Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress

John D. Moteff
Specialist in Science and Technology Policy

August 23, 2012

Congressional Research Service
7-5700
www.crs.gov
R42683

CRS Report for Congress
Prepared for Members and Committees of Congress

Summary

In 2006, the Critical Infrastructure Task Force of the Homeland Security Advisory Council initiated a public policy debate arguing that the government's critical infrastructure policies were focused too much on protecting assets from terrorist attacks and not focused enough on improving the resilience of assets against a variety of threats. According to the Task Force, such a defensive posture was "brittle." Not all possible targets could be protected and adversaries could find ways to defeat defenses, still leaving the nation having to deal with the consequences. The Task Force advocated that greater encouragement for resilience would broaden the range of risk reduction options and should be the overarching policy framework for reducing risks associated with all threats to critical infrastructure. Others in the homeland security community agreed.

Critical infrastructure are those assets the loss of which would result in great harm to the nation's security, economy, health and safety, and morale. They include assets necessary to generate and distribute such basic goods and services such as electricity, drinking water, telecommunications, banking and finance, etc. Resilience refers to the ability of a system to resist, absorb, recover from, or successfully adapt to a change in environment or conditions. The Task Force argued that government policies encouraged employing greater defenses such as surveillance equipment, guards, etc., around these assets but did less to encourage efforts that would allow assets to continue operating at some level, or quickly return to full operation, if attacked. Such efforts might include increasing redundancies (such as having multiple backup power generation capability) or designing more robust systems for the future (such as using more hardened concrete for stronger fixed facilities).

In 2008, as part of its oversight function, the House Committee on Homeland Security held a series of hearings addressing resilience. At those hearings, the Department of Homeland Security (DHS) argued that government policies and actions did encourage resilience as well as protection. Even so, subsequent policy documents made greater reference to resilience. At first those references were relatively superficial, but later they became more substantive. Policy has evolved to the point that resilience and protection of critical infrastructure assets are recognized as distinct options to be equally considered when seeking to reduce the risks associated with potential attacks on critical infrastructures.

As policy has evolved, programs have also evolved somewhat, to support efforts at improving critical infrastructure resiliency. The Office of Infrastructure Protection within the DHS conducts risk assessments at the asset and regional level that now include a resilience index along with a protection index. The program allows asset owners/operators to compare their level of resilience to other similar assets and allows them to analyze how certain improvements might contribute to better resilience. Also, the DHS Science and Technology Directorate supports some resilience-oriented research and development projects. In addition to projects developing better technologies to aid in response and recovery, the Directorate also supports projects that are developing technologies for structures to withstand blasts or large physical displacements or systems which can self-heal after being damaged.

The Federal Emergency Management Agency within DHS provides grants, primarily to state and local governments or public authorities, that largely support resilience by improving the ability to respond to and recover from incidents. Mitigation grants, which allow communities to reduce the potential consequences of an incident before it happens, offer limited support for improving the resilience of critical infrastructures. There is relatively little direct government support or

incentives for private sector owners/operators to implement resilience-oriented (or protective-oriented) measures. It is not clear if market incentives are sufficient to drive such investments. Congress may choose to consider the adequacy of private investments in resilience, whether the private market provides sufficient incentives, and options for government action if markets do not.

Contents

Figures

Contacts

Introduction

This report discusses the concept of resilience in the context of critical infrastructure and homeland security. It also identifies and discusses issues related to the evolution of policy and programs at the Department of Homeland Security (DHS) that are meant to, or could, promote the resiliency of the nation's critical infrastructure. The purpose of the report is to aid Congress in its oversight of critical infrastructure programs and activities at DHS.

The U.S. PATRIOT Act (P.L. 107-56, Sec. 1016(e)) defined critical infrastructure as:

> systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.[1]

DHS has identified 18 sectors of the economy that they believe possess such systems and assets.[2] Among these are electric power generation and distribution, drinking water, communications and information systems, oil and gas production and distribution, transportation systems, and banking and finance.[3]

DHS's 2009 *National Infrastructure Protection Plan* defined resilience as "the ability to resist, absorb, recover from, or successfully adapt to adversity or a change in conditions."[4] In a homeland security context, a change of conditions implies a terrorist attack, a natural hazard, such as hurricane or earthquake, or a technological failure, such as a dam collapse or a serious accident at a nuclear power plant.

Reducing the potential risks associated with the loss of critical infrastructure resulting from a terrorist, natural hazard, or technological disaster (hereinafter referred to collectively as all-hazard events) is a key element in the nation's homeland security strategy and a topic of continued interest in Congress.[5] To the extent that resilience can contribute to reducing that risk, Congressional interest extends to the policies and programs associated with promoting resilience.

[1] This definition has been adopted by Congress in a number of other statutes, such as the Defense Production Act (50 USC App 2152 (2)) and Homeland Security Act 2002 (6 USC 101).

[2] The 2009 *National Infrastructure Protection Plan* defines "asset" as a person, structure, facility, information, material, or process that has value. It defines "system" as any combination of facilities, equipment, personnel, procedures, and communications integrated for a specific purpose.

[3] A full list of sectors can be found at http://www.dhs.gov/files/programs/gc_1189168948944.shtm.

[4] Department of Homeland Security, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*, 2009, p. 111.

[5] In May of 2008, the House Committee on Homeland Security held a series of hearing focusing on resilience as a organizing principle for homeland security activities, in general, and critical infrastructure activities, in particular. In March 2010, the Government Accountability Office released a follow-up study for the Committee addressing similar issues. See, U.S. Government Accountability Office, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296, March 2010. In the 112th Congress, Senators Lieberman and Collins introduced a bill (S. 1546) that would, in effect, rename the National Protection and Programs Directorate (NPPD) as the Infrastructure and Resilience Directorate and Representative King introduced a bill (H.R. 3116) that would establish a Rural Resilience Initiative.

This report focuses on the resilience of critical infrastructure. The resilience of a community, a region, or the nation as a whole is also important to homeland security, and depends in part on the resilience of critical infrastructure, but also involves a broader range of elements, behaviors, and social-economic relationships that are beyond the scope of this report.[6]

Background

Defining Resilience

The Merriam-Webster dictionary defines resilience as "the ability to recover from or adjust easily to misfortune or change."

Researchers in different fields, including psychology, economics, ecology, and highly complex engineering systems have sought to apply this concept to the systems they study.[7] Beginning in the 1990s, researchers and policymakers studying earthquakes and earthquake policy began applying the term to communities and their vital infrastructures (water, electricity, transportation, etc., also referred to as lifelines) as they looked for ways to mitigate the impact from earthquakes.[8] Moved by efforts to look at homeland security from an all-hazard perspective, and informed largely by the modeling ideas from the earthquake community, researchers and policy analysts are now considering the concept in terms of reducing the risks associated with the disruption of critical infrastructure operations resulting from terrorist attacks.

There are almost as many definitions of resilience as there are people defining it. Most definitions, if not all, assume a change in the system's normal operating environment that has the potential, if not the effect, of disrupting normal system performance.[9] Many definitions of resilience assume a momentary disruption or loss in performance followed by a quick recovery to normal system performance. Some definitions also include the ability of a system to continue operating during changing conditions, if only at a diminished level, or where system performance drops gradually as opposed to precipitously.[10] Still other definitions include the ability of a system to adapt to changed conditions.[11] In other words, the change in the operating environment may be long lasting and the system has adapted to perform at an acceptable or sustainable level.

[6] For example, community resilience would include finding families housing, children classrooms, local businesses places to operate, in order to maintain some semblance of "normal life" while recovering from an event. Such efforts go beyond keeping the electricity and water flowing.

[7] See, Christine Pommerening, "Resilience in Organizations and Systems: Background and Trajectories of an Emerging Paradigm," Critical Infrastructure Program, George Mason University, in *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, (February 2007). See also, Kathryn A. Foster, "A Case Study Approach to Understanding Regional Resilience," Institute of Urban and Regional Development, University of California, Berkeley, Working Paper 2007-08 (November 2006).

[8] For example, see Michel Bruneau et al., "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," *Earthquake Spectra*, vol. 19, no. 4 (November 2003).

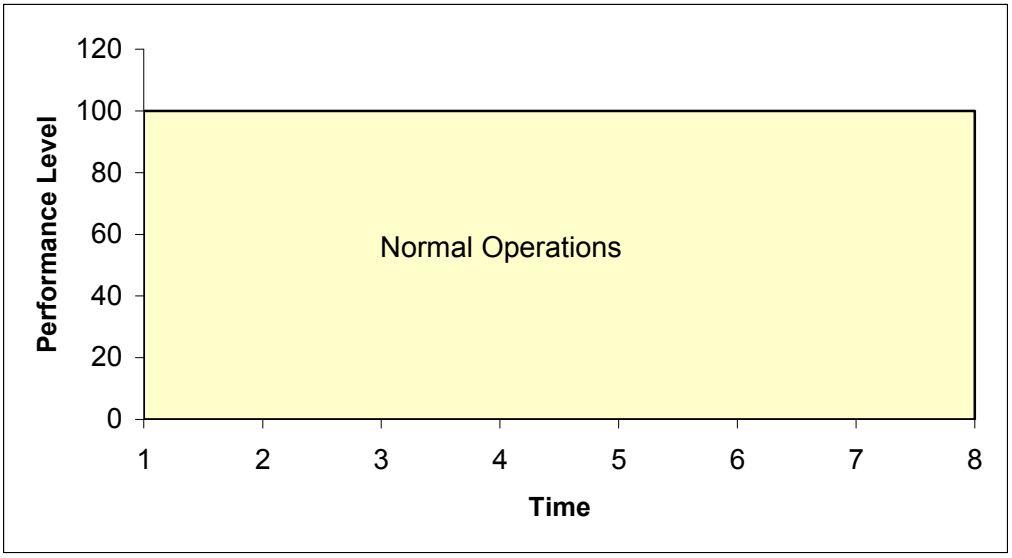
[9] A system could be an engineering system, such as an electric power plant, a community, or an organization. This report focuses on the technical system and the organization that operates and supports it.

[10] Brad Allenby and Jonathan Fink, "Toward Inherently Secure and Resilient Societies," *Science*, vol. 309, no. 5737 (August 12, 2005).

[11] W. Neil Adger et al., "Social-Ecological Resilience to Coastal Disasters," *Science*, vol. 309, no. 5737 (August 12, 2005).

Resilience can be depicted as in the following figures.[12]

Figure 1. Generic System Operations Under Normal Conditions



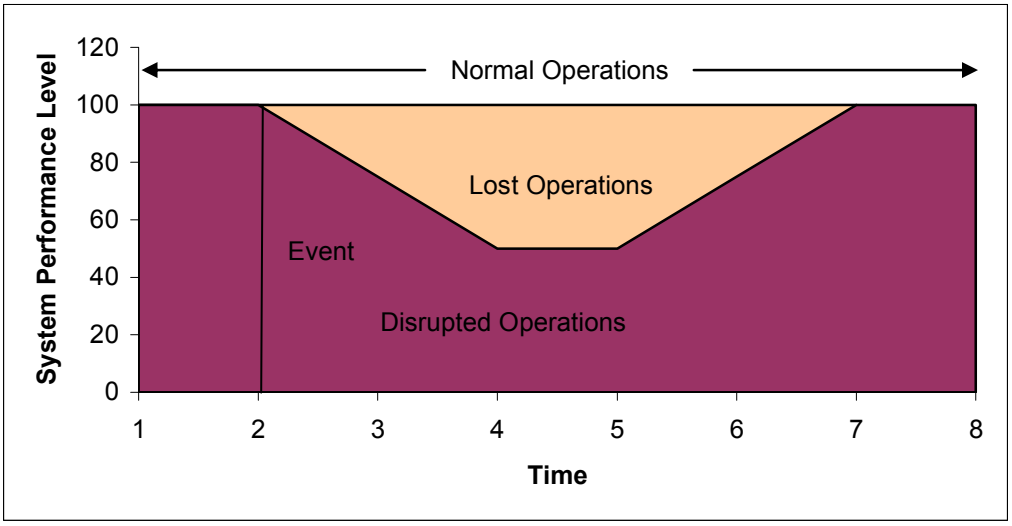
Source: CRS.

Figure 1 depicts the normal operation of, say, System A. System A could be a community's public drinking water system, a regional electric power grid, or, perhaps, the national railroad system. Performance can be measured in many different ways. For example, it could be measured in terms of the number of households beings served, the power being generated within an electric grid, the tonnage of freight moving through the rail system, or the revenue generated by normal system operations. Time can be measured in terms of seconds, or less; years, or longer. For illustrative purposes, the performance of System A in **Figure 1** is measured in dimensionless units over some dimensionless time period. In this case, System A performs at a constant 100 units over the entire time period during normal operations.

The darker area in **Figure 2** depicts the performance of System A resulting from a disrupting event, say a flood, at Time = 2. Performance drops steadily over time, levels off at 60 units, and then, say through recovery efforts, regains normal performance of 100 by Time = 7. The lighter area represents the loss of operations during that time.

[12] While the following discussion is original to this report, the basic model expressed in the figures has been well established. See, Michel Bruneau, et al., op. cit. Also, Eric D. Vugrin, Drake E. Warren, and Mark A. Ehlen, "A Resilience Assessment Framework for Infrastructure and Economic Systems: Quantitative and Qualitative Resilience Analysis of Petrochemical Supply Chains to a Hurricane," Prepared for Presentation at American Institute of Chemical Engineers, 6th Global Congress on Process Safety, San Antonio, TX, March 22-24, 2010. A more thorough analysis of similar resilience profiles can be found in Homeland Security Studies and Analysis Institute, *Risk and Resilience: Exploring the Relationship*, Arlington, VA, November 22, 2010.

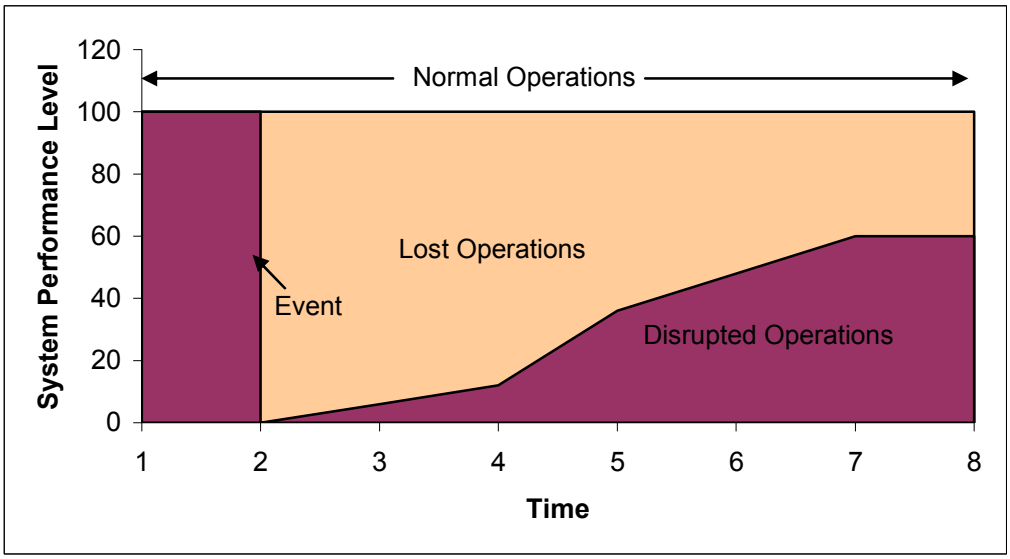
Figure 2. Generic System Operations After an Event, Scenario A



Source: CRS.

Figure 3 could depict the performance of System A resulting from a different disrupting event, say an earthquake or terrorist truck bomb, or it could represent the reaction of a different system, System B, to the same event assumed in **Figure 2**. In either case, the system fails abruptly, performance drops to 0, gradually recovers some of its performance, but does not return to the original performance level in the time recorded.

Figure 3. Generic System Operations After an Event, Scenario B



Source: CRS.

By most definitions, the system in scenario B (**Figure 3**) would be considered less resilient than the system in scenario A (**Figure 2**).

Measuring Resilience

Just as there is no standard definition of resilience, there is no standard measure of resilience.[13] One measure could be the amount of time it takes to recover fully to normal operations. The quicker the recovery, the more resilient the system. Another measure could be in terms of total loss of performance. For example, in Figures 2 and 3, the difference between normal operations and the interrupted performance equals the loss of performance during the disruption. Reducing the total loss of performance increases resilience. This approach not only captures the amount of time it takes to recover, but also the initial reaction to the disrupting event, including whether the initial reaction was a precipitous drop in performance or a gradual one, and whether the system continued to function at some level or was put out of operation completely.

How one measures resilience may depend on what policymakers consider most relevant to their decisionmaking. If monetary losses are important, it may be more appropriate to measure the total (or net) loss of revenue associated with the disruption. If, however, policymakers are more concerned about how long it takes to get their constituents' power back on, then simply measuring time to full recovery may be appropriate.

Resilience Enhancing Actions

The resilience of an asset or system can be improved in a number of ways.

Adding redundancies to the asset or system can improve resilience by being able to reroute production or process flows through one or more parallel components or subsystems. The internet is resilient because information packets can reach their destination by any number of routes: lose the use of a few routers, and messages continue to flow; lose a lot of routers and information may still continue to flow, albeit at a slower rate. Another simple example might be a firm or a sector (e.g. oil refining) that has multiple production facilities. If one or more of those production facilities were to shut down, firms may be able to increase production at the others.

Having back-up components available can also improve resilience by being able to quickly replace a component or asset whose function is disrupted. A prime example are mobile communication assets that can be driven to locations where fixed assets have been lost or disrupted. A key strategy for improving the resilience of electric power distribution is to have sufficiently sized and available back-up transformers that can be transported where needed.

Substitution can improve resilience by allowing a process to switch from one input or component to another, perhaps with slightly different properties but without major impact on the final product or process. For example, some industrial burners used to produce heat, may be able to switch from one fuel to another, or one grade of fuel to another. Materials often can be substituted for one another. For example, various copper and aluminum alloys can sometimes be used to make similar products.

[13] Michel Bruneau and others at the Multidisciplinary Center for Earthquake Engineering Research have developed a framework, cited by many others, for measuring resilience that considers the following "properties" (robustness, redundancy, resourcefulness, and rapidity) and the following "dimensions" (technical, organizational, social, and economic). See Michel Bruneau, op. cit.

Products and processes can also be redesigned to reduce or eliminate their vulnerabilities to specific threats. For example, new construction in earthquake-prone regions are increasingly using designs that can dampen the forces induced by earthquakes and improve the chances of those assets or facilities to remain standing or even functional. In some cases, processes could be redesigned to use less hazardous inputs to reduce the potential of hazardous releases of those substances during a terrorist attack or natural event.

Resilience may also depend on the ability to improvise during a disruptive event, perhaps by re-engineering processes in real-time or making do with materials and assets at hand. The specific actions one might take may be difficult to plan for ahead of time. However, having a detailed understanding of how an asset or system operates, and perhaps conducting exercises where improvising is practiced, could improve the ability to respond creatively to unique situations.

The resilience of a critical infrastructure asset could also be enhanced by giving it priority access to scarce critical resources, thereby maintaining its services or getting its services back on-line more quickly to aid in a more general community recovery.

Many discussions regarding resilience of critical infrastructure stress the importance of modeling system operations, including the system's interdependencies with other systems beyond the immediate control of operators, assessing vulnerabilities, and contingency planning. Planning (i.e., preparedness) is particularly important if one is using back-up systems or substitution to help respond to events. Knowing what and where back-up systems are located and how to transport them to the needed locations, or identifying and having ready alternate sources of materials is important.

Applying these various options may cost money and may not provide the best efficiencies under normal circumstances. However, in some cases they may add efficiencies to normal operations. To a large extent, the financial feasibility of these various resiliency enhancing options depends on the risks a firm, or community, or the nation is willing to accept.[14]

Resilience and Risk

According to the 2010 *Quadrennial Homeland Security Review Report*, "Ultimately homeland security is about effectively managing risks to the Nation's security."[15] DHS defines risk as:

> The potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences.[16]

Put another way, risk can be thought of as the consequences associated with an event, discounted by the probability of that event occurring.[17]

[14] Time and the discounting of future costs and potential benefits, affects this decision.

[15] Department of Homeland Security, *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*, February 2010, p. 2.

[16] Department of Homeland Security, *DHS Risk Lexicon*, 2010 Edition, September 2010, p. 27.

[17] An event with potentially large consequences, but with relatively low probability of occurring, may have associated with it the same level of risk as a more probable event, but with lower consequences.

The 2009 *National Infrastructure Protection Plan* provides a framework for assessing and managing the risk associated with the loss of critical infrastructure. According to the NIPP,

> Risk is influenced by the nature and magnitude of a threat, the vulnerabilities to that threat, and the consequences that could result.[18]

Put into a general formula, risk is a function of threat (t), vulnerability (v), and consequences (c):[19]

$$\text{Risk} = f(t,v,c)$$

To reduce risk, the nation can try to reduce any one, any combination, or all three of the variables. Improving resiliency reduces risk primarily by reducing the vulnerability to and potential consequences of an attack or natural event. A building or overpass designed or modified to absorb the physical displacements caused by an earthquake may prevent the asset from falling, reducing loss of nearby property and life. Building a house on stilts and having access to some sort of water craft might allow residents more time to evacuate or even to stay in their homes during a flood, resulting in less loss of life and property. Stockpiling materials or food in safe locations may speed recovery and reduce the total consequences associated with an all-hazards event.

Policy

Homeland Security Council—Critical Infrastructure Task Force: Protection Versus Resilience

According to Homeland Security Presidential Direction 7 (HSPD 7),

> It is the policy of the United States to enhance the protection of our Nation's critical infrastructure....[20]

In January 2006, the Critical Infrastructure Task Force of the Homeland Security Council published a report that concluded:

> Given the diverse spectrum of potential threats [to the nation's critical infrastructure], coupled with the reality that resources are limited, policies and strategies focusing on achieving resilience would be more robust than current guidance, which focuses primarily on protection.[21]

[18] Department of Homeland Security, National Infrastructure Protection Plan: Partnering to enhance protection and resiliency, 2009, p. 27.

[19] This is primarily a notional formula. To derive a specific quantitative formula or set of formulae, particularly for the case of a terrorist attack, is made difficult by uncertainties involved (especially uncertainties regarding threat) and the potential interdependencies of the variables. For example, the threat, often described in part by the likelihood that a particular attack would occur, might be dependent on the both the vulnerability of the target and the likely consequences.

[20] Homeland Security Presidential Directive/ HSPD-7. *Critical Infrastructure Identification, Prioritization, and Protection.* December 17, 2003. Paragraph 7.

[21] Homeland Security Advisory Council. *Report of the Critical Infrastructure Task Force*. January 2006. Executive (continued...)

Among the Task Force recommendations were:

> promulgate critical infrastructure resilience as the top-level strategic objective … to drive national policy and planning … [and] … align policy and implementation directives for risk-based decisionmaking with the critical infrastructure resilience objective.…[22]

The Task Force pointed out that HSPD 7 and other high level DHS strategy and guidance documents concerning critical infrastructure repeatedly identified "protection" as the key factor driving the national effort.[23] Citing the Merriam-Webster dictionary definition of "protect" as: "to cover or shield from exposure, injury, or destruction," and HSPD-7, which stated that "to protect means reducing the vulnerability of critical infrastructure … in order to deter, mitigate, or neutralize terrorist attack,"[24] the Task Force concluded that the strategy and guidance biased action toward defensive measures.

The Task Force asserted, however, that it would not be possible to protect all possible targets against every conceivable threat, nor would it be possible to eliminate all vulnerabilities. The Task Force concluded that a strategy based on protection, in isolation, would be brittle and insufficient.[25]

The Task Force proposed that a strategy based on resilience would foster consideration of a broader range of options to help reduce the risks associated with the loss of critical infrastructure. The Task Force did not suggest that resilience replace protection efforts, but that resilience offered an overarching strategy that included protection, preparedness, and efforts to prevent attacks from happening.[26]

The Task Force also argued that owners and operators of critical infrastructure could make a better business case for investing in resilience, measured in terms of the amount of time and effort needed to restore operations, than trying to justify investments to increase protection or reduce vulnerabilities, which, according to the Task Force, are more difficult to quantify.[27]

Other organizations and individuals followed with similar statements calling for a greater emphasis on resilience in addressing both critical infrastructure security and/or, more broadly, homeland security.

The Reform Institute stated:

(...continued)

Summary. pg. iii.

[22] Ibid. pp. iii and iv.

[23] The Task Force referred to the National Strategy for Homeland Security, the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets, the National Strategy for Securing Cyberspace, Homeland Security Presidential Directives 7 and 8 (since superseded) and the National Infrastructure Protection Plan. Note: HSPD-8 has since been replaced by PDD-8 (March 2011). HSPD-7 has been under review.

[24] Homeland Security Presidential Directive/ HSPD-7. *Critical Infrastructure Identification, Prioritization, and Protection.* December 17, 2003. Paragraph 6(h).

[25] Homeland Security Advisory Council. Op Cit. p. 4.

[26] The Task Force also stated that "preparedness, like protection, is necessary but insufficient for achieving resilience." This perhaps reflects the broader characterization of resilience that includes the ability of the system to continue functioning to some degree after being attacked rather than just how quickly the system can recover.

[27] The Task Force did not elaborate on this argument.

> The simple fact is that not all hazards can be averted … devastating incidents will occur. What is within our power … is to better prepare our nation and its critical infrastructure to absorb the blows of catastrophe in order to prevent them from seriously disrupting critical activities.… Placing resilience at the heart of our homeland security policy will bring much-needed overarching focus to the work of government agencies.…[28]

James Carafano struck similar themes:

> The U.S. government must shift from unrealistic strategies that emphasize protecting infrastructure to strategies that focus on resiliency. Spending billions to protect infrastructure still leaves the nation vulnerable. Resiliency promises to sustain society in the face of known threats and unexpected disasters.[29]

Brian Jackson at RAND discussed the weaknesses associated with a strategy based solely on traditional "preventive" efforts.[30] According to Jackson, traditional preventive efforts include detecting and halting or disrupting an attack, before damage can be done (similar to the Task Force's discussion of "protection"). Jackson argued that there are inherent uncertainties associated with terrorist attacks that present particular problems for preventative efforts. Uncertainties include identifying which individuals are threats, what types of weapons to look for, and which assets the terrorist group may target. The adversary can also take countermeasures to avoid defenses put in place. Jackson also argued that addressing threats in a preventative manner can lead to a layering of security measures for each new realized threat. Jackson asserted that such layering cannot be sustained indefinitely and that failure of such preventative measures undermines public confidence.

Resilience, on the other hand, according to Jackson, offers a way to reduce the consequences should an attack prevail and offers to broaden the range of ways to reduce risks. Jackson also noted, however, that as the scale of a potential attack increases, traditional preventative measures can look more attractive than having to rely on resilience to survive the attack.[31]

In a September 2009 report, the National Infrastructure Advisory Council (NIAC) found the "current policy framework fundamentally sound but could be improved to better reflect principles of resilience.…"[32] The report also recommended that DHS: expand programs to allow funding for programmatic and grant funding of resilience efforts;[33] encourage each sector to set resiliency goals;[34] and assist in building resilience in the next generation of infrastructure.[35] The report also noted the importance of repair and maintenance on resilience.[36]

---

[28] The Reform Institute, Building a Resilient Nation: Enhancing Security, Ensuring a Strong Economy, p. 1.

[29] James Jay Carafano, *Resiliency and Public-Private Partnerships to Enhance Homeland Security*, The Heritage Foundation, Backgrounder, June 4, 2008, pp. 1, 4.

[30] Brian A. Jackson, *Marrying Prevention and Resiliency: Balancing Approaches to an Uncertain Terrorist Threat*, RAND Corporation, Santa Monica, CA, 2008.

[31] For example, Jackson could be referring to the detonation of a nuclear bomb, sabotage of a nuclear reactor, or the release of a virulent biological agent with very large scale consequences against which preventive actions could be taken and given some priority. On the other hand, some things, like earthquakes, cannot be prevented, and resilience would have to be relied upon.

[32] National Infrastructure Advisory Council, *Critical Infrastructure Resilience*, Final Report and Recommendations, September 8, 2009, p. 11.

[33] Ibid, p. 14.

[34] Ibid.

DHS Response

G.W. Bush Administration

Early high level government policy documents rarely mentioned resilience. Neither the first *National Homeland Security Strategy* (2002) nor Homeland Security Presidential Directive 7 (2003) mention resilience at all. Both acknowledged that it would be impossible to protect all targets or eliminate all vulnerabilities. Both focused on the impact strategic investments in protection and security could have on deterring and deflecting terrorist attacks against the most critical assets and could help mitigate the effects of terrorist attacks by forcing terrorists to consider targets with lesser consequences. The extent to which resilience was alluded to at all focused primarily on the need to recover rapidly from an incident after it occurred.

The National Strategy for the Physical Protection of Critical Infrastructure and Key Resources (2002) did cite resilience as an issue. In discussing one of the eight principles guiding the nation's protection efforts, the document mentioned making infrastructure more "robust" through such measures as redundancy, hardening, and dispersal and more "resilient" through effective protection and response planning.

The debate started by the Task Force appeared to have had some immediate impact on DHS and the development of the 2006 *National Infrastructure Protection Plan,* which DHS was in the process of producing at the time of the Task Force's report. Whether in response to the Critical Infrastructure Task Force, or by coincidence, DHS used the words resilient, resilience, or resiliency, twice as much in the final version of its 2006 *National Infrastructure Protection Plan* (NIPP), released after the Task Force's report, than in the Plan's earlier draft, released for comment in November 2005.[37] Perhaps more telling, the early draft did not define resiliency in its glossary of terms, whereas the final version did.

The final 2006 version of the NIPP seemed to put resilience on par with protection, talking about building a "more secure and resilient nation," "improving protection and resilience," and "managing protection and resiliency approaches." The NIPP also discussed research and development goals that included work in self-healing systems (which one could consider to be a resiliency measure). However, the NIPP still considered resiliency to be part of a protective strategy. For example, among its list of "protective actions," alongside such efforts as perimeter hardening, enhanced buffer zones, fencing, and enhanced police and security officer presence (typical protective measures), were developing redundancies and back-up systems (resiliency enhancing measures). The NIPP did not include a separate comparable list of actions that could increase resiliency.

In May 2008, in hearings before the House Committee on Homeland Security, Robert Stephan, then Assistant Secretary for Infrastructure Protection at DHS, testified that the department fully embraced the concept of resilience and that it was "built into practically everything" that the

(...continued)

[35] Ibid, p. 26.

[36] Ibid, p. 27.

[37] The base draft used those terms 20 times, the final version used those terms 50 times. The 2009 version of the Plan mentions those terms 124 times and included the term in its title, *National Infrastructure Plan: Partnering to Enhance Protection and Resiliency*.

department was doing. He noted that it was important to achieve the proper balance between protection and resilience. He went on to state the "more extreme advocates of the resiliency construct dismiss the importance" of prevention and protection in certain cases, stating, "We cannot afford to protect everything, but we cannot simply stand by and protect nothing."[38]

Turning the Task Force's construct around, the Assistant Secretary reiterated the NIPP assertion that "protection" served as an overarching strategic concept which could include resiliency measures.

> Protection can include … hardening facilities, building resiliency, redundancy, incorporating hazard resistance into facility or system or network design, initiating active or passive countermeasures, installing security systems, promoting workforce security programs, and implementing cyber measures, among other various precautions.

Notwithstanding Assistant Secretary Stephan's assertion that the department's critical infrastructure efforts already fully embraced resilience, subsequent policy documents made increasing mention of resilience. The 2009 update of the NIPP included resiliency in its title (*National Infrastructure Protection Plan: Partnering to enhance protection and resiliency*) and used the terms resilience, resilient, or resiliency more frequently throughout the document than the plan's first release. However, the use of the term resilience was due primarily to repetitive references to "protective programs and resiliency strategies" in places where the earlier 2006 version only made reference to "protective programs." According to the Government Accountability Office (GAO), one of the objectives in updating the NIPP in 2009 was to increase the Plan's emphasis on resilience as a risk reduction approach. However, it was not meant to signal a major shift in policy.[39] The NIPP Program Office also informed the GAO that it was providing additional guidance to the agencies charged with developing Sector Specific Plans to better incorporate resilience in their plans.[40]

Obama Administration

Indicative of the evolving integration of resilience into homeland security policy, the incoming Obama Administration established a Directorate for Critical Infrastructure Protection and Resiliency Policy in the reorganized National Security Staff. Also in 2009, the Homeland Security Studies and Analysis Institute began a series of reports to develop a framework for incorporating resilience into the nation's critical infrastructure effort.[41]

---

[38] U.S. Congress, House Committee on Homeland Security, *Partnering with the Private Sector to Secure Critical Infrastructure: Has the Department of Homeland Security Abandoned the Resilience-Based Approach?*, 110th Cong., 2nd sess., May 14, 2008, Serial No. 110-114, p. 7. Later during questioning, the Assistant Secretary suggested that certain people "would like to drive a wedge and cause us to make a choice between protection, prevention, and the response and recovery side, or the resiliency side." See p. 36.

[39] U.S. Government Accountability Office, *Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience*, GAO-10-296, March 2010.

[40] Each of the 18 critical infrastructure sectors are tasked with developing Sector Specific Plans (SSPs) for managing the risks unique to their sector. Each sector has a lead agency assigned to it (Sector Specific Agency) which is responsible for developing, in consultation with the infrastructure owners/operators, for developing the SSPs. The NIPP offers a common framework for all of the sectors to follow.

[41] Homeland Security Studies and Analysis Institute. *Concept Development: An Operational Framework for Resilience*. August 27, 2009, *Risk and Resilience: Exploring the Relationship*, November 22, 2010, and *Preparedness, Response, and Resilience Task Force: Interim Task Force Report on Resilience*, May 16, 2011.

The *Quadrennial Homeland Security Review* (QHSR), released in February 2010, made frequent direct and indirect references to resiliency. The QSHR stated three concepts that are essential to, and form the foundation for, a comprehensive approach to homeland security: security, resilience, and customs and exchange (i.e., facilitating the normal daily activities of society). It went on to state that:

> preventing a terrorist attack remains the cornerstone of homeland security ... [but] despite our best efforts, some attacks, accidents, and disasters will occur. Therefore the challenge is to foster a society that is robust, adaptable, and has the capacity for rapid recovery. In this context, individuals, families, and communities-and the systems that sustain them-must be ... prepared to withstand disruptions, absorb or tolerate disturbances, ... adapt to changing conditions, and grow stronger over time.[42]

The QHSR identified five core missions. Mission 1 was *Preventing terrorism and enhancing security*. Goal 1.3 of that mission was: Manage Risks to Critical Infrastructure, Key Leadership, and Events. Two of the four objectives under that goal were (1) protect critical infrastructure (prevent high consequence events by securing critical assets, systems, networks, or function from attacks or disruptions), and (2) make critical infrastructure resilient (enhance the ability of critical infrastructure systems, networks, and functions to withstand and rapidly recover from damage and disruption and adapt to changing conditions). The significance here is the separation of protection and resilience as two distinct options.

Mission 5 was *Ensuring Resilience to Disasters*. Goals under this mission included (1) mitigating hazards, (2) enhancing preparedness, (3) ensuring effective emergency response, and (4) rapid recovery. Objectives under these goals included mitigating risks to communities by improving community capacity to withstand disasters by mitigating known and anticipated hazards, and ensuring continuity of essential services and functions. All of these goals and objectives could be considered resiliency-enhancing efforts.

The *National Security Strategy*, released May 2010, also included the concept of resilience.[43] One element of the strategy called for strengthening security and resilience at home. The strategy reaffirmed the notion that not all threats can be deterred or prevented and that resilience is also required. The strategy called for strengthening public-private partnerships to improve resilience by developing incentives to design structures and systems that can withstand disruptions and mitigate consequences; ensuring redundant systems are available where necessary to maintain the ability to operate; decentralizing critical operations to reduce vulnerability to single points of disruption; developing and testing continuity of operations plans; and investing in improvements and maintenance of existing infrastructure.

In March 2011, the Obama administration issued a new Presidential Decision Directive (PDD) 8, *National Preparedness* (replacing the Bush-era Homeland Security Presidential Directive of the same name and number).[44] The PDD seeks to strengthen "the security and resilience of the United States through systematic preparation for the threats that pose the greatest risk.…" The PDD called for the development of a National Preparedness Goal that identifies the core capabililties

[42] Department of Homeland Security. *Quadrennial Homeland Security Review: A Strategic Framework for a Secure Homeland.* pp.14-15.

[43] Executive Office of the White House, *National Security Strategy*, May 2010.

[44] For more on PDD-8, see CRS Report R42073, *Presidential Policy Directive 8 and the National Preparedness System: Background and Issues for Congress*, by Jared T. Brown.

judged necessary for national preparedness in each of five mission areas. The five mission areas are prevention, protection, mitigation, response, and recovery. Adding mitigation to the mission areas was a primary modification to previous guiding documents. For each core capability, capability targets also are to be identified. The first edition of the National Preparedness Goal was published in September 2011. As might be expected, the concept of resilient critical infrastructure is touched upon in the mitigation, response, and recovery mission. Elaborating on one of the seven mitigation core capabilities, the NPG states that long-term vulnerability reduction should build and sustain resilient systems, communities, and critical infrastructure lifelines, so as to reduce vulnerability and lessen adverse consequences. The Response and Recovery missions both include an Infrastructure Systems core capability that calls for the stabilization of critical infrastructure functions. In Recovery, the core capability includes a target of developing plans to redevelop community infrastructure to contribute to (future) resilience.

Summary of Policy Evolution

To some, the debate whether to promote protection or resilience as the overarching strategic vision for the nation may appear to be a debate over semantics. And, to some extent, arguing whether protection incorporates resilience or resilience incorporates protection may obscure the very real difference between the two. Reducing risks by building higher fences and deploying more guards around a particular facility or asset (protection) is very different than reducing risks by building a second facility or asset somewhere else or strategically stockpiling replacement equipment that can get the facility or asset up and running again quickly (resilience). Perhaps a more useful way of making the distinction between protection and resilience is that protection focuses on the threat and resilience focuses on the consequences (see risk equation above).

DHS has made an effort to incorporate resiliency into its more recent guiding documents. While it does not go so far as the Task Force recommendation, this evolution does seem to acknowledge that protection and resilience represent two ends of the spectrum of possible risk reduction efforts and that both need to be considered when assessing the best options for reducing risks. As policymakers (in Congress and the Executive branch) deliberate on the best options, it may be helpful to recognize that while protection may be a preferred option under certain scenarios, it is not always possible.

Programs

If one accepts that DHS has made progress in incorporating resilience into its policies and goals, a subsequent question could be "What is DHS doing programmatically to improve the resilience of critical infrastructures?"

As cited earlier, Assistant Secretary Robert Stephan stated that "it is fair to say that there is resilience built into practically everything that the Department of Homeland Security does."

The Assistant Secretary proceeded to mention more than a dozen activities including forums (e.g., the National Communications System's Route Diversity Forum), various communication protocols (e.g., the water sector's Water/Wastewater Agency Response Network, or WARN), planning guides, exercises, site assistance visits, and analytical products from the National Infrastructure Simulation and Analysis Center and DHS's Homeland Infrastructure Threat and

Risk Analysis Center, all of which he asserted contribute in some way to DHS's concept of resilience.

One can also argue that the department programs to help owner/operators of critical infrastructure identify threats, assess the vulnerability of their assets and operations to those threats, and assess the possible consequences from those threats, are necessary before one can identify and implement protective or resilient options for reducing those risks. These programs include the development and refinement of the *National Infrastructure Protection Plan* (NIPP), training for owners/operators on how to participate in and implement the NIPP, development and support of information sharing networks like the Homeland Security Information Network, support for partnership meetings and cooperation, cataloging critical infrastructure assets, etc.

Nevertheless, in its report *Critical Infrastructure Resilience, Final Report and Recommendations*, released September 8, 2009, the National Infrastructure Advisory Council found that "while there are government programs that address resilience tangentially, government lacks a cohesive set of programs and activities that directly address CIKR [critical infrastructure and key resources] resilience."[45]

Similar conclusions were reached by the Community Resilience Task Force of the Homeland Security Advisory Council in June 2011. The Task Force stated that "many relevant activities are already underway, particularly those in fostering development of preparedness capabilities, but [the Task Force] observes that those activities are rarely linked explicitly to resilience."[46] The Task Force went on to find that "resilience is not well understood by key homeland security stakeholders; it therefore had not been treated as an integral element of plans and programs to date,"[47] and "there are no policies, national objectives, or promulgation of the specific means required to actually assess, achieve, or sustain resilience."[48]

Despite this somewhat amorphous depiction of department efforts to support resiliency, a few programs do explicitly take resilience into consideration.

Office of Infrastructure Protection—Regional Resiliency Assessment Program

The Government Accountability Office, in its 2010 report, *Critical Infrastructure Protection: DHS Efforts to Assess and Promote Resiliency Are Evolving but Program Management Could Be Strengthened*, concluded that DHS had made some progress in integrating resiliency concepts into some of its programs and analytical tools. In particular, the report examined the department's Site Assistance Visits (SAVs), Enhanced Critical Infrastructure Protection Security Survey (ECIP), and the Regional Resiliency Assessment Program (RRAP). In addition, the report noted that the department had begun training its Protective Services Agents (PSAs) on incorporating resiliency concepts into their interactions with the owners and operators of critical infrastructure assets. One of the PSAs' responsibilities include facilitating SAVs.

[45] National Infrastructure Advisory Council, op. cit., p. 27.

[46] Homeland Security Advisory Council, *Community Resilience Task Force Recommendations*, June 2011, p. 3.

[47] Ibid, p. 12.

[48] Ibid, p. 14.

The ECIP survey is a web-based tool that is used during a site visit to collect and analyze mostly security-related information (e.g., physical security measures such as fences, gates, etc., security force status such as security patrols and command and control, security management, information sharing, and protective measures). It uses this information to develop a set of metrics (Protective Measure Indexes) by which an owner/operator can compare the security of his facility with other similar facilities. The survey also characterizes dependencies on other infrastructures (e.g., electrical and water services, transportation) and contingency plans associated with the facility. These latter components contribute to the development of a Resiliency Index, similar to the protective Measure Indexes. The survey also contains a "dashboard" that displays the various indexes and allows the owner/operator to make changes in the elements to see what effect they would have on overall protection and resilience.

In developing a resilience index, the ECIP considers three elements—robustness, resourcefulness, and recovery—and, assesses such factors as redundancies and substitutions, the existence of comprehensive emergency actions plans, and the existence of priority agreements with local utility providers.[49] Robustness refers to the ability to maintain critical operations and functions in the face of a crisis. Resourcefulness refers to the ability to respond to and manage a crisis. Recovery refers to the ability to return to normal operations as quickly and efficiently as possible. Each of these factors are scored and weighted, based on expert opinion, then added and averaged, resulting in the index. Therefore, the index is an indicator, but not an actual measure of resilience. In other words, it does not measure either the amount of time it would take to recover or the costs associated with a loss or disruption of operations.

The Regional Resiliency Assessment Program (RRAP) essentially expands and integrates a number of ECIPs across all the critical assets in a given region. For example, while an individual ECIP might consider the existence of contingency plans for reconstituting water service to a facility, the RRAP would look more closely at the potential vulnerabilities to the supply of water within the region and how a given facility might respond to a situation that exploits those vulnerabilities. For example, a facility's water supply contingency plan might rely on the delivery of water by truck, but a broader regional assessment might indicate that the delivery is dependent on a bridge whose traffic might be vulnerable to the same events as the facility. The RRAP is particularly useful in analyzing natural disasters, which tend to affect larger areas and number of assets than perhaps a terrorist event.

At the time of its report, the GAO noted that while DHS had made some progress in incorporating resiliency into these programs and tools, it had not yet developed the ability to track what if any resiliency measures were actually being taken by critical infrastructure owners/operators. Also, while DHS stated that it was training its PSAs on resiliency concepts, PSA guidance documents had not yet included resiliency concepts.

FEMA Grants

The Federal Emergency Management Agency (FEMA) administers a number of grant programs. Most focus on planning and developing the capabilities needed to respond and recover from an all-hazard event, addressing primarily community and regional resilience. However, some also touch upon critical infrastructure resilience, directly or indirectly.

[49] The basic framework developed by Bruneau et al.

For example, the State Homeland Security Grant Program (SHSGP) and the Urban Areas Security Initiative (UASI), which primarily support the preparedness activities of states and local communities, take into consideration the presence of critical infrastructure in the state or urban area when allocating the annual grant budget.[50] These grants can support public expenditures for overtime personnel costs associated with protecting critical infrastructure assets. The grants also can support vulnerability assessments of critical infrastructure assets and the development of security plans. The grants can also support citizen preparedness through the development and support of Citizen Corps Councils which include both public and private owner/operators of critical infrastructure assets. Although no longer specifically mentioned in the context of critical infrastructure, grants can also be used by government entities to purchase certain equipment, including surveillance equipment, barriers, access-controls, etc., that could be used at critical infrastructure sites. Nearly all of this equipment, however, focuses on protective measures.

The grants only support those costs incurred by state and local governments. Any direct impact to critical infrastructure assets would be limited to those assets which the state or local government own/operate or which otherwise costs the government money. The impact on privately owned/operated critical infrastructure assets would appear to be limited to supporting the formation and activities of Citizen Corps Councils or possibly being involved in a vulnerability assessment conducted or paid for by some public entity eligible to receive grant funds.

The primary contribution of these two grant programs to resilience (in this case focused primarily on community resilience) is through their support for planning, organizing, and implementing response and recovery efforts following a natural disaster or terrorist event.

FEMA also administers a Transit Security Grant Program.[51] This grant program supports public transportation agencies to secure their critical transportation infrastructure and protect their passengers. Transportation infrastructure include intra-city buses, commuter buses, ferries, and all forms of passenger rail. Like SHSG and UASI, allowable activities include planning, operations, equipment, training, and exercises.

The FY2012 grant guidelines identified three priorities: operational activities, operational packages, and remediation of assets on the Top Transit Asset List. Operational activities include training, drills and exercises, public awareness, and vulnerability assessments and security planning. Operational packages include canine teams, mobile explosive screening teams, and anti-terrorism teams. The Top Transit Asset List includes those assets that DHS has determined meet the definition of critical at the national level. It includes underwater tunnels, underground stations and tunnels, and high density bridges.

Eligible grantees must work from a risk assessment and a security plan. The risk assessment and security plan are to consider, among other items, efforts to provide redundant or back-up assets that would enable the transportation system to continue to operate in the event of an attack or incident. Such a requirement would relate to resilience. Nevertheless, as with SHSG and UASI, many of the supported activities and eligible expenditures could be considered protective in

[50] Deparment of Homeland Security: Federal Emergency Management Administration, *FY2012 Homeland Security Grant Program Funding Opportunity Announcement*. See, http://www.fema.gov/pdf/government/grant/2012/fy12_hsgp_foa.pdf.

[51] Department of Homeland Security: Federal Emergency Management Administration, *FY2012 Transit Security Grant Program Funding Opportunity Announcement.* See, http://www.fema.gov/pdf/government/grant/2012/fy12_tsgp_foa.pdf.

nature: training in behavior recognition and counter-surveillance training, security enhancements such as intrusion detection and visual surveillance with live monitoring, or hardening of control centers. However, the grants can also be used to protect tunnel ventilation and drainage systems and flood gates and plugs, both of which one could say contribute more directly to resilience by mitigating damage associated with an event.

The FY2012 grant guidelines for the Port Security Grant program specifically mentions enhancing recovery and resiliency capabilities as one of the FY2012 priorities.[52] Eligible recipients include private sector facility owners/operators along with state and local governments and public entities. Recipients must belong to a port-wide management planning group and participate in a port-wide risk management plan. Recipients also are encouraged, but not required, to develop a business continuity/resumption of trade plan. Although not required, the guidelines noted that priority would be given to the development and implementation of such a plan. Funds can be used for operational activities, planning, equipment, training, and exercises, but also some construction. As with the previously mentioned grants, much of this is protection-oriented. However, specific mention is made regarding equipment or systems for continuity of critical port operations and, under the category of construction, funds can be used to house generators that support risk mitigation.

FEMA also supports mitigation grant programs, including Hazard Mitigation and Pre-Disaster Mitigation, which one might think could support activities that increase the resiliency of critical infrastructure.[53] These programs support risk assessments, mitigation plans, and implementation of mitigation measures. Eligible expenses include government expenditures to purchase and clear property and to make structural improvements to buildings (e.g., elevating buildings in flood plains or building ring levees). The grants focus on natural events and do not necessarily focus on critical infrastructure.

FEMA also offers courses on how to mitigate risks to buildings against terrorist attacks; for example, Building Design for Homeland Security and Primer for Design of Commercial Buildings to Mitigate Terrorist Attacks. FEMA also publishes guidelines such as *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*, *Primer for Design Safe School Projects in Case of Terrorist Attack*, and *Terrorism Risk Management in Buildings (Insurance, Finance, and Regulation)*. These documents mention resilience-oriented measures such as the use of fire-resistive construction techniques, designs that resist progressive collapse, and the consideration of redundancy and alternative sources of fuel, water, air, etc.

FEMA manages another program that touches upon resilience. The Voluntary Private Sector Preparedness program (PS-Prep) is not a grant program but a voluntary standards program. Established by Congress in the Implementing Recommendations of the 9/11 Commission Act (P.L. 110-53, Sec. 901), PS-Prep has, in cooperation with the private sector, international standard-making bodies, and other stakeholders, developed and adopted a set of standards the private sector can use to help prepare for and respond to emergency situations.[54] While addressing

[52] Department of Homeland Security, *FY2012 Port Security Grant Program Funding Opportunity Announcement*. See, http://www.fema.gov/pdf/government/grant/2012/fy12_psgp_foa.pdf.

[53] Department of Homeland Security. Federal Emergency Management Administration, *Hazard Mitigation Assistance Unified Guidance*, June 1, 2010.

[54] The standards adopted are SPC 1.2009 from ASIS International, BS 25999 from the British Standards Institution, and NFPA 1600 from the National Fire Protection Association. A firm can seek certification under any of these three standards.

preparedness processes and requirements in general, the standards discuss specifically both protective/preventive options as well as resiliency-related options like alternative work sites, redundancies and diversity in personnel, equipment, information and materials, etc., as ways to mitigate risks. The PS-Prep program has also accredited a number of third-party entities that can be used to certify a firm's compliance with these standards. In March 2012, AT&T became the first firm to receive certification under PS-Prep.[55]

S&T Programs

Another area in which DHS may help promote resiliency is in research and the development of new understanding and technologies. The Science and Technology Directorate divides its activities into four program areas: Acquisition and Operations Support; Research, Development, and Innovation; Laboratory Facilities; and University Programs. A comprehensive analysis of the Directorate's projects and their relevance to improving resilience is beyond the scope of this report. However, a brief summary analysis of the first two program areas follows, based on the Directorate's FY2013 budget justification document.[56]

One of the projects within the Acquisition and Operations Support program supports the activities of the Homeland Security Studies and Analysis Institute. As stated earlier in this report, the Institute produced a series of reports on the fundamental characteristics of resilience and how it applies to homeland security. Infrastructure resilience remains one of the Institute's key mission areas and could contribute to a greater understanding of resilience and how to promote it.

Roughly two-thirds of the Directorate's budget goes toward Research, Development, and Innovation. The program supports over 150 individual projects. Many of these are protection-oriented. Projects within the Border Security, the Chemical, Biological, and Explosive Defense, and the Counter Terrorist thrust areas focus on developing new sensor technologies and systems, biometrics, data fusion, behavior prediction, modeling and simulation, etc., in order to improve capabilities in surveillance, detection/screening/tracking and characterizing threats on the ground, in the air, in and under the water, in tunnels, and in cyberspace. It should be noted that some of these detection technologies could also assist in response and recovery or lessening the overall impact of a chemical, biological, or radiological attack by characterizing and tracking affected areas, allowing for targeted and more cost-effective responses.

A number of projects, particularly those in the Disaster Resilience thrust area, focus more specifically on incident response and recovery. These include the development of decontamination and disposal techniques and technologies, location technologies, incident management systems, and information sharing systems.

There also a few projects that may help improve resilience by reducing the damage caused by an attack, or possibly improving the capability for the affected system to continue functioning during or after an incident. For example, the Resilient Electric Grid project is developing and deploying fault current limiting, high temperature superconducting cable power substations that can be interconnected to share power in a way to prevent cascading effects and thereby improve

[55] Department of Homeland Security, "DHS Announces AT&T PS-Prep Certification," press release, March 14, 2012, http://www.dhs.gov/news/2012/03/14/dhs-announces-att-ps-prep-certification.

[56] Department of Homeland Security, *Science and Technology Research, Development, Acquisitions, and Operations*, Fiscal Year 2013 Congressional Justification.

resilience of the grid.[57] Another example is the Blast Analysis of Complex Structure projects that could facilitate the application of techniques to mitigate the effects of explosive blasts on structures. A number of examples also exist in the Cyber Security thrust, such as the Experimental Research Testbed, the Leap Ahead Technologies, the Moving Target Defense, and the Tailored Trustworthy Spaces projects that focus on techniques that conceivably could keep information networks running while under attack or experiencing disruptions.

Program Summary

DHS can be thought of as having always contributed to community resilience in its efforts to improve the ability of communities to respond and recover from incidents through grants and various assistance programs. This has been furthered by more recent emphasis given to mitigation of risks before as well as after an incident. However, many of these efforts focus on public institutions and assets. While some may receive assistance from these programs, many critical infrastructure assets owned and operated by the private sector receive none. To the extent that DHS has sought to help private and public sector owner/operators of critical infrastructure assess their risks associated with various threats, it has also contributed to critical infrastructure resilience. More recently, those efforts have taken into consideration more specifically resilience-oriented risk reduction options. However, to a large extent, taking specific action to facilitate implementation of resilience-oriented corrective measures, including longer-term redesign of systems, has not gone as far as that recommended by the National Infrastructure Advisory Council or the Community Resilience Task Force of the Homeland Security Advisory Council. To some extent, this may be due to the reluctance to use public funds to help reduce the risks to privately owned assets. However, the National Infrastructure Advisory Council cautioned that it is not clear that market incentives are sufficient to drive such investments.[58]

Issues for Congress

To date, Congress has taken primarily an oversight role in regard to critical infrastructure resilience, holding hearings and requesting reports from its congressional support agencies. However, it has been two years since GAO reported that DHS had not yet developed the ability to measure the extent to which owners and operators of critical infrastructure assets had taken resilience-enhancing actions. Congress may choose to continue its oversight of the progress being made in the area of metrics.

Congress also may revisit the PS-Prep program. Congress gave DHS the responsibility to establish a voluntary preparedness standard for the private sector in 2007. DHS adopted three such standards in 2010, and the first firm received certification under the program in 2012. Congress may opt to examine the status of that program and identify impediments, if any, to its implementation.

[57] A fault current in an electrical system is an abnormal current, usually higher than the current in a system under normal conditions. The higher current can cause damage to system components. A fault current limiter is a technique or device (in this case making use of high-temperature superconducting materials) that acts to limit the increase in current, thereby offering some protection of system components.

[58] National Infrastructure Advisory Council, op. cit., p. 10. For example, the price of electricity, and therefore the loss of revenue experienced by the owner/operator of an electric utility during a disruption, may not fully capture the social costs associated with, say, increased commuting times, lost output, or spoiled food, associated with the disruption.

Updating the latest metrics on the extent to which firms are adopting resiliency measures or the extent to which firms are seeking certification through the voluntary PS-Prep program could provide insight into the need, if any, for additional incentives beyond those provided by the market. If additional incentives are warranted, Congress could consider expanding its preparedness and mitigation grant programs to include more private sector owner and operators of critical infrastructure. This could be accompanied with additional funding. To do so, however, may require the reallocation of funds in the current budget-constrained environment. Alternatively, Congress could consider making the voluntary standards mandatory, at least for those assets and systems judged to pose the greatest risks. However, the recent inability of Congress to find consensus on cybersecurity standards for privately held critical infrastructure would indicate such an effort would also raise significant debate.[59]

Author Contact Information

John D. Moteff
Specialist in Science and Technology Policy
jmoteff@crs.loc.gov, 7-1435

[59] Jaikumar Vijayan, "No Partisan Fight over Cybersecurity Bill, GOP Senator Says," *ComputerWorld*, August 16, 2012. See, http://www.computerworld.com/s/article/9230341/No_partisan_fight_over_cybersecurity_bill_GOP_senator_says.