

# Use of the Defense Production Act of 1950 for Critical Infrastructure Protection<sup>1</sup>

## Executive Summary

- Critical infrastructure protection requires an integration of multiple goals, objectives, and policies. Currently, this nation lacks agreement on a comprehensive philosophic and legislative framework that integrates competing policies for infrastructure protection purposes.
- The Defense Production Act of 1950 is a powerful legislative tool for managing critical infrastructure service failures. At the core of critical infrastructure protection philosophy is a concern for national security, national defense, and the public health and welfare. Critical infrastructure preparedness, response, and restoration could all benefit from using the DPA in a judicious and targeted manner.
- Congress has not thoroughly debated using the DPA for critical infrastructure disruptions. During the Year 2000 preparations, the Administration was equally divided on whether, and to what extent, the President could use the DPA in the event of a significant critical infrastructure disruption.
- Several complex legal and policy issues permeate the debate. These include the definition of “national defense” in an information age context as well as the execution of Congress’s delegation by the Administration, as reflected in Executive Order 12919.

---

<sup>1</sup> © Lee M. Zeichner, All Rights Reserved (2001). I would like to extend my deep appreciation to the National Archives Administration for their support in providing access to original Defense Production Act debates and related resource materials. NARA is a national asset. I would also like to thank my legal assistants, Morgan Allen, Alexis Ovitt, and Jeanne Geers for their superb research skills and capabilities. Finally, my gratitude to John McCarthy (USCG-ret) for his valuable insights in analyzing the activities surrounding Year 2000 policy discussions.

- If the Defense Production Act is not overhauled for critical infrastructure purposes, Congress should immediately consider alternative legislative frameworks for managing national critical infrastructure disruptions. Absent this framework, the nation will continue to lack a unified approach to managing national cyber emergencies.

## The Defense Production Act and Critical Infrastructure Protection

As we move beyond the fifty-year anniversary of passage of the Defense Production Act of 1950 (“DPA”),<sup>2</sup> both Congress and the Administration should revisit the genesis of this profound legislative framework.<sup>3</sup> Congress debated the DPA during a dynamic period in our national history. With the memory of Pearl Harbor fresh in the Congress’s institutional psyche and an undeclared conflict in Korea, both Congress and the Administration cooperated to develop a legislative framework that integrated competing defense, national economic security, and related policy demands.

### Overhaul of the DPA for Critical Infrastructure Protection

Close to five years after the President’s Commission on Critical Infrastructure (“PCCIP”) issued its report,<sup>4</sup> and now into the second Presidential Administration to govern in an information-based economy, the nation lacks

an integrated legal, policy, and management philosophy to support critical infrastructure protection efforts.

Multiple reports, technologists, and commentators have acknowledged the nation’s significant reliance on critical infrastructure services. Our economic strength and stability are linked inextricably to the reliable delivery of essential services—including information and communications, energy, financial, transportation, emergency medical and police, and water. Paradoxically, our robust capacity to deliver critical infrastructure services over information networks leaves the nation vulnerable in new and different ways. Economic security, long an element of national security and national defense, depends on

the reliable delivery of these critical infrastructure services more than ever.

However, governance and policy solutions from the “physical world” do not occur seamlessly in cyberspace. Reliance on information systems and networks creates diverse risks—threats and vulnerabilities that are not addressed in traditional plans and processes. Problems and solutions cross over political boundaries and challenge many of the legislative frameworks and philosophies developed during the past 50 years. As a result, managing infrastructure disruptions demands alternative preparedness, response, and restoration strategies.

---

*... the nation lacks an integrated legal, policy, and management philosophy to support critical infrastructure protection efforts.*

---

2 Defense Production Act of 1950, as amended, 50 USC App. § 2061 *et seq.* (“DPA”). This paper focuses exclusively on Title I authority to expedite the priority delivery of goods and services for the federal government’s critical infrastructure goals and purposes.

3 For an excellent overview and analysis of the DPA, please refer to *Defense Production Act: Purpose and Scope*, by David E. Lockwood, Congressional Research Service Order Code RS20587 (Updated June 22, 2001).

4 The PCCIP recommended use of the DPA for national critical infrastructure disruptions. See *Protecting America’s Infrastructures, the Report of the President’s Commission on Critical Infrastructure Protection* at 81 (October, 1997).

## Year 2000 Cyber-Solutions Dismantled

Critical infrastructure protection requires an integrated policy framework. Risk management, public-private collaboration, national defense, law enforcement, intelligence, emergency preparedness and response—all are significant elements of an integrated solution. In order to prepare for the Year 2000 glitch, this nation was forced to piece together an integrated governance framework; the capabilities simply did not exist.<sup>5</sup>

Much of the important work conducted prior to the Millennium Rollover involved developing bridging mechanisms to cross over political boundaries and programs for the physical world. Unfortunately, both the federal government and state governments have for the most part dismantled solutions developed in preparation for the Year 2000 glitch, including physical watch centers as well as integrated policy frameworks. Consequently, there are considerable deficiencies in the nation's ability to prepare for, respond to, and recover from extensive critical infrastructure service failures.

### DPA as a Component of an Integrated Framework

The DPA is one of the most significant Congressional authorities for supporting critical infrastructure protection efforts. Since President Truman signed the DPA into law in 1950, successive Administrations have stitched the DPA delegations into a safety net of Executive Orders, decision directives, and other significant legal doctrine, most of which implement our

most vital defense and security programs.<sup>6</sup> A Congressional and Administration strategy that diminishes the full reach of the DPA undermines our ability to ensure essential operational responsibilities for the national security and defense.

This paper examines four issues in support of broadly applying the DPA to critical infrastructure protection activities.

---

*Reliance on information systems and networks creates diverse risks--threats and vulnerabilities that are not addressed in traditional plans and processes.*

---

1. Why did the Truman Administration encourage Congress to pass the DPA, and how does history inform the current debate?
2. What role does the DPA play as a legislative tool in addressing complex critical infrastructure challenges?
3. What are the competing legislative philosophies for managing critical infrastructure protection?
4. Why must Congress and the Administration collectively develop an integrated framework that includes and promotes use of the DPA? What are the ramifications for the nation if the government fails to resolve these relevant policy challenges?

## Truman and Clinton: Defense Production Act Philosophies

### Truman Introduces the DPA Framework

Slightly over 50 years ago, during the summer of 1950, the Truman Administration's Director

<sup>5</sup> See *Amendment to Executive Order 13073, Year 2000 Conversion*, Executive Order 13127 (June 14, 1999).

<sup>6</sup> See, e.g., *Assignment of National Security Emergency Preparedness Telecommunications Functions*, Executive Order 12472 (1984) (Restoring wireline communications for the federal government).

of the National Security Resources Board entered the Dirksen Building with his counsel for the first of a three-day hearing on legislation entitled the Defense Production Act of 1950. The Administration proposal combined certain of the emergency economic powers exercised during and after World War II into a permanent legislative framework.<sup>7</sup> These powers were necessary to place goods and services where they were most needed. President Truman could exercise these powers during peacetime and absent any declaration of national emergency.

The core of the proposal would allow the President to prioritize and expedite delivery (or allocation) of critical materials. If company A contracts to deliver widgets to company B, but the government needs the widgets—whether for itself or for Company C—the President could so order the prioritization of contract delivery according to terms “necessary to promote the national defense.”

For three days, members of the Banking and Currency Committee debated a series of questions exploring the relationship between economic stability, national defense, and the projection of power and national authority. The Senators’ questions revealed deep concerns over both the Cold War and an ongoing need to restructure national economic programs, courses of action, and priorities:

- Does economic and industrial stability translate into the projection of power and, if so, how does this promote the national defense?
- How much extraordinary authority should the Congress delegate to the President during peacetime? That is, do we need a legislative framework if there is no war, significant

military conflict, or Presidential declaration of emergency? Indeed,

- Could Congress trust the President to administer the legislative framework? If not, how could Congress possibly perform these responsibilities?

The exceptional debate that followed raised complex questions for a nation that had learned more than a little about national defense during the preceding decade. The irony of delegating extraordinary economic powers to preserve a free economy was not lost on the Senate that week, but the complexity of mobilizing after Pearl Harbor (not to mention the perception of the country as weak and vulnerable, which might have precipitated the attack) was fresh on the mind of each and every Senator. The debate conveyed a profound sense of national import where reasonable public servants could differ.

Members of the Banking and Currency Committee also understood that the nation was entering the Cold War and by week’s end sided with the Truman Administration. There was no solid agreement on how the new world order impacted national defense, but the Senate clearly understood the importance of bridging complex and emerging policy concerns into a single, integrated legislative framework.

### **Clinton Administration Debates Use of DPA for Y2K crisis**

A half-century later, as the nation prepared for the Year 2000 (“Year 2000” or “Y2K”) glitch in the summer of 1999, senior officials in the Clinton Administration and their counsel met to discuss whether the DPA could and should be used in the event a Y2K infrastructure outage resulted in a national crisis. Senior leaders grappled with two questions:

---

<sup>7</sup> See U.S. Senate. Committee on Banking and Currency Congress of the United States. *Defense Production Act of 1950* (to accompany by S. 3936), 81<sup>st</sup> Congress, 2d Session. (S. Rpt. 81-2250) 1950 at 45.

1. What is the national philosophy for preparing for, responding to, and recovering from significant critical infrastructure outages?
2. Could the DPA be used to expedite delivery or allocation of goods and services to fulfill these goals?

Multiple areas of disagreement emerged in the six-month Y2K discussions. The most significant concerned the relevance of the Federal Response Plan framework in managing critical infrastructure disruptions of national significance and negotiating the roles and responsibilities of multiple agencies in managing a national cyber-crisis.<sup>8</sup> Pursuant to Executive order 12919, signed in 1994, FEMA is charged with coordinating plans and programs among the civilian agencies for national defense industrial resource preparedness issues.<sup>9</sup>

But did it make sense in the Information Age to saddle FEMA with responsibility for both cyber and traditional natural disaster management? In addition, what was the best process for negotiating and coming to agreement on priorities? If a significant cyber-disruption occurred, how would the consequences be managed and prioritized? Should the federal government seek to restore services as quickly as possible

via the DPA or manage the consequences of the disruption through traditional means, such as via the Federal Response Plan?<sup>10</sup> How would law enforcement, intelligence, and defense issues be parsed by FEMA within the framework developed by the Clinton Administration?

The lack of any pertinent Congressional testimony, debate, or other legal guidance on use of the DPA unquestionably impaired the Administration's ability to settle these disagreements.<sup>11</sup> Senior administration officials debated the issue late into December, 1999. As the Millennium Rollover came and went, no final agreement was ever reached.<sup>12</sup>

Answers to these questions have significant impact on whether to use the DPA, and if so how broadly to interpret its terms. In sum: As we enter the 21<sup>st</sup> century, how does "national defense" relate to the delivery of critical infrastructure services? Specifically:

- What is the relationship between national defense and the orderly functioning of the nation's critical infrastructure services?
- If the DPA could be used, what prioritization plans and policies were in place to determine which entities benefited from the expedited

8 The Federal Response Plan is based on the Robert T. Stafford Disaster Relief and Emergency Assistance Act, as amended, 42 USC § 5121 *et seq.* ("Stafford Act").

9 *National Defense Industrial Resources Preparedness*, Executive Order 12919 (June 7, 1994) (One exception relates to energy issues, which are coordinated by the Department of Energy).

10 As an example, a Federal Response Plan approach ruled out use of other highly responsive and successful programs that service critical infrastructure emergencies. *See, e.g.*, Defense Priorities & Allocations System ("DPAS"). [A highly flexible process for administering critical infrastructure crisis, DPAS is administered by the Office of Strategic Industries and Economic Security, Bureau of Export Administration (Dept. of Commerce) pursuant to the DPA. See 15 CFR Part 700.]

11 Congress has not addressed the basic terms and definitions in the DPA for application in an economy that relies on critical infrastructure services. How, for example, do the terms incorporate the nation's dependence on information services? "Energy" is clearly included in the DPA, but how does the energy infrastructure reliance on communications alter the statutory definition? See DPA definitions at 50 US App. § 2152.

12 This was not the first time senior officials within the Clinton Administration carefully examined the DPA and its implementing programs. *See, e.g.*, *Report of the Interagency Subworking Group of the National Security Council's Ad Hoc Interagency Working Group on National Security Emergency Resources Preparedness* (December, 1996), Administration working group recommends overhaul of Executive Order 12919, and other authorities, which implement the DPA.

delivery of goods and services during a crisis?

- Did the nation understand interdependencies among infrastructure systems? Was restoration of one type of infrastructure (e.g., electricity) more important than another (e.g., communications)?

### From Truman to Clinton: Common Themes

In many ways, the Clinton Administration's debate over use of the DPA for Y2K failures echoes the Truman Administration's dialogue with the Senate Banking and Currency Committee. As in the 1950 debate, both camps agreed that the landscape had changed, whether from the emergence of the Cold War or the advent of the Information Age. However, two camps emerged reflecting significant philosophical splits within the national security and emergency management communities.

The first camp cited the DPA language and legislative intent to demonstrate that Congress had never meant to apply the DPA to information age issues. Absent "scuds and missiles" or a declared national emergency, use of the DPA was both inappropriate and unnecessary. The second camp argued that the DPA might be necessary to prioritize goods and services for fixing and restoring critical infrastructure systems that had failed because of the Y2K bug. This use, they concluded, fulfills the DPA's legislative intent in maintaining a strong industrial and military base.

---

*As we enter the 21st century, how does "national defense" relate to the delivery of critical infrastructure services?*

---

### What is the Nation's Philosophy for Managing Critical Infrastructure Risk?

This section discusses the need for an integrated governance philosophy for managing critical infrastructure disruptions of national significance. This philosophy is more important than ever, given the lack of Congressional and Administration agreement on programs and processes to manage critical infrastructure failures at this time. Within the federal government, administration of the Year 2000 glitch revealed multiple "competing" philosophies. In hindsight, the national Y2K effort was highly successful.<sup>13</sup> Throughout the preparation process, however, it was obvious that the nation was not prepared to respond to and recover from a national critical infrastructure failure.

In an effort to define policy and management objectives for critical infrastructure failures, this section examines five legislative models and philosophies:

1. Integrated Risk Management (PDD-63) model,
2. Traditional Emergency Preparedness,
3. Law Enforcement and Intelligence,
4. National Defense, and
5. Consumer Protection.

---

<sup>13</sup> The nation, including the state and local governments and industry, deserve high praise for resolving a potential crisis. But efforts to address lessons learned and to benefit from the experience have been lost. As soon as the Millennium Rollover passed, the federal government dismantled valuable facilities, partnerships, and institutions, all of which offered significant value; similarly, in many state and local governments, valuable facilities and institutions were set aside.

## Beyond PDD-63: An Integrated National Risk Management Philosophy

Only though an integrated risk management governance philosophy can the nation develop appropriate programs for protecting the nation's critical infrastructures. A legislative program should support and further this philosophy.

Since release of Presidential Decision Directive-63 ("PDD-63") in May, 1998, the United States has embarked on an aggressive critical infrastructure program. More than any other country, the United States has developed a progressive philosophy for critical infrastructure policy coordination, development, and analysis. Significant themes include the following.

### ***At the core of critical infrastructure protection is a concern for national security.***

Since its inception in the aftermath of the tragic Oklahoma City bombing, critical infrastructure protection has always focused on widespread and catastrophic damage. In most cases where infrastructures fail, for whatever reason, owners and operators in industry and government are typically able to manage response and recovery efforts through normal business and risk management processes. For purposes of the Defense Production Act analysis, this is a significant distinction. Congress never intended the DPA to be used for general business purposes or for emergencies that could be managed under normal business continuity and disaster preparedness programs. Conversely, however, where such damages could result, use of the

DPA as part of an integrated framework is both prudent and appropriate.

***Critical infrastructure service failures could result in significant catastrophic damage; in many cases, service failures could cascade into multiple other failures in ways that are not fully understood or predictable.***

A second characteristic of critical infrastructures is their interdependency with other critical infrastructure systems and services.<sup>14</sup> The prudent use of the DPA to prevent catastrophic downstream or cascading damages must be considered. Often a failure to restore service will lead to other infrastructure failures.

Adopting alternative consequence management philosophies under these circumstances, which includes use of the DPA, is vital.

### ***Critical infrastructure protection is a shared responsibility.***

Critical infrastructure protection involves unique partnerships. Not all partnership activities between the public and private sectors support the specialized needs of the critical infrastructure community. Critical infrastructures are largely owned and operated by industry and state and local governments. In many cases, the research and development that lead to infrastructure advancements is conducted within particular portions of the academic community. Concerns are highly operational, focusing heavily on service delivery.

In contrast, many of the programs established for traditional emergency response purposes focus on first responder capabilities and needs.

---

***Adopting alternative consequence management philosophies... which includes use of the DPA, is vital.***

---

14 For an excellent background on this issue, refer to *Preliminary Research and Development Roadmap for Protecting and Assuring Critical National Infrastructures*, Transition Office of the President's Commission on Critical Infrastructure Protection and the Critical Infrastructure Assurance Office at Chapter 3 (July, 1998).

Emergency medical, police, and fire rescue often have dramatically different goals and skills. This is not to say that these divergent communities do not need to be aligned—in fact, they do.<sup>15</sup> It makes little sense, however, to assume that preparedness and response activities in one community will provide similar value in all others.

***Successful critical infrastructure protection leads to economic stability and a more enhanced national defense.***

The final core attribute of a critical infrastructure policy is that full operational capability—an integrated national critical infrastructure program with improvements in reliability of service—projects national authority and power, economic stability, and ultimately promotes the national defense. Use of the DPA as part of an integrated philosophy furthers these goals, which are at the core of the DPA's purpose.

For purposes of Defense Department functions and operational needs, this should be fairly obvious. The Defense Department relies heavily on infrastructure services, whether conducting operations at home or abroad. A failure to develop reliable service delivery patterns would have catastrophic effects on our ability to project power overseas.

**Traditional Emergency Preparedness**

The repeal of the Civil Defense Act of 1950 by the Stafford Act almost 10 years ago set the

parameters of the current emergency preparedness and response legal and policy framework. Pursuant to the Stafford Act, and the Federal Response Plan that implements operational responsibility under that law, our nation relies heavily on traditional emergency preparedness programs and policies to manage a range of complex disasters.

As the Year 2000 crisis demonstrated, our nation lacks a similar preparedness, response, and restoration framework specifically constructed to include critical infrastructure protection. Many commentators have suggested applying traditional emergency preparedness processes to critical infrastructure protection. This is principally how the nation managed preparedness for the Year 2000 transition. However, the Stafford Act, and the programs that are implemented under the legislative framework, were never intended or designed for critical infrastructure protection.<sup>16</sup>

---

***Similar to traditional emergency preparedness, a pure law enforcement or intelligence philosophy will not, by itself, resolve complex critical infrastructure challenges.***

---

There are several important distinctions. First, the underlying philosophy for most emergency preparedness policies and programs is to mitigate the damages of a crisis. This framework, which is both successful and well integrated through years of trial and error, does not traditionally include industry critical infrastructure disruptions, which is a private sector concern. This is so even where the disruptions adversely impact the delivery of critical federal government services. As discussed elsewhere, the Y2K Operations Supplement to the Federal

15 There is, of course significant overlap. For example, first responders are increasingly under pressure to develop interoperable, more robust, and secure communications. Bandwidth and spectrum problems will increasingly plague first responder capabilities – both are critical infrastructure concerns.

16 The Stafford Act repealed the Civil Defense Act of 1950, which centralized emergency response process in the Executive Office of the President. 42 USC § 5121 *et seq.*

Response Plan *explicitly excluded* core critical infrastructure activities.<sup>17</sup>

Second, the funding mechanisms for providing federal assistance and aid are set in law. Stafford Act funding for emergency response activity flows from the federal government under conditions set by the Stafford Act and its Administrative guidance. For example, during Y2K, a Presidential “emergency” was needed – as opposed to a “major disaster” declaration.”<sup>18</sup>

Third, the amount of aid needed to support critical infrastructure disruptions is unknown. Federal government administrators understand the cost of traditional emergency preparedness activities. The cost of critical infrastructure disruptions is not well understood or easily quantifiable. Cyber-related disasters could result in enormous damages absent appropriate mitigation programs and processes.

Finally, traditional emergency preparedness goals are accomplished in today’s legislative framework by aligning federal disaster relief programs with similar operational structures across the federal government and at the state and local levels. Long-term partnerships and relationships – which are crucial for disaster management capability, are built on skill sets, goals, and arrangements vastly different than those in the critical infrastructure community.

## Law Enforcement / Intelligence

Similar to traditional emergency preparedness, a pure law enforcement or intelligence philosophy will not, *by itself*, resolve complex critical infrastructure challenges. Historically, the nation moved in that direction shortly after the Oklahoma City bombing with release of PDD-39. Two years later, the federal government imported PDD-39 into the Federal Response Plan mechanism as the Terrorism Annex.<sup>19</sup> This policy distinguished between consequence management and crisis management, creating room in the aftermath of an incident for law enforcement to investigate and fulfill its Congressional responsibilities.<sup>20</sup> Where the attack is ongoing, law enforcement and intelligence gathering are crucial to locating and stopping the damage. Room for consequence management authorities to conduct their work is negotiated pursuant to the Federal Response Plan mechanism

How would a law enforcement philosophy and framework support and fulfill critical infrastructure objectives? In many cases, policy choices may exist in opposition. As in the Year 2000 preparations, it is unclear whether significant infrastructure outages result from a malicious nation-state attack, teenage hacker, insider mistake, or some other source. Irrespective of the source of the outage, each of the policy choices is valid. The challenge, as argued,

17 These included: (1) Business continuity and contingency planning necessary to ensure that vital services are not disrupted due to Y2K problems, (2) Reconstitution of Y2K-affected State and local information technology systems, (3) Cyber-terrorist attacks (addressed in PDD-63), and (4) National security telecommunications emergencies in industry and in the Federal government *Y2K Operations Supplement to the Federal Response Plan* at 8 (1999).

18 For an excellent primer on programmatic particulars, refer to *Disaster Assistance: Improvement Needed in Disaster Declaration Criteria and Eligibility Assurance Procedures*, Report of the Subcommittee on VA, HUD, and Independent Agencies, Committee on Appropriations, US Senate, GAO-01-837 (August 2001).

19 Terrorism Incident Annex to the Federal Response Plan. (“PDD-39 directs the undersigned departments and agencies to perform specific responsibilities that may affect the performance of their responsibilities under the FRP.”)

20 Similarly, PDD-63 requires the National Infrastructure Protection Center to “monitor” reconstitution activities. Where owner/operators are unable to stop an attack in order to restore service, assistance from law enforcement and intelligence operations would be extremely valuable.

is integrating them into a cohesive framework that reflects the nation's best interests.

## National Defense

How would a national defense philosophy align with critical infrastructure goals? Since 1995, multiple commentators have encouraged a national defense approach to resolving critical infrastructure protection. These opinions include:

- Require the Defense Department institutionally to manage and coordinate a national critical infrastructure program;
- Require the Defense Department to undertake executive agency responsibility for a coordinated incident response and restoration center; or
- Wrap critical infrastructure protection policies under the rubric of Homeland Defense or Homeland Security.

At a minimum, the Defense Department is a customer of critical infrastructure services and must be able to negotiate a level of performance consistent with its goals. Similar to the other issues above, identifying a critical infrastructure framework will lead to appropriate analysis of how the Defense establishment will align with other stakeholders and constituencies.

## Consumer Protection

The final philosophic and legislative option for managing critical infrastructure is consumer protection. A consumer protection methodology provides, at a minimum, assistance and information to support consumer goals and options. Consumer protection was a critical component of the significant work performed by the President's Council on Year 2000 Conversion. One of the valuable lessons from Y2K is the importance of managing consumer confidence, providing information to assist consumer decision making, and supporting awareness as a part of any national effort. However, consumer protection issues do not rise to

the national defense level that the DPA demands.

## Summary – Philosophic Link to DPA

At the core of critical infrastructure protection philosophy is a concern for national security, national defense, and the public health and welfare. Critical infrastructure defines a set of policy priorities, i.e., managing competing policy concerns and, where necessary, prioritizing infrastructure service delivery over other equally plausible policy choices.

The Defense Production Act is the principal legislative tool for managing critical infrastructure operational needs. Were the nation to require critical infrastructure service delivery, then the full and robust use of the DPA would be essential. Critical infrastructure preparedness, response, and restoration could all benefit from using the DPA in a judicious and targeted manner.

## The Origin and Misperceptions of the DPA

The debate over application of the DPA for critical infrastructure is ultimately a valid disagreement on how the nation should prepare for, respond to, and recover from critical infrastructure incidents of national significance. The DPA must be one of the tools available to the Administration to manage complex critical infrastructure disruptions.

That said, there is limited agreement on whether and to what extent the DPA could be used for those purposes. Some of these disagreements are factual, such as whether critical infrastructure incidents truly rise to the level of national import and significance.

Other disagreements are more philosophic, such as whether the nation needs an alternative "preparedness and response" framework to manage critical infrastructure protection.

Finally, some disagreements are technical and legal. These include tracing back the legislative intent of Congress in creating the DPA and applying significant terms such as “national defense” to information age challenges.

This section argues in favor of using the DPA as part of a larger critical infrastructure legislative program. The reasoning and assumptions articulated include:

- Critical infrastructure incidents can result in significant national damage;
- The federal government relies heavily on the reliable supply of critical infrastructure services for serving national defense needs; and
- The government must consistently project strength, economic stability, and political cohesion. Reliable delivery of critical infrastructure services is a cornerstone of these goals.

There are multiple misperceptions about the DPA, many of which were debated during its introduction in 1950. In 1975, 25 years after introducing the DPA, the Congress’ Joint Committee on Defense Production again thoroughly examined the DPA as well as the overarching framework in which the DPA had been used.<sup>21</sup> From these and other discussions, there is a rich library of original history from which current decisions might be measured.

## What is “National Defense”?

The most important legal trigger for use of the DPA is the meaning of the term “national defense.” To take advantage of the programs in the DPA, the President must find that a “national defense” nexus exists. Thus, in the context of critical infrastructure disruptions, the President must make a determination that the expedited delivery of goods or services are “necessary to promote the national defense.”

From the first day that President Truman proposed the DPA, through Y2K and the recent use of the law by the Bush Administration,<sup>22</sup> no single topic has garnered more debate and disagreement than the meaning of this term.

Since 1950, Congress has adopted two definitions. The first, also known as the traditional definition, includes those “programs for military and energy production or construction, military assistance to any foreign nation, stockpiling, space, and any directly related activity”<sup>23</sup> The second, added in 1995, links use of the DPA to the Stafford Act, expanding the term to include “emergency preparedness activities conducted pursuant to title VI of the [Stafford Act].”(Emphasis added). 50 USC App. §2152(13).

Congress’s decision to extend the term “national defense” to include “emergency preparedness activities conducted pursuant to the [Stafford Act]” has engendered development of two alternative positions. Some have taken the

---

*From the first day that President Truman proposed the DPA, through Y2K and the recent use of the law by the Bush Administration, no single topic has garnered more debate and disagreement than the meaning of [national defense].*

---

21 See, e.g., Hearings Before the Joint Committee on Defense Production, Congress of the United States, 94<sup>th</sup> Congress, 2<sup>nd</sup> Session (April 28, 1976).

22 See Memorandum for the Secretary of Energy, Electric Supply Shortage in California (January 19, 2001).

23 DPA, 50 USC App. §§2061, 2152(13).

position that the amendment only grants Presidential authority to engage in certain activities that the Director of FEMA is authorized to engage in, as enumerated in Title VI of the Stafford Act. Others, looking to Title VI in its entirety, adopt a more expansive view, arguing that “emergency preparedness” is defined broadly in Title VI, and that it includes, but is by no means limited to, those activities specified in Title VI.

## Misperceptions

Debates over the meaning of national defense during the Y2K discussions suffered from lack of tangible legislative history and context. As a result, multiple misperceptions inappropriately drive policy and decision-making.

The first significant misperception is that the President may activate the DPA solely for war or mobilizing to go to war. As the discussion on national defense demonstrates, the President must, at a minimum, make a national defense determination. However, Congress has never limited the application to wartime necessity. In fact, many of the Senators during the initial debates in 1950 queried the Truman Administration on this point. The importance of developing an integrated approach to economic security, defense production, and national defense convinced the Senate that such restrictions were not in the best interests of the nation. To date, the DPA makes available materials, services, and facilities in both peacetime and during crisis.

For critical infrastructure purposes, this is an especially important aspect of the DPA. In most cases, critical infrastructure outages will not result from war or an act of war, although this is certainly possible. Rather, the DPA provides a far more practical framework for managing infrastructure outages far short of all-out war.

The second misperception is that the DPA is limited only to preparedness activities. The DPA provides the President with broad authority to expedite delivery of goods and services. Priority contracting and allocation powers, for example, may be used in response and restoration as well as preparedness activities. In many ways, the DPA provides a type of insurance program, which can be used when needed. For response and restoration of critical infrastructure, the use of the DPA is essential. There are no similar Congressional authorities that provide a framework for managing restoration and recovery efforts through expedited delivery of essential goods and services.

The third misperception is that the DPA may only be used after Congress or the President declares a national emergency; this, too, is false. For many Senators

involved in the original debates, this was the most troubling component of the Truman legislative proposal. Why should Congress delegate to the President broad peacetime and wartime authority based only on a national defense determination? However, ever since the 1950 debates, Congress has not required a national emergency determination as a trigger for use of the DPA.

For critical infrastructure purposes, the ability to activate the DPA absent a formal national emergency finding is practical and useful. Many critical infrastructure outages could lead to national emergencies, and this is part of the attraction for using the DPA. Having to first declare a national emergency would impinge on use of this significant authority.

## Conclusion

This paper argues for Congress and the Administration to examine an integrated legislative and policy framework to manage significant

---

*A failure to apply the DPA to critical infrastructures leaves this nation unprotected from a cyber attack or significant critical infrastructure disruption.*

---

critical infrastructure disruptions. There is no framework in place that integrates multiple policies, such as traditional emergency preparedness, law enforcement, national defense, and risk management programs that prioritize restoration of infrastructure services.

The DPA is an important tool for use in managing critical infrastructure disruptions of

national significance. A failure to apply the DPA to critical infrastructures leaves this nation unprotected from a cyber attack or significant critical infrastructure disruption. Critical infrastructure supports the national defense in multiple ways. Absent use of the DPA, Congress should begin work immediately on developing alternative legislative frameworks for managing national critical infrastructure disruptions.