



Defense Production Act and Global Catastrophic Risk – A Primer

The Defense Production Act of 1950 (DPA, [50 U.S.C. §4501 et seq.](#)) grants the government a range of authorities to shape how the private sector provides materials, services, and expertise to the government in US national defense. The DPA is most known for its **Title I authorities**, which require companies to accept contracts for goods and services necessary for the national defense, and its **Title III authorities**, which create financial incentives and subsidies for critical domestic industries to produce more goods and materials than would otherwise be provided.

Over the past 70 years, the DPA's authorities have become the foundation of US preparedness for and response to national emergencies arising from all threats, with a wide range of uses. Throughout the Cold War, the DPA enabled domestic industries to out-compete the Soviet Union in the provision of military equipment. The DPA's definition of "national defense" explicitly encompasses domestic emergency response due to amendments to the Act. So, when major natural disasters have occurred, the DPA has helped communities get priority access to the critical materials they need to support response and recovery operations.

How the DPA relates to global catastrophic risk (GCR)

The US Congress has defined GCR in law as "the risk of events or incidents consequential enough to significantly harm or set back human civilization at the global scale." ([6 U.S.C §821\(6\)](#)).

According to academic and expert researchers, a number of threats and hazards potentially pose global catastrophic risk: nuclear weapons, climate change and ecological collapse, pandemics and biotechnology, artificial intelligence (AI), near-Earth objects, such as asteroids and comets, and supervolcanic eruptions.

Should a global catastrophe occur, the government would need support from private industry. Medical supplies, energy systems, transportation, communications, food production and logistics, among other critical infrastructure and goods, are mostly owned or operated by private firms. Domestic manufacturing might need to be retooled or expanded quickly to meet demand in a crisis. And technical and operational expertise needed for innovation, production, and distribution – all of which heavily resides in the private sector – would need repurposing for participation in the government response.

Historical case study – COVID-19 response

The COVID-19 pandemic was an unprecedented peacetime emergency that saw the DPA used at a scale not seen in decades. Once the coronavirus began overwhelming global supply chains in early 2020, the US government [turned](#) to DPA Titles I and III to alleviate critical medical shortages and to speed up vaccine development. Both the Trump and Biden administrations issued a series of orders and directives to mobilize industry against the pandemic. For example, in late March 2020, President Trump signed executive orders invoking DPA Title I to prioritize the production of personal protective equipment (PPE) and ventilators. Between March 2020 and September 2021, federal agencies [used](#) Title I at least 73 times for the COVID-19 response.



Furthermore, DPA authorities underpinned “Operation Warp Speed” – the public-private partnership to accelerate COVID-19 vaccine development and distribution. The federal government issued DPA priority ratings for key vaccine contracts, which moved vaccine makers’ orders for raw materials and equipment to the front of the line. According to the [White House](#), the Trump Administration used the DPA at least 18 times to aid vaccine development efforts. It also included Title III investments to expand manufacturing capacity. For instance, in mid-2020, the Department of Defense [announced](#) \$75.5 million of DPA funds to ramp up production of COVID-19 testing swabs, doubling output to 40 million swabs per month.

GCR scenario – a major volcanic eruption

In 2028, a [VEI-7](#) eruption occurs in Turkey at Acigöl-Derinkuyu (one of many possible [locations](#) worldwide, including in the US), completely devastating the local region with immediate effects in a geopolitically sensitive region of the world. Beyond the provision of immediate assistance to a NATO ally and the resulting humanitarian crisis, the miles high volcanic plume high injects aerosols and sulfur dioxide into the stratosphere, leading to a “[Little Ice Age](#)” like climatic effects, or a “[Year Without A Summer](#)” at a minimum, having severe knock-on effects on agricultural production worldwide.

Under Title I authorities, key agricultural inputs and products (calorie-dense foods, fertilizers, clean water, food-grade fuel, and cold storage) are deemed critical to national defense. The Department of Agriculture issues prioritized orders for emergency rations, seeds, and planting stock for resilient crops, as well as water filtration and sanitation supplies. Section 102 is invoked to prevent hoarding of seeds, water and fuel. DPA use is necessary not just for the American food supply but also for fulfilling the nation’s vital role as a major food exporter to prevent destabilizing, widespread famines known to lead to armed conflict.

Under Title III authorities, funds are allocated for the expanded construction of indoor farming near urban centers, rapid expansion of resilient food production (such as mycoprotein, algae and bacterial protein), repurposing of idle warehouses and meatpacking plants, fuel subsidies, and grants for local communities to produce and distribute low-light resilient crops.

Under Title VII authorities, the government convenes experts preidentified from the agricultural industry through the National Defense Executive Reserve. They assist government scientists in identifying new strains of cereal crops that can be effectively grown under the new conditions across the globe, drawing from seed banks like the Svalbard Global Seed Vault and other genetic repositories.

GCR scenario – AI-enabled cyberattack on energy grids

In 2030, a highly advanced [AI-enabled malware](#) activates simultaneously in multiple regional utility networks across the country. The [attack](#) disables grid substations, corrupts supervisory control and data acquisition (SCADA) systems, and interrupts communications networks. The disruption lasts for months due to AI-enhanced malware’s ability to evade detection and remediation through code changes and adversarial techniques. Hundreds of millions of Americans are without access to reliable electricity, clean water, cellular or internet connectivity, or financial systems. National logistics grinds to a halt, severely limiting the distribution of physical goods. Hospitals and other emergency services quickly deplete medical and critical supplies.



Under Title I authorities, the Department of Energy issues priority orders for grid restoration, including manufacturing and delivery of high-voltage transformers, SCADA replacements, and analog backup systems. The Department of Homeland Security issue orders for the production and deployment of analog communications systems. Diesel and gasoline deliveries are diverted to hospitals, food distribution centers, emergency shelters, and military, National Guard, and FEMA mass care operations.

Under Title III authorities, the Department of Energy issues targeted loans and purchase guarantees to key industrial manufacturers to produce industrial-grade transformers, relays and batteries, among other parts and supplies needed for repairing substations and transformers. Hospitals, data centers and local communities are funded to rapidly deploy modular microgrids and solar-diesel hybrid backup systems. The Department of Health and Human Services uses Title III funds to expand domestic drug manufacturing, focusing on essential generics and injectable medicines, as well as the production of off-grid-compatible medical devices and support systems.

Under Title VII's voluntary agreement authority, the Cybersecurity and Infrastructure Security Agency (CISA) convenes cybersecurity experts from across the affected critical infrastructure nodes to develop concrete plans of action for remediating the ongoing cyberattack. Many of these cybersecurity experts were previously identified and screened for government clearances under the National Defense Executive Reserve program established in Title VII of the DPA. These private sector experts voluntarily deploy into government to help support CISA, US Cyber Command, and other government agencies in implementing the governmental actions necessary for the remediation. Because of the spillover effects from the attack on non-US critical infrastructure, these plans of action are shared and followed by other allied countries.