideas to industry actors. When U.S. tax dollars are in play, regulation and oversight is appropriate, but unnecessary delay is not. Here the DPA may itself provide a model that works: The CFIUS process, while a burden on industry actors, is fast, with clear deadlines measured in days. Likewise, the government might look

at AI tools to see where and how the contracting and grant processes might be streamlined and simplified.

10. Pricing

Considering the Act's requirement for specific authorizing legislation to impose wage stabilization and price controls, the provisions addressed to price gouging, as well as generalized concerns about use of the DPA to "nationalize" industry, further legislative clarity on equitable pricing and price ceilings under the DPA would be useful. DOD, of course, has longstanding practice negotiating DPA contracts. The law might be updated to reflect this practice, to limit the risk that the government might use the DPA to require companies to accept contracts below market value, or conversely, to prevent companies in emergency or sole source contexts from demanding excessive or inappropriate compensation. Here, the lessons derived from the COVID experience need to be purposefully extracted and applied going forward, in law if need be.

11. Transparency

If one purpose of the DPA is to ensure that the nation's industrial capacity is mobilized to meet emergencies, Congress should require more detailed and timely reporting in emergencies on how the Act is being used, including specific contractual obligations and incentives. Hearings should clarify why the Act was and was not used to respond to the nation's critical shortages in medical supplies and medicines during the continuing COVID-19 crisis. We should know now what lessons to extract from the COVID-19 experience, as the DPA could become a critical tool in responding to future breakout moments involving emerging technologies, including AI.

12. Litigation

Litigation is likely regarding the reach of the DPA into academic and industry AI, and it is preferable to test the reach of the law now, rather than at a moment of crisis or need in the years ahead. In this regard, the 2015 FBI-Apple iPhone litigation may provide

the model and the deterrent. The government is not always at its best, and most nuanced, in times of crisis. At such times, it is more likely to overreach or focus exclusively on immediate needs than on long-term consequences. Litigation also risks the disclosure of trade secrets and milestones, not necessarily in court, but perhaps in media responses and commentary. In the context of the PATRIOT Act and FISA Amendments Act, it has taken almost two decades to find something of a security-privacy equilibrium. As with software code, Congress patches the law. Of course, an even better course is to find a common understanding between parties based on shared interests, and—where helpful—embed that understanding in legislation, perhaps in the form of a DPA reauthorization.

Nonetheless, efforts to use the DPA in new ways or to reach beyond traditional DIB actors that populate the AI field risks litigation. Indeed, the DPA contemplates litigation and enforcement in granting jurisdiction to federal district courts over DPA disputes. At least six challenges are likely:

- A. The authority is being used beyond the traditional predicate necessity of “national defense.”
- B. The authority being used does not track with the statutory or regulatory requirements of the DPA.
- C. Use of the authority violates the individual’s or institution’s First Amendment rights to free speech.
- D. Use of the authority violates the individual’s or institution’s Fourth Amendment rights.
- E. Use of the authority violates the individual’s or institution’s Fifth Amendment rights.
- F. The authority has fallen into disuse, if it was ever used, and is no longer extant under the doctrine of desuetude.

If litigated, courts will weigh the language of the statute along with practice and legislative history. Where language is plain, many

judges will go no further. Thus, from the standpoint of public policy, whether one is inclined to support the use of the DPA or not, a better understanding of how the law might be used for AI purposes is desirable to avoid litigation, mitigate concerns, and offer clarity in the law.

Conclusion

As often happens, U.S. law has not kept pace with technological change. Statutory law and case law never keep up with Moore's Law. This is true with respect to the DPA, the principal legislative tool available to the executive branch to harness the nation's industrial and technological capacity in furtherance of U.S. national security.

Time now for a 21st century DPA, one that will effectively provide the authority to regulate and mobilize AI for national security purposes, create an effective process for doing so, and do so consistent with a contemporary understanding of America's constitutional values. FIRRMA is a step in the right direction, expanding the authority of CFIUS review beyond Cold War domains into a fuller range of strategic domains, such as critical infrastructure and technologies, all within a process with clear and short timelines and subject to court review.

What should a 21st Century DPA include and look like?

- It should effectively address the 12 issues identified above.
- It should incorporate the lessons learned during America's COVID-19 pandemic about harnessing America's industrial capacity, or more precisely, failing to do so in a timely manner.
- It should, through the legislative process, establish understandings and expectations not just within the traditional defense industry sectors, but within the AI innovation community as well.
- And it should be written with the language and values of the 21st century, as opposed to the 1950s, so that executive actors do not hesitate to use its authority purposefully, wisely, and well, and industry and academic actors do not hesitate to respond in kind.

Most importantly, legislative consideration of the DPA—as an AI tool—will help establish expectations and identify issues so that when crisis comes, the law can be used as a source of authority to expedite, rather than a source of dispute to litigate. As the Biden Administration demonstrated with COVID-19, building public expectations regarding how the law will be used, and a willingness to use the law, can be as important as the authority itself.

Author

The Honorable James E. Baker, a CSET Distinguished Fellow, is a professor at Syracuse University College of Law with a courtesy appointment in the Maxwell School. Judge Baker also serves as Director of the Institute for Security Policy and Law. He is the author of *The Centaur's Dilemma: National Security Law for the Coming AI Revolution* (Brookings: 2021).

Acknowledgments

For feedback and assistance, the author would like to thank Chuck Babington, Josh Geltzer, Danny Hague, Laurie Hobart, Matt Mittelsteadt, Mark Rosen, Adrienne Thompson and Lynne Weil.



© 2021 by the Center for Security and Emerging Technology. This work is licensed under a Creative Commons Attribution-Non Commercial 4.0 International License.

To view a copy of this license, visit <https://creativecommons.org/licenses/by-nc/4.0/>.

Document Identifier: doi: 10.51593/20190021

Reading List

“Apple v. FBI: Concerning an Order Requiring Apple to Create Custom Software to Assist the FBI in Hacking a Seized iPhone,” EPIC, <https://epic.org/amicus/crypto/apple/#legal>.

Defense Production Act of 1950, Pub. L. No. 81-774, 64 Stat. 798 (1950), [https://www.fema.gov/media-library-data/1515074994368-bdc5ff1d7b24e5e60888661aaca15bf1/Defense_Production_Act_\(current_thru_2017\).pdf](https://www.fema.gov/media-library-data/1515074994368-bdc5ff1d7b24e5e60888661aaca15bf1/Defense_Production_Act_(current_thru_2017).pdf).

Exec. Order No. 13603, 77 FR 16651 (2012), <https://www.federalregister.gov/documents/2012/03/22/2012-7019/national-defense-resources-preparedness>.

Exec. Order 13917, 85 FR 26313 (2020), <https://www.federalregister.gov/documents/2020/05/01/2020-09536/delegating-authority-under-the-defense-production-act-with-respect-to-food-supply-chain-resources>.

Federal Emergency Management Agency, *The Defense Production Act Committee Report to Congress* (Washington, D.C.: Department of Homeland Security, August 2011), <https://fas.org/irp/agency/dhs/fema/dpac.pdf>.

FISA Amendments Act of 2008, Pub. L. No. 110-261, 112 Stat. 2436 (2008), <https://www.govinfo.gov/content/pkg/STATUTE-122/pdf/STATUTE-122-Pg2436.pdf#page=1>.

Foreign Investment Risk Review Modernization Act of 2018, H.R. 5841, 115th Cong. (2018), <https://www.congress.gov/bill/115th-congress/house-bill/5841/text>.

Patriot Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001), <https://www.congress.gov/107/plaws/publ56/PLAW-107publ56.pdf>

Endnotes

¹ Ben Buchanan, “The AI Triad and What It Means for National Security Strategy” (Center for Security and Emerging Technology, August 2020), <https://cset.georgetown.edu/wp-content/uploads/CSET-AI-Triad-Report.pdf>.

² Priscilla Alvarez, Curt Devine, Drew Griffin, and Kristen Holmes, “Trump administration’s delayed use of 1950s law leads to critical supplies shortages,” CNN, July 14, 2020, <https://www.cnn.com/2020/07/13/politics/delayed-use-defense-production-act-ppe-shortages/index.html>.

³ George H.W. Bush, “Statement on Signing the Defense Production Act Amendments of 1992,” October 28, 1992, <https://www.presidency.ucsb.edu/documents/statement-signing-the-defense-production-act-amendments-1992>.

⁴ Congressional Research Service, *The Committee on Foreign Investment in the United States (CFIUS)* (Washington, D.C.: Congressional Research Service, February 2020), 35, <https://crsreports.congress.gov/product/pdf/RL/RL33388>.

⁵ Federal Emergency Management Agency, *The Defense Production Act Committee Report to Congress* (Washington, DC: Department of Homeland Security, September 16, 2015), iii, https://www.fema.gov/media-library-data/1444409712951-aa84d20d8c72d8abd85f77730123b4e5/DPAC_Report_to_Congress_2015.pdf.

⁶ Bureau of Industry and Security, “Industrial Base Assessments,” Department of Commerce, accessed November 1, 2020, <https://www.bis.doc.gov/index.php/other-areas/office-of-technology-evaluation-ote/industrial-base-assessments>.