Backgrounder

Published by The Heritage Foundation

No. 2404
April 27, 2010

How to Fix Critical Infrastructure Protection Plans: A Guide for Congress

Jena Baker McNeill and Richard Weitz, Ph.D.

Abstract: *Highways, bridges, power plants, and cyber networks are all part of the national infrastructure—which is essential for the daily functioning of American society. The Department of Homeland Security carries the prime responsibility for protecting "critical infrastructure" from terrorist attacks and natural disasters. The problem currently plaguing the federal government efforts to implement a unified protection plan for the country is that, when it comes to determining which infrastructures are truly critical and which are important but not always essential, chaos reigns. For its part, Congress has at least 86 committees and subcommittees that oversee the Department of Homeland Security, providing for a complex and often burdensome system that impedes successful policy implementation. Three national security experts provide a guide for Congress with which to navigate the country's infrastructure priorities.*

National infrastructure—from roads, dams, bridges, and power plants to cyber networks—assists in the daily functioning of American society. The Department of Homeland Security (DHS) has the principal responsibility for leading national efforts to identify, assess, and protect critical infrastructure from acts of terrorism and other disasters. In 2003, President George W. Bush issued Homeland Security Presidential Directive-7 (HSPD-7), which assigned responsibility for coordinating national measures to strengthen protection of critical infrastructure and resources to the Secretary of Homeland Security.

Talking Points

- The national infrastructure is vital for the daily functioning of American society, thus representing an attractive target for terrorists. Not all infrastructure is equally important, nor can every aspect be protected equally, so the focus must be on the protection of *critical* infrastructure.
- As the lead authority on critical infrastructure protection, the Department of Homeland Security has used the National Infrastructure Protection Plan (NIPP) as its planning document for critical infrastructure protection. But the NIPP lacks adequate tools to assess and manage risks in a way that accurately accommodates the complexity and dynamics of infrastructure, and the current system of congressional oversight is cumbersome and confusing.
- Building solid relationships between the government and the private sector, including small and medium-sized businesses, and encouraging their investments in infrastructure quality can increase the likelihood that critical infrastructure can continue to function, or bounce back quickly, after a terrorist attack or natural disaster.

This paper, in its entirety, can be found at:
http://report.heritage.org/bg2404

Produced by the Douglas and Sarah Allison Center for Foreign Policy Studies
of the
Kathryn and Shelby Cullom Davis Institute for International Studies

Published by The Heritage Foundation
214 Massachusetts Avenue, NE
Washington, DC 20002–4999
(202) 546-4400 • heritage.org

HSPD-7 also instructed the new Department of Homeland Security to support these measures through the development of a National Infrastructure Protection Plan (NIPP) "to identify and prioritize United States critical infrastructure and key resources and to protect them from terrorist attacks."[1]

The first NIPP was issued in 2006 with scheduled revisions every three years. In February 2009, the Department of Homeland Security completed the first review. The new revisions, however, made only small progress in integrating federal, state, local, and private-sector efforts into a truly cooperative national enterprise that can ensure the resiliency of national infrastructure while allowing the economy it supports to grow, innovate, and prosper. Instead of focusing on the current approach to critical infrastructure protection, Congress—in partnership with the Administration, the private sector, and diverse state and local actors—should:

- Develop a congressional process to ensure that legislative initiatives aimed at critical infrastructure protection are based on sound notions of risk;
- Shift the focus toward resiliency, emphasizing protection of the critical infrastructure that, if destroyed, would have catastrophic consequences;
- Continue engagement with the private sector (including domestic and foreign businesses) through better information-sharing channels and continued outreach aimed at small and medium businesses;
- Broaden education, awareness, and training for security professionals charged with protecting America's infrastructure, while promoting critical-infrastructure research and development; and
- Re-examine the current grant-centered approach to improving capabilities at the state and local levels, which all too often fails to produce the right outcomes in terms of added security, and move toward a system of cooperative agreements that would allow the federal government and its state and local partners to negotiate outcomes more effectively.

Guarding the Gates

The NIPP defines the main roles and responsibilities of the federal, state, and local government agencies, as well as of the private-sector actors engaged in protection of critical infrastructure and key resources (CIKR). It also provides a unifying structure for integrating CIKR protection and resiliency into a single national framework based on risk-prioritization to protect America's CIKR from terrorist attacks and natural or technological hazards.[2]

Within the NIPP, there are 18 sector-specific plans (SSPs) that tailor the application of the NIPP to the unique requirements of each of the 18 CIKR sectors. The SSPs (nine have been made public; nine are considered too sensitive for public release)[3] assign responsibilities to 11 sector-specific agencies (SSAs) and other actors that manage the CIKR-protection programs in the 18 sectors. The SSPs also provide guidance for sharing information within a sector, with uniform methods for conducting risk analysis, and which actions and protocols to pursue during emergencies. The following are the CIKR sectors and their sector-specific agencies:[4]

- agriculture and food (Department of Agriculture, Food and Drug Administration);
- banking (Department of the Treasury);
- communications (Department of Homeland Security);

1. Press release, "Homeland Security Presidential Directive-7," U.S. Department of Homeland Security, December 17, 2003, at *http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm#1* (April 7, 2010).
2. U.S. Department of Homeland Security, "National Infrastructure Protection Plan: 2009," February 2009, p. 1, at *http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf* (April 8, 2010).
3. U.S. Department of Homeland Security, "Sector-Specific Plans," December 30, 2008, at *http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm#2* (April 8, 2010).
4. U.S. Department of Homeland Security, "More About the Office of Infrastructure Protection," December 23, 2008, at *http://www.dhs.gov/xabout/structure/gc_1189775491423.shtm* (April 8, 2010).

- defense industrial base (Department of Defense);
- energy (Department of Energy);
- government facilities (Department of Homeland Security);
- information technology (Department of Homeland Security);
- national monuments and icons (Department of the Interior);
- mail and shipping (Transportation Security Administration);
- public health and health care (Department of Health and Human Services);
- transportation systems (Transportation Security Administration, Coast Guard);
- drinking water and water treatment (Environmental Protection Agency);
- chemical sector (Department of Homeland Security);
- commercial facilities (Department of Homeland Security);
- critical manufacturing (Department of Homeland Security);
- dams (Department of Homeland Security);
- emergency services (Department of Homeland Security); and
- nuclear reactors, materials, and waste (Department of Homeland Security).

The above sectors work under their SSAs in partnership with their respective federal, state, and local governments, as well as with non-governmental and private agencies. Together, the NIPP base plan and its complementary sector-specific plans are meant to provide a unifying structure for integrating current and future CIKR protection efforts by the entire homeland security community, with a focus on developing and implementing effective operational measures within each individual sector.

Reviewing the Review. In order to reflect new developments among the evolving risks to U.S. critical infrastructure, the NIPP is reviewed and reissued by DHS every three years. Sector-specific plans are reviewed and addressed in the interim period between full updates. On February 17, 2009, DHS released the finalized version of the NIPP, completing the first triennial review process. Although the core NIPP principles and policies remain similar to those in the 2006 draft, the 2009 version did update the plan to incorporate major homeland-security-related developments, including updates to program elements and concepts during the past three years, the issuance of 18 SSPs, and a new 18th CIKR sector (critical manufacturing).[5]

In her first day in office, Secretary of Homeland Security Janet Napolitano issued five action directives, listing subjects about which she wanted to receive priority internal DHS reviews. Critical infrastructure protection was the first subject on the list, followed by risk analysis, state and local intelligence-sharing, and transportation security, also related to the NIPP.[6] Yet the Obama Administration has made only minor gains in terms of placing critical infrastructure protection and resiliency at the forefront of its policy agenda.

The burden is on DHS to continually develop CIKR protection from the ground up—resisting the urge to govern from the top down. The reason for this is twofold. First, principles of limited government call for an increased role for the private sector and state and local governments. Second, economic realities require solutions that achieve security goals but maintain the flexibility of the private sector to conform practices in the most cost-effective manner.

Managing Risk. In large part, DHS has been unable to resolve its challenges in critical infrastructure protection because it still lacks adequate tools to assess and manage risks. The level of the annual grants has been steadily falling—from $344 million (FY 2005), to half that total in FY 2006 and FY 2007, to under $49 million in FY 2008—highlighting the need for risk assessment to guide resource allocation. Despite increases in recent years, it is evident that each dollar must be used more effectively.[7]

5. U.S. Department of Homeland Security, "National Infrastructure Protection Plan: 2009."
6. Jonah Czerwinski, "Day One at DHS Starts with 5 Directives," Homeland Security Watch, January 22, 2009, at *http://www.hlswatch.com/2009/01/22/day-one-at-dhs-start-with-5-directives/* (April 8, 2010).

While the NIPP acknowledges that some degree of risk will always endure and rightly adopts an "all-hazards" approach toward protecting America's CIKR, the wide variety of threats to the myriad of potential targets means that it is impossible to protect every CIKR from every possible disruption. The current approach to critical infrastructure protection employed by DHS and its partners is inadequate for the following reasons:[8]

- **The complexity of infrastructure.** The infrastructure landscape is varied—spanning the non-tangible cyber domain to ports and roads and bridges. This means that there is no silver-bullet assessment of which steps are needed to protect a particular piece of infrastructure. DHS, however, has failed repeatedly to recognize this fact—and continues to give infrastructure the same weight of risk, and an equal distribution of resources. In fact, not all infrastructure is at risk to terrorism or natural disasters. That is why DHS's recommendation in the recently released Quadrennial Homeland Security Review to conduct a National Risk Assessment is a bad idea.[9] A National Risk Assessment simply does not make sense given the fact that the varied levels of risk in today's infrastructure make it nearly impossible to create a standardized computation of risk.
- **Criticality overuse.** The problem with the criticality designation is that it is often overused. Policymakers, uncomfortable about acknowledging that not all attacks or accidents can be prevented, turn to criticality as a crutch—pouring more and more resources into all infrastructure instead of tailoring dollars to those that are truly critical. Essentially, there is an incentive to deem infrastructure critical because of the resources that become available from such a designation. This is an inherent flaw in the NIPP, a framework which centers its approach on what it perceives as critical. Addressing this challenge will require a shared effort between the private sector and the federal government, as well as hard choices, to disaggregate what is "critical" (essential for sustaining and supporting Americans' daily lives) from what is "dangerous" (e.g., chemical facilities) but not necessarily critical.
- **Resiliency lip service**. Over the past few years, resiliency has become the term *du jour* of critical infrastructure policy. However, it is a term that has come to mean vastly different things to different people. All too often, resiliency has come to encompass an overly broad meaning of protecting the entire spectrum of critical infrastructure responsibilities. Resiliency should not be used as a term to indicate across-the-board spending on infrastructure protection or more guns, gates, and guards. The right definition is one that involves steps to increase the likelihood that *critical* infrastructure can continue to function or bounce back quickly despite a disruptive event. Improving the capacity of CIKR to rebound rapidly from terrorist attacks or natural disasters enhances the ability of critical assets to overcome disruptions and improves the overall efficiency of the American economy—and this should be the focus of critical infrastructure protection.[10]
- **Inadequate information-sharing channels**. Several factors have impeded the flow of information between public-sector and private-sector agencies engaged in information protection. Some private entities have expressed unease about the legal and regulatory consequences of providing governmental authorities with considerable data regarding their sensitive and proprietary critical infrastructure activities.[11]

7. U.S. Department of Homeland Security, "Fact Sheet: Critical Infrastructure and Homeland Security Protection Accomplishments," September 5, 2008, at *http://www.dhs.gov/xnews/releases/pr_1220878057557.shtm* (April 8, 2010).
8. *Ibid*.
9. U.S. Department of Homeland Security, "Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland," February 2010, p. 66, at *http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf* (April 8, 2010).
10. Jena Baker McNeill, "Building Infrastructure Resiliency: Private Sector Investment in Homeland Security," Heritage Foundation *Backgrounder* No. 2184, September 23, 2008, at *http://www.heritage.org/Research/Reports/2008/09/Building-Infrastructure-Resiliency-Private-Sector-Investment-in-Homeland-Security.*

Furthermore, company managers can be reluctant to share trade secrets and other information with industry partners that are also their competitors.[12] To address concerns about information security, DHS has adopted additional measures to restrict access to any data voluntarily provided by companies as well as guidelines limiting how public authorities can use that information. The Obama Administration, however, must further assess whether these steps have made sufficient progress in meeting private sector concerns—and how to best mitigate them.

- **Defining partnerships.** The NIPP employs a "top-down" model for CIKR protection, where partners exchange data, assessments, best practices, and other information at multiple levels.[13] These networks embrace many actors, but perhaps the most important are those between the diverse public-sector and private-sector entities involved in each sector. According to DHS, more than 700 public-sector and private-sector entities, 300 more than when the 2006 NIPP was issued, are now members of a NIPP Sector Partnership, which consists of the 18 sector-coordinating councils (SCCs), each with a government coordinating council (GCC) for their respective sector.[14]

  These public–private partnerships are essential to CIKR protection since the private sector owns and manages an estimated 85 percent of all critical infrastructure in the United States.[15] Private actors are, therefore, best positioned to determine and implement risk-mitigation strategies to reducing the vulnerability of the CIKRs they own and operate to various disruptions. Yet, government agencies can contribute essential resources to CIKR protection and are also well positioned to address threats. For example, they possess unique intelligence on foreign terrorist threats against U.S.-based assets. Likewise, partnerships can also serve to enhance the credibility of SSPs with potential business users by ensuring that the guidelines are written with the input of the individuals who work in or with the relevant commercial sector, and therefore understand its capabilities and vulnerabilities.[16] These institutions, however, need a better idea of the roles and responsibilities of both the private sector and the federal government—including vulnerability assessments, determining criticality, and other activities involved in critical infrastructure protection.
- **Facing evolving threats**. When DHS issued the SSPs for the then 17 sectors in December 2007, department leaders stressed that these plans were not finished products, but rather living documents meant to provide a general framework for future planning. However, part of changing in the face of new threats means developing an accurate picture of risk, and the NIPP is not agile enough to do so. The NIPP has made some changes, including the addition of a "critical manufacturing" sector and CIKR mission integration within state and local fusion centers; expansion of CIKR protection-related education, training, outreach, and exercise programs; and an examination of how adversaries can use CIKR as weapons of mass destruction—however, these efforts still fail to interweave risk as the litmus

11. U.S. Government Accountability Office, "Critical Infrastructure Protection: Sector-Specific Plans' Coverage of Key Cyber Security Elements Varies," GAO-08-113, October 2007, at *http://www.gao.gov/new.items/d08113.pdf* (April 8, 2010).
12. Information Sharing Environment, "Information Sharing Environment Implementation Plan," November 2006, p. 75, at *http://ise.gov/docs/ise-impplan-200611.pdf* (February 16, 2010).
13. U.S. Department of Homeland Security, "National Infrastructure Protection Plan: 2009."
14. Elizabeth Newell, "News+Analysis Critical Alliance," GovernmentExecutive.com, October 1, 2009, at *http://www.govexec.com/features/1009-01/1009-01na2.htm* (April 8, 2010).
15. U.S. Department of Homeland Security, "Critical Infrastructure Sector Partnership," at *http://www.dhs.gov/xprevprot/partnerships/editorial_0206.shtm* (April 26, 2010).
16. Press release, "Remarks by Secretary Michael Chertoff at a U.S. Chamber Event on the Completion of the 17 Sector Specific Plans, as Part of the National Infrastructure Protection Plan," U.S. Department of Homeland Security, May 21, 2007, at *http://www.dhs.gov/xnews/speeches/sp_1179843074582.shtm* (April 8, 2010).

test for change—instead reverting to a stove-pipe system of criticality.

The Administration must seek ways in which to better examine risk. When something becomes a new threat—the system must be able to change dynamically to accommodate this development. An example of this problem is in relation to cyber networks. The cyber domain has proven to be a major threat to infrastructure in that networks are in themselves infrastructure but also other infrastructure relies on cyber networks to operate. As the 2009 NIPP observes, "Cyber infrastructure enables all sectors' functions and services, resulting in a highly interconnected and interdependent global network of CIKR."[17] This shows the need to enhance the security of electronic information and communications systems, including the data they store and distribute. But to do so adequately—critical infrastructure protection will need to adapt to the increased risk as well as change to accommodate the unique nature of the cyber domain.

Deciding how to grow and adapt to evolving threats is fundamentally a product of sound risk-assessment methods, something that neither Congress nor DHS has interwoven sufficiently in the law or policymaking process.

Fundamental Problems

The more fundamental problem of critical infrastructure protection goes back even further to the process of lawmaking. All too often Congress has relied on its own perceptions of risk and how to mitigate risk without any type of risk-based assessment. This biased risk perception, often influenced by politics and other non-security-related aims, as well as the need to "look good" on security, often creates failed policies. An example is cargo security. The 100 percent maritime security mandate was touted by Members of Congress as a means by which to protect ports and other maritime infrastructure from a nuclear bomb in a cargo container. Congress mandated that 100 percent of the maritime cargo coming into the United States undergo radiological scanning. Congress did this, however, without an accurate picture of whether this scenario was actually a credible threat to the industry. In practice, politics drove most of the debate on this measure—and Congress decided it was a problem that must be resolved without any hard data to back its claims. Legislating on imagination, as opposed to risk, has all too often led to costly, economically crippling measures, such as the 100 percent scanning mandate, that do little to add to the security of the nation.

Without resolving these challenges, it will be difficult for the Administration to make any real progress toward building an effective national enterprise capable of handling tangible threats to truly critical infrastructure.

Rethinking NIPP

Congress should remove itself from the business of dictating risk and setting standards for critical infrastructure based on ideas that are wholly unrelated to actual security. Protectors of U.S. national infrastructure and the Administration—in partnership with Congress, the private sector, and diverse state and local actors—should:

- **Emphasize the catastrophic.** DHS has recently established two tiers of CIKR, which attempt to distinguish higher risk infrastructure from those associated with less risk. This is a good step, but DHS needs to go further. National CIKR protection, recovery, and resilience efforts should focus on protecting those assets whose disruption could inflict the most catastrophic human or financial losses. Secretary Napolitano made improving DHS efficiency one of her priorities, but focusing critical infrastructure dollars on all assets, as opposed to the most at risk, does not align with this goal. For instance, it is imperative that electric utilities across the United States be protected from terrorist attacks and natural disasters. The destruction of electric utilities would be catastrophic for the nation—and the ability of the grid to bounce back quickly is of utmost importance. On the other hand, infrastructure that does not deal with the immediate survival of the population, such as rail facili-

17. U.S. Department of Homeland Security, "National Infrastructure Protection Plan: 2009," p. 12.

ties, require fewer critical infrastructure resources and less attention. The question that needs to be asked is whether a particular piece of infrastructure is essential for sustaining and supporting the daily lives of Americans.

- **Accelerate resiliency enhancements.** Further efforts to facilitate the timely restoration of essential CIKR following an intentional or natural disaster are warranted. Having quality infrastructure provides a firm foundation for rebounding from a catastrophe. The government should encourage the private sector, which owns most infrastructure, to invest in quality. The federal government could offer additional incentives to promote private-sector protection and resiliency efforts, such as establishing a public recognition program for firms that achieve noteworthy success, or granting CIKR-supportive companies preference in federal contracting or simply promoting the SAFETY Act—which provides liability protection from terrorist acts for companies that develop anti-terrorism technologies. Such technologies can include those used in critical infrastructure protection. At a fundamental level, providing clear transparency and legal protections on information-sharing and innovation would be excellent first steps.

  Successfully focusing businesses on resiliency enhancements could have the dual effect of improving the efficiency of business operations under normal as well as under emergency conditions. If a private-sector company makes investments in improving the quality of its cyber networks, these enhancements can also help the company conduct business more efficiently, helping to decrease financial loss and improve customer confidence in their network and data quality.

- **Keep small and medium-sized businesses in mind.** Infrastructure-protection programs need to focus more on reaching out to small and medium-sized businesses, given their vital importance in many CIKR sectors as well as their unique vulnerabilities. The workers and the companies served by these businesses are the backbone of the U.S. economy; in a disaster, they are also the most vulnerable.[18] Small enterprises usually have one location and generally do not have back-up plans, nor do they store files, records, or other critical data off site. FEMA has started to address this issue through its Ready Business initiative mentorship program—which pairs larger private-sector companies with smaller businesses.[19] Although DHS recommends that the sector-coordinating councils include small-scale owners and operators of CIKR, these appear to be underrepresented in the SCCs and other NIPP information-sharing and idea-sharing mechanisms, threatening to lead CIKR policymakers to neglect their distinct concerns and needs. It is good that DHS is beginning to address small and medium businesses since these entities make up half of the American workforce—however, greater efforts are needed.

- **Broaden education, awareness, and training.** Further progress must be achieved in promoting the skills of the security professionals engaged in protecting America's critical infrastructure. For example, the Administration and Congress should further promote the National Security Professional Development process to improve the human capital resources of federal homeland security leaders supporting critical homeland security missions, such as CIP, while DHS simultaneously enhances efforts to establish a national network of critical infrastructure training and education programs.[20]

- **Get oversight right.** One of the major reasons why Congress often seems to enact ineffective critical infrastructure legislation is because of its current oversight system. At least 86 different

18. James Jay Carafano, "Homeland Security's Blind Spot," *The Washington Examiner*, September 14, 2009, at *http://www.washingtonexaminer.com/opinion/columns/Homeland-Security_s-blind-spot-8237821-59175902.html* (April 8, 2010).
19. Federal Emergency Management Agency, "Ready Business Mentoring Guide," April 25, 2006, at *http://www.ready.gov/business/_downloads/mentor_guide.pdf* (April 8, 2010).
20. James Jay Carafano, "Missing Pieces in Homeland Security: Interagency Education, Assignments, and Professional Accreditation," Heritage Foundation *Executive Memorandum* No. 1013, October 16, 2006, at *http://www.heritage.org/Research/HomelandSecurity/em1013.cfm.*

subcommittees and committees have some form of oversight over the Department of Homeland Security—creating a daunting number of committees with jurisdiction over critical infrastructure matters. Few Members of Congress have detailed knowledge of homeland security and critical infrastructure protection issues despite being tasked with legislating on these very matters.[21] The result is that policies often reflect the political priorities of the Member rather than genuine national needs. For this reason, Congress must consolidate oversight of homeland security into four committees, two in the Senate and two in the House. Simultaneously, Congress needs to develop an "in-house" way to examine risk and threats to the nation based on scientifically acceptable risk methodologies. Something similar to a Congressional Budget Office for risk-assessment would be highly useful as Congress examines security-related regulatory schemes in order to avoid politics and the tendency of Members to create risk where there is none.

- **Promote CIKR-related research**. When it comes to research, a vital part of critical infrastructure protection, private-sector leaders have more flexibility and free-market incentive to experiment than their federal counterparts, whose actions are typically more constrained by legislative restrictions, public expectations, and other factors. In fact, the DHS budget request for FY 2011 cuts science and technology spending for almost all of its research areas.[22] Dealing with federal budget realities means that agencies should foster a favorable environment for private-sector innovation. Doing so should include promotion of the SAFETY Act, which encourages private-sector companies to invest in anti-terrorism technologies.

  One specific area of critical infrastructure protection that needs to be researched further is "complex systems." Infrastructure is highly complex, and it is vital that both the government and the private sector understand how systems perform and work. "When systems become overly complex, their behavior cannot be easily predicted by traditional methods of analysis," such as examining a system's individual components and aggregating their effects. Furthermore, "[i]n a complex system, elements are [often] so interconnected and their relationship so multifaceted that their properties cannot be properly understood without assessing their interrelationship with each other as well as their relationship with the wider system and its environment." Since complex systems are difficult to analyze, understanding how they work, predicting their behavior, or determining the optimum means for changing their performance presents a unique challenge that should be carefully explored.

- **Consider cooperative agreements**. The U.S. government's grant structure has proven to be the wrong tool for increasing preparedness, response, and recovery capabilities outside the federal government. The main reason for this is that the current grant system "does not foresee substantial federal involvement when in fact DHS is integrally involved [in the process]—from issuing requirements to unfunded mandates to requiring yearly applications for funds."[23] It may be time for DHS and Congress to acknowledge that "a better approach to improving capabilities at the state and local level through the federal apparatus would be the use of cooperative agreements."[24] A cooperative agreement is where the federal government and the states and localities function as "true and

21. Jena Baker McNeill, "Congressional Oversight of Homeland Security in Dire Need of Overhaul," Heritage Foundation *Backgrounder* No. 2161, July 14, 2008, at *http://www.heritage.org/Research/Reports/2008/07/Congressional-Oversight-of-Homeland-Security-in-Dire-Need-of-Overhaul*.
22. Jena Baker McNeill, "The FY 2011 Homeland Security Budget: Spending Doesn't Match the Missions," Heritage Foundation *Backgrounder* No. 2376, February 26, 2010, at *http://www.heritage.org/Research/HomelandSecurity/bg2376.cfm*.
23. Jena Baker McNeill, James Jay Carafano, and Matt A. Mayer, "Eight Years After 9/11: Analyzing Congress's Homeland Security Agenda," Heritage Foundation *WebMemo* No. 2608, September 9, 2009, at *http://www.heritage.org/Research/HomelandSecurity/wm2608.cfm*.
24. *Ibid*.

equal partners and negotiate outcomes at the beginning, including covering programmatic and financial oversight requirements, and then direct funds to achieve those desired outcomes without the need for yearly applications."[25] This would also take the politics out of the process and help improve the ability of state and local governments to respond to disaster.

- **Secure global supply chains.** In partnership with foreign governments and the international business community, DHS should bolster its Critical Foreign Dependencies Initiative—which seeks to identify international CIKRs vital to the functioning of the American economy—and increase its efforts to strengthen the resiliency of key global commercial networks.[26] U.S. officials could use the World Customs Organization and related institutions to launch further initiatives, such as the SAFE Framework and the International Shipping and Port Facility Security (ISPS) Code, to develop more and stronger mechanisms to secure key components of the global infrastructure. Additionally, the United States can work with select foreign governments to develop international liability protection regimes in the model of the U.S. SAFETY Act protections to encourage global use of the most effective counterterrorist tools regardless of their origin.[27]

Conclusion

The NIPP can provide a vital tool for promoting successful critical infrastructure protection. Congress can make a valuable contribution by promoting a sound risk methodology and policies focused on keeping Americans free, safe, and prosperous.

*—**Jena Baker McNeill** is Policy Analyst for Homeland Security in the Douglas and Sarah Allison Center for Foreign Policy Studies, a division of the Kathryn and Shelby Cullom Davis Institute for International Studies, at The Heritage Foundation. **Richard Weitz**, Ph.D., is Senior Fellow and Director of the Center for Political–Military Analysis at Hudson Institute.*

25. *Ibid.*
26. U.S. Department of Homeland Security, "Fact Sheet: Critical Infrastructure and Homeland Security Protection Accomplishments."
27. Jena Baker McNeill, "The SAFETY Act," Heritage Foundation *WebMemo* No. 2490, June 17, 2009, at *http://www.heritage.org/Research/HomelandSecurity/wm2490.cfm.*