This chapter will appear in the second edition of *Homeland Security and Emergency Management: A Legal Guide for State and Local Governments,* edited by Ernest B. Abbott and Otto J. Hetzel, due out in spring 2010.

CHAPTER 6
THE ROLE OF THE PRIVATE SECTOR IN EMERGENCY PREPAREDNESS, PLANNING, AND RESPONSE

By Evan Wolff and George Koenig

> [T]he private sector controls 85 percent of the critical infrastructure in the nation. Indeed, unless a terrorist's target is a military or other secure government facility, the "first" first responders will almost certainly be civilians. Homeland security and national preparedness therefore often begins with the private sector . . . **Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world**.[1]
>
> —9/11 Commission Report (emphasis added)

I. Introduction

The private sector is likely to be the first line of defense against the next man-made or natural disaster. Any government planning or response that does not adequately account for the private sector's role in any response or recovery is doomed to fail. This should come as no surprise to all who have witnessed numerous large scale disasters that have struck the United States in the last several decades – whether it is a terrorist attack, a hurricane, an earthquake, a flood, fire, etc. The private sector's role in disaster planning and response is so essential because it owns and operates the overwhelming majority of the national, state, and local critical infrastructure and key resources.

This chapter will focus on the vital role of the private sector in emergency planning, preparedness and response. As will be discussed below, successful government/private sector collaboration requires an understanding of the following:

(i) critical infrastructure protection (CIP)[2] - including key federal planning directives, documents, legislation, and regulations; and

---

[1] THE NAT'L COMMISSION ON TERRORISTS ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT (2004) (hereinafter "The 9/11 Commission Report"), p. 398;

[2] The authors acknowledge the challenge of learning the homeland security lexicon and apologize in advance for the heavy use of acronyms. For each key acronym we use, we will define it in the body of the chapter, but for ease of reference, the following is a summary of key acronyms:

ANAB	ANSI-ASQ National Accreditation Board
ANSI	American National Standards Institute
BCP	Business Continuity Plan
CFATS	Chemical Facility Anti-Terrorism Standards

(ii) individual and private sector preparedness (including business continuity planning).

Ultimately, a successful response to the next disaster will depend upon all the work that was done by individuals, companies, communities and government at all levels before the event happens.

II. Critical Infrastructure Protection (CIP)

Our nation's financial, physical, and cyber security depends on the effective functioning of its critical infrastructures. Congress defines critical infrastructures as the:

> ''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

CII	Critical Infrastructure Information
CIKR	Critical Infrastructures and Key Resources
CIP	Critical Infrastructure Protection
CIPAC	Critical Infrastructure Partnership Advisory Council
CUI	Controlled Unclassified Information
CVI	Chemical Vulnerability Information
DHS	U.S. Department of Homeland Security
FEMA	Federal Emergency Management Agency
FOIA	Freedom of Information Act
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
HSA	Homeland Security Act of 2002
HSAS	Homeland Security Advisory System
HSPD-7	Homeland Security Presidential Directive-7
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISACs	Information Sharing and Analysis Centers
ISE	Information Sharing Environment
NFPA 1600	National Fire Protection Association Standard 1600
NIAC	National Infrastructure Advisory Council
NIMS	National Incident Management System
NIPC	National Infrastructure Protection Center
NIPP	National Infrastructure Protection Plan
NPPD	National Protection and Programs Directorate
NRF	National Response Framework
NRP	National Response Plan
OHS	White House Office of Homeland Security
PCII	Protected Critical Infrastructure Information
PDD-63	Presidential Decision Directive 63
PSO	Private Sector Office
PS-Prep	Voluntary Private Sector Preparedness Accreditation and Certification Program
QHSR	Quadrennial Homeland Security Review
SSAs	Sector-Specific Agencies
SSI	Sensitive Security Information
SSPs	Sector-Specific Plans
SVAs	Security Vulnerability Assessments
TRIA	Terrorism Risk Insurance Act

> impact on security, national economic security, national public health or safety, or any combination of those matters.''[3]

What makes certain systems and assets "critical" is almost self-evident. For instance, it is inconceivable that our country could function without: power plants; a safe and abundant food supply; hospitals and emergency rooms; automobile, rail and air transportation systems; financial networks (including ATMs, credit cards, etc.), telecommunications, and the internet. It is through the functioning of critical infrastructures that the private sector provides the goods and services that make our way of life possible.

Critical infrastructures, by definition, are often interdependent; there is a substantial risk that a decrease in capacity in one critical infrastructure sector may have a catastrophic, cascading effect in another sector – regardless of region or locality. This notion of "interdependence" really strikes at the heart of the concept of critical infrastructure – simply because your home, business, facility, region, or industry was not directly attacked, destroyed, or damaged by a disaster does not mean that you will not be severely impacted. For example, if a power plant is damaged or destroyed by a hurricane or tornado, it would adversely impact the region's electrical supply. A reduced supply of electricity could impact numerous industries that might not otherwise have been damaged; for example: (i) banking – ATMs might be shut down; (ii) transportation -- rail cars powered by electricity might not be able to transport commuters to and from work. Another example is a cyber-attack that cripples the internet. We have become so dependent on the internet that such an attack could dramatically impact commerce across the United States; for instance, if a cyber attack was severe and debilitating enough, businesses would need to receive orders by slower, older-fashioned methods (e.g., mail, fax, etc.); fast and simple email communications would not be possible; documents could not be easily exchanged and edited. And the list goes on. As will be discussed below, because the overwhelming majority of critical infrastructures are privately owned, any effort to protect them and our nation requires collaboration and support from the private sector.

Protecting the nation's critical infrastructure, has taken an evolutionary path involving executive branch direction and coordination, congressional action and oversight, agency regulation, federal programs, private-sector outreach, and information sharing. A seminal document in this area is the National Infrastructure Protection Plan (NIPP), which established the vernacular and process for organizing governments and the private sector in a unified direction in order to more urgently address the task of CIP. Emerging legal standards are being established through litigation surrounding previous acts of terrorism and future threats. The U.S. Department of Homeland Security (DHS) is also in the process of establishing preparedness standards that may become a driver of policy and actions in this area. Recently, the Obama Administration has raised growing concerns about the nation's vulnerability to an attack or major mishap in cyberspace and we can expect more policy developments in the months and years ahead as political appointees enter the Administration and gain more executive experience. Lastly, at the time this chapter was submitted for publication, DHS had begun the first ever process of systematically reviewing "emergency preparedness, response, and recovery, continuity of operations/continuity of government, and

[3] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) of 2001, 42 U.S.C. § 5195c(e).

individual and community preparedness," for the Congressionally mandated Quadrennial Homeland Security Review (QHSR). [4]

By understanding CIP, all parties will have a better organizational framework to understand roles and responsibilities of the government and private sector in emergency preparedness and response. Although Congress has begun venturing into "security" focused regulation of critical infrastructure sectors (e.g., chemical security), much of the work to date has been in the area of policy and strategy development -- and it remains largely voluntary and collaborative in nature.

A. Federal & State Strategies for Public-Private Partnerships

The role of the private sector in protecting critical infrastructure has been largely a voluntary one. Some of the earliest efforts in CIP were focused on encouraging the private sector to develop information sharing and analysis centers. After September 11, 2001, there was a surge of intense focusing on protecting the homeland from another terrorist attack and the vital role of the private sector in that mission. While the role of government and the private sector has and will continue to evolve, significant improvements in public-private collaboration have been realized.

1. Pre-9/11 Critical Infrastructure Protection Environment

The concept of CIP is a relatively recent post-Cold War phenomenon. Prior to September 11, 2001, a number of events in the 1990s forced policy makers to think about protecting the homeland from a different vantage point. The major impetus for the developing field of CIP was several terrorist attacks in the United States and against American facilities and personnel abroad.[5] As a consequence of these events and heightened concerns in general, President Clinton created a Commission in the summer of 1996 to examine the increasing threat of terrorism and how the nation might better protect itself.[6] The Commission published a final report and in the spring of 1998 President Clinton issued Presidential Decision Directive 63 ("PDD-63").[7] The Directive recognized that future adversaries may not be nation-states, but rather transnational groups that directly attack civilian populations and assets -- to cause us harm and achieve their policy goals. It stated that enemies

> "…may seek to harm [the United States] in non-traditional ways including attacks within the United States. Because our economy is increasingly reliant upon interdependent and cyber supported infrastructures, **non-traditional attacks on our infrastructure**

[4] Id.
[5] For instance, in February 1993, a Sunni extremist, Ramzi Yousef, planted a bomb in World Trade Center's parking garage killing six people. A few years later, in what was then the worst terrorist attack on U.S. soil, an American and Army veteran, Timothy McVeigh, bombed the Alfred P. Murrah Federal Building in Oklahoma City in the spring of 1995. As a final example, during the summer of 1996, U.S. military personnel were targeted in a deadly attack at Khobar Towers in Saudia Arabia.
[6] See http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1996_register&docid=fr17jy96-92.pdf
[7] Presidential Decision Directive No. 63 (1998), *available at* http://www.fas.org/irp/offdocs/pdd/pdd-63.htm on Critical Infrastructure Protection"); *also see* Presidential Decision Directive 62 (May 22, 1998), *available at* http://www.fas.org/irp/offdocs/pdd-62.htm.

> **and information systems may be capable of significantly harming both our military power and our economy**."[8]
>
> (emphasis added)

PDD-63 led various departments and agencies to develop new initiatives and programs focusing on the threat of non-traditional attacks on the nation's infrastructure. As an example, the Federal Bureau of Investigation created a National Infrastructure Protection Center (NIPC)[9] to "…serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity."[10] The Directive further recognized the central role of the private sector in critical infrastructure protection ordering the federal government to "…consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center."[11]

After September 11, 2001, the focus on protecting critical infrastructures and key assets took on even greater sense of urgency.

2. Critical Infrastructure Protection in a Post-9/11 World

Shortly after September 11, 2001, President Bush named Pennsylvania Governor Tom Ridge to lead the White House Office of Homeland Security (OHS). Initially, OHS was responsible for the developing and coordinating homeland security strategy.[12]

a. National Strategy for Homeland Security – A Work in Progress

In July 2002, the White House issued the *National Strategy for Homeland Security (*hereinafter the "*Homeland Security Strategy*").[13] The *Homeland Security Strategy* had three objectives: (i) to prevent terrorist attacks within the United States; (ii) to reduce America's vulnerability to terrorism; and (iii) to minimize the damage and recover from attacks that do occur.[14] The *Homeland Security Strategy* specifically addressed the role of the Private Sector:

> Given our traditions of limited government, the American private sector provides most of our goods and services . . . .
>
> A **close partnership between the government and private sector is essential** to ensuring that existing vulnerabilities in our critical are identified and eliminated as quickly as possible. **The private sector should conduct risk assessments on holdings and invest in systems to protect key assets.** The internalization of

[8] Presidential Decision Directive No. 63, *supra* note 7.
[9] Eventually, this Center would be incorporated into DHS. *See* http://www.dhs.gov/xabout/history/editorial_0133.shtm
[10] *Id.*
[11] *Id.*
[12] *See* Executive Order 13228; available at http://www.fas.org/irp/offdocs/eo/eo-13228.htm
[13] *See* THE WHITE HOUSE, THE NATIONAL STRATEGY FOR HOMELAND SECURITY (2002) *available at* http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf
[14] *Homeland Security Strategy* at 1.

> these costs is not only a matter of good corporate citizenship but also an essential safeguard of economic assets for shareholders, employees, and the Nation.[15]
>
> (emphasis added)

The *Homeland Security Strategy* continued to emphasize a cooperative and voluntary partnership between government and the private sector. This was necessary because the President and Congress had not yet formed DHS, nor did the federal government have broad legislative and regulatory authority in the area of homeland security.

An updated version of the *Homeland Security Strategy* was published in 2007 (hereinafter the "*Revised Homeland Security Strategy*").[16] The *Revised Homeland Security Strategy* made several changes to the *Homeland Security Strategy*. First, it reformulated the objectives to broaden the objectives to cover non-terrorist events including "[protection of] the American people, our critical infrastructure, and key resources."[17] While government is typically in the best position to assess potential threats[18] against the United States, industry is in a better position to recognize its own vulnerabilities, recommend resiliency strategies, deploy technology, implement protective measures and hopefully do so in a cost-effective manner. The *Revised Homeland Security Strategy* acknowledges "that effective preparation for catastrophic natural disasters and man-made disasters, while not homeland security *per* se, can nevertheless increase the security of the Homeland."[19] But one of the most striking changes was the clear sense of Post-Hurricane Katrina realism about our ability to protect against every type of catastrophe:

> "Recognizing that the future is uncertain and that we cannot envision or prepare for every potential threat, **we must understand and accept a certain level of risk as a permanent condition**. Managing homeland security risk requires a disciplined approach to resource prioritization and the diversification of protective responsibilities across the full spectrum of our Nation's homeland security partners."[20]
>
> (emphasis added)

---

[15] *Id.* at 12.
[16] *See* THE WHITE HOUSE, THE NATIONAL STRATEGY FOR HOMELAND SECURITY (2007) *available at* http://www.dhs.gov/xlibrary/assets/nat_strat_homelandsecurity_2007.pdf; According to DHS the *Revised Homeland Security Strategy*, builds directly from the *Homeland Security Strategy* and reflects an increased understanding of the terrorist threats confronting the United States, incorporates lessons learned from exercises and real-world catastrophes – including Hurricane Katrina – and proposes new initiatives and approaches; *see* http://www.dhs.gov/xabout/history/gc_1193938363680.shtm
[17] *Revised Homeland Security Strategy*, p. 1
[18] In April 2005, the Federal interagency process led by the Homeland Security Council prepared fifteen all-hazard planning scenarios; *available at* http://media.washingtonpost.com/wp-srv/nation/nationalsecurity/earlywarning/NationalPlanningScenariosApril2005.pdf
[19] *Id.* at 3.
[20] *Id.* at p. 25

The *Revised Homeland Security Strategy* also discusses what, in the minds of many, is the most important concept in homeland security preparedness: risk management. According to the new strategy:

> "The assessment and management of risk underlies the full spectrum of our homeland security activities, including decisions about when, where, and how to invest resources that eliminate, control or mitigate risks **In the face of multiple and diverse catastrophic possibilities, we accept that risk – a function of threats, vulnerabilities, and consequences – is a permanent condition. We must apply a risk-based framework across all homeland security efforts** in order to identify and assess potential hazards (including their downstream effects), determine what levels of relative risk are acceptable, and prioritize and allocate resources among all homeland security partners, both public and private, to prevent, protect against, and respond to and recover from all manner of incidents."[21]
>
> (emphasis added)

In sum, the *Homeland Security Strategy* and the *Revised Homeland Security Strategy* lay out the nations' homeland security objectives; emphasize the essential role of the private sector in any efforts; and underscore that in a post 9/11 and post-Hurricane Katrina world, risk is a permanent condition that can only be addressed through a risk-management framework.

b. Strategies for Physical Protection of Critical Infrastructures and Key Assets and to Secure Cyberspace

In February 2003, the Bush Administration published The *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* (hereinafter "*Critical Infrastructure Strategy*") and the *National Strategy to Secure Cyberspace* (hereinafter "*Cyberspace Strategy*").[22] These strategies reflect "a transition to an important new national cooperative paradigm."[23] The *Critical Infrastructure Strategy* noted:

> "The basic tenets of *homeland* security are fundamentally different from the historically defined tenets of *national* security. Historically, securing the United States entailed the projection of force outside of our borders. We protected ourselves by 'keeping our neighborhood safe' in the global, geopolitical sense. The capability and responsibility to carry out this mission rested largely with the federal government. **The emergence of international terrorism within our borders has moved the front line of domestic security to Main Street, USA . . .**

[21] *Id.* at p. 41
[22] *See* THE WHITE HOUSE, THE NATIONAL STRATEGY FOR THE PHYSICAL PROTECTION OF CRITICAL INFRASTRUCTURES AND KEY ASSETS (2003) *available at* http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf; *see also*, THE WHITE HOUSE, THE NATIONAL STRATEGY TO SECURE CYBERSPACE (2003) *available at* http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf
[23] Critical Infrastructure Strategy, p. 3.

> Acting alone the federal government lacks the comprehensive set of tools and competencies required to deliver the most effective protection and response for homeland security threats. Therefore, **to combat the threat terrorism poses for our critical infrastructures and key assets, we must draw upon the resources and capabilities of those who stand on the new front lines – our local communities and private sector entities that comprise our national critical infrastructure sectors.**[24]
>
> (emphasis added)

As previously noted, critical infrastructures are vital systems and assets that if incapacitated or destroyed would have a debilitating or paralyzing impact on the United States' national security, economic security, public health or safety, or any combination thereof.[25] The *Critical Infrastructure Strategy* identified the following critical infrastructures:

- Agriculture and Food
- Water
- Public Health
- Emergency Services
- Defense Industrial Base
- Telecommunications
- Energy
- Transportation
- Banking and Finance
- Chemical Industry and Hazardous Materials
- Postal and Shipping
- [Critical Manufacturing][26]

Although not classified as critical infrastructures, there are also important sites/resources for which additional security considerations are necessary – these are referred to as key assets. Key Assets are defined as:

[24] *Id.*
[25] 42 U.S.C. § 5195c(e)
[26] The "Critical Manufacturing" Sector was added in March 2008. For a current list of critical infrastructures and key assets, *see* http://www.dhs.gov/xprevprot/programs/gc_1189168948944.shtm

> "individual targets whose destruction could cause large-scale injury, death, or destruction of property, and/or profoundly damage our national prestige, and confidence. Such assets and activities alone may not be vital to the continuity of critical services on a national scale, but an attack on any one of them could produce, in the worst case, significant loss of life and/or public health and safety consequences."[27]

The *Critical Infrastructure Strategy* identified five key assets:

- National Monuments and Icons
- Nuclear Power Plants
- Dams
- Government Facilities
- Commercial Key Assets[28]

In sum, these two strategies provide a conceptual framework for identifying potential vulnerabilities and a new "national cooperative paradigm" to better protect the country. Although these strategies are a significant step forward in how we "think" about homeland security and what it is we are trying to protect, additional detailed planning and statutory authorities must follow. As will be discussed below, once DHS was formed, a more focused effort on homeland security policy and planning would take place.

c. Formation of the Department of Homeland Security:

Primacy of the Private Sector

In the summer of 2002, President George W. Bush proposed the formation of the Department of Homeland Security. This would be the most significant reorganization of the federal government in more than fifty years.[29] On November 25, 2002, the Homeland Security Act of 2002 (hereinafter the "HSA") was enacted.[30] DHS would incorporate more than twenty agencies, offices and elements from other Departments.[31] Even a cursory reading of the HSA underscores the primacy of the private sector in accomplishing the broad mission of homeland security.

---

[27] Critical Infrastructure Strategy, p. 7.
[28] *See generally* Critical Infrastructure Strategy
[29] The President's proposal is *available at* http://www.dhs.gov/xlibrary/assets/book.pdf
[30] Homeland Security Act of 2002, Pub. L. No. 107-296, § 214, 116 Stat. 2125 (2002)(hereinafter "HSA"), *available at* http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf
[31] For more information about what entities were incorporated into the new Department s*ee* http://www.dhs.gov/xabout/history/editorial_0133.shtm

For instance, one of the first provisions in the HSA directs the Secretary to appoint a Special Assistant (now an Assistant Secretary)[32] to advise the Secretary on private sector matters including: (i) strategic communications; (ii) impact of regulations; (iii) impact of agency activity; (iv) creating and managing advisory councils; (v) federal funding of technology development; (vi) public-private partnerships; and (vii) development of "best practices" for CIP.[33] The Private Sector Office's (PSO) role was to think strategically about homeland security and to do so in a broader, cross-cutting, non-sector specific manner. One of the most important focuses of the PSO is to help make the "business case for homeland security." In other words, in order to get the private sector to invest in security, it must make financial sense (i.e., there must be a return on investment)[34].

Title II of the HSA entitled "Information Analysis and Infrastructure Protection" established a directorate to focus on threat analysis to partner with the private sector on improving CIP.[35] One key aspect of CIP is the government's need to obtain information from private sector companies about potential vulnerabilities. The HSA developed a program for protecting such information – referred to as "Critical Infrastructure Information" (hereinafter "CII"). CII will be discussed in more detail below. Although DHS has been reorganized several times, CIP continues to be one of its essential missions. Another area where the private sector can make great contributions is in the development of technology to protect against attack. However, at the time that the HSA was being debated in Congress there was some hesitation on behalf of the private sector to become involved in developing technology because of possible tort liability. Consequently, Congress included in the HSA certain "risk management" and "litigation management" protections for sellers of qualified equipment.[36] In the final analysis, the HSA led to a significant reorganization in the federal government, but it did not give a lot of new authorities to the Department, nor did it provide much specific guidance as to how DHS would improve CIP and how it would work with the private sector.

d. National Infrastructure Protection Plan (NIPP): Unifying Structure for a National Protection and Resiliency Program

Towards the end of DHS's first year, the Bush Administration published Homeland Security Presidential Directive 7 (''HSPD-7''). HSPD-7 established the U.S. policy for ''identify[ing] and

[32] *See* http://www.dhs.gov/xabout/structure/gc_1157655281546.shtm
[33] HSA § 102(f)
[34] Examples of the type of business case that can be made include the business benefits of hurricane preparedness and supply chain security. Hurricane preparedness positively affects employee morale, job satisfaction, enthusiasm, and compassion, even when a hurricane does not hit; *See* Florida State University's Professor Wayne Hochwarter's study on hurricane preparedness, *press release available at* http://unicomm.fsu.edu/pages/releases/2006_08/HurricanePreparedness.html; According to a Stanford University Study, supply chain security has business benefits that outweigh costs; *available at* http://www.nam.org/~/media/Files/s_nam/docs/237300/237208.pdf.ashx
[35] The Directorate has since been dissolved and the CIP mission has been folded into the National Protection and Programs Directorate, *see* http://www.dhs.gov/xabout/structure/editorial_0794.shtm.
The information analysis mission has been incorporated into the Office of Intelligence and Analysis, *see* http://www.dhs.gov/xabout/structure/gc_1220886590914.shtm
[36] *See* "Support Anti-Terrorism by Fostering Technologies Act of 2002 (SAFETY Act)"; 6 U.S.C. § 441-44 (2006).

prioritiz[ing] United States critical infrastructure and key resources...'' and mandates a national plan to achieve that policy.[37]

Pursuant to the requirements of HSPD-7, DHS released the original National Infrastructure Protection Plan (''NIPP'') in June 2006. However, the planning process is evolutionary and the 2006 NIPP was replaced in February 2009 with a revised edition that takes into account recent developments.[38] The NIPP underscores the importance of protecting critical infrastructures and key resources (CIKR) and establishes as its overarching goal to:

> Build a safer, more secure, and more resilient America by preventing, deterring, neutralizing, or mitigating the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit elements of the Nation's CIKR; and to strengthen national preparedness, timely response, and rapid recovery of CIKR in the event of an attack, natural disaster, or other emergency.[39]

The purpose of the NIPP is to provide "the **unifying structure** for the integration of existing and future **CIKR protection efforts and resiliency strategies** into a single national program . . .."(emphasis added)[40] As mentioned earlier, because the private sector controls the lion's share of the nation's CIKR, industry's voluntary participation in the NIPP's risk management process is critical. The NIPP calls for, among other things, the effective distribution of funding and resources, strong public-private partnerships, multi-directional information sharing, and a comprehensive risk management framework.

The NIPP uses a risk-management framework and identifies several initiatives, goals and benchmarks for infrastructure protection. Because it is impossible to predict with certainty the exact nature of a disaster or catastrophic incident, the NIPP's risk-management framework utilizes an all-hazards approach and is applied on an asset, system, network, or function basis, depending on the fundamental characteristics of the particular CIKR sector. For example, critical infrastructure sectors primarily dependent on fixed assets and physical facilities (e.g., petro-chemical plants, manufacturing facilities) may require an asset-by-asset physical protection assessment while sectors with dispersed or more virtual assets (e.g., telecommunications and information technology) may require a business continuity/resiliency approach that focuses on networks, systems, functions and the need for redundancy.

---

[37] The White House, Homeland Security Presidential Directive-7 (December 17, 2003) available at http://www.dhs.gov/xabout/laws/gc_1214597989952.shtm; For a list of all Homeland Security Presidential Directives *see* http://www.dhs.gov/xabout/laws/editorial_0607.shtm

[38] *See* The U.S. Department of Homeland Security, National Infrastructure Protection Plan (hereinafter "NIPP"), (2009), *available at* http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[39] *Id.* at 9.

[40] *Id.*

The NIPP requires specific government agencies to work closely with members of the private sector to obtain the information necessary to ensure that sector assets are adequately represented and that sector and cross-sector dependencies and interdependencies can be identified and analyzed. HSPD-7 designates executive departments and agencies as Sector-Specific Agencies (''SSAs''). SSA designations reflect the subject-matter expertise of the particular department or agency when applied to a distinct critical infrastructure sector (i.e., the Department of Treasury is the SSA for the financial services sector; the Department of Defense is the SSA for the defense industrial base sector). According to then Secretary Chertoff:

> Within the **CIKR protection** mission area, national priorities must include preventing catastrophic loss of life and managing cascading, disruptive impacts on the U.S. and global economies across multiple threat scenarios**.** Achieving this goal **requires a strategy that appropriately balances resiliency . . . with focused, risk-informed prevention, protection, and preparedness activities so that we can manage and reduce the most serious risks that we face.**
>
> These concepts represent the pillars of the [NIPP] and its 18 supporting Sector-Specific Plans (SSPs). The plans are carried out in practice by an integrated network of Federal departments and agencies, State and local government agencies, private sector entities, and a growing number or regional consortia – all operating together within a largely voluntary CIKR protection framework.[41]
>
> (emphasis added)

Because DHS has very little regulatory authority in the area of CIP (with the most notable exception being the chemical sector discussed below), it is relying on a cooperative effort. The NIPP uses a partnership model that is intended to encourage relationships and improve coordination within individual sectors and across sectors.[42] Each of the sectors and SSAs is responsible for developing an SSP that addresses some of the particular challenges, threats and characteristics in their respective sector.[43]

e. CIP Advisory Councils: Getting Public Feedback

DHS is constantly seeking feedback from the private sector regarding CIP and ways to improve the NIPP. On October 16, 2001, President Bush established the National Infrastructure Advisory Council (NIAC) to provide him "advice on the security of information systems for critical infrastructure supporting other sectors of the economy: banking and finance, transportation, energy, manufacturing, and emergency government services."[44] The NIAC still meets regularly and provides the President periodic advice and prepares reports on relevant topics.[45] Additionally, former Secretary Chertoff formed the Critical Infrastructure

[41] *Id.* at Preface
[42] For a description of the partnership model *see* http://www.dhs.gov/xprevprot/partnerships/editorial_0206.shtm
[43] Several of these SSPs are *available at* http://www.dhs.gov/xprevprot/programs/gc_1179866197607.shtm
[44] *See* Executive Order 13286 revising Executive Order 13231; available at http://www.dhs.gov/xlibrary/assets/EO_13231_Revised.pdf
[45] *See* http://www.dhs.gov/xprevprot/committees/editorial_0353.shtm for more information on the NIAC.

Partnership Advisory Council (''CIPAC'') in March 2006, to encourage collaboration between government and the private sector. The purpose of the CIPAC is to improve the sharing of sensitive information with the private sector on critical infrastructure and to encourage greater collaboration for NIPP and other purposes.[46] Because of the sensitive nature of CIPAC discussions, CIPAC is exempt from certain public disclosure laws and many meetings will be closed to public participation but some ''meetings will be open [to the public] as feasibly consistent with security objectives.''[47]

In sum, the NIPP and supporting SSPs provide a coordinated approach to CIKR protection and outline roles and responsibilities for federal, state, and local governments, the private sector, and other nongovernmental organizations.

f. State Infrastructure Protection Plans

Because each state is unique and has its own distinct assets and vulnerabilities, individual states have begun developing their own state infrastructure protection plans or committees to coordinate efforts. For instance, the Commonwealth of Virginia has published its "Critical Infrastructure Protection and Resiliency Strategic Plan" (hereinafter "Virginia Critical Infrastructure Plan").[48] Similar to the NIPP, the Virginia Critical Infrastructure Plan incorporates into its planning "Private Sector Owners and Operators" and indicates that they are "responsible for taking action to support risk management planning and investments in security as a necessary component to prudent business planning and operations."[49] The federal and state plans are intended to be complementary.[50]

g. National Response Framework (NRF)

The National Response Framework ("NRF") was published in January 2008.[51] The NIPP and NRF are synchronized with each other. The NRF provides guidance for government at all levels and the private sector in preparing for, responding to and recovering from disasters and emergencies of whatever origin. It replaces the previous National Response Plan (NRP) that had received significant criticism after Hurricane Katrina. The NRF attempts to incorporate many of the hard-learned lessons of Hurricane Katrina. Before Hurricane Katrina, much of the focus was on preventing another terrorist attack on U.S. soil. After Hurricane Katrina, many policy-makers raised concerns about whether the federal government had been unprepared for a catastrophic natural disaster because of flawed government reorganization and over-emphasis on preventing terrorist attacks. It was also more fully recognized that some disasters would be difficult if not

[46] Charter of the Critical Infrastructure Partnership Advisory Council *available at* http://www.dhs.gov/xlibrary/assets/CIPAC_charter.pdf
[47] Infrastructure Partnership Advisory Council, 71 Fed. Reg. 14930, 14932 (Mar. 24, 2006); *available at* http://edocket.access.gpo.gov/2006/06-2892.htm
[48] Commonwealth of Virginia "Critical Infrastructure Protection and Resiliency Strategic Plan" *available at* http://www.ocp.virginia.gov/Initiatives/documents/VA_Plan.pdf
[49] *Id.* at § 2.2.4.
[50] *Id.* at § 5.2.
[51] The National Response Framework (hereinafter ("NRF"); available at http://www.fema.gov/pdf/emergency/nrf/nrf-core.pdf

impossible to completely protect against and therefore policy makers and private sector operators needed to develop strategies for recovery after an event.

As indicated by DHS, the NRF's goal is to establish a comprehensive, national, all-hazards approach to domestic incident response. Similar to the NIPP, the NRF remains an evolving document. Also, like the NIPP, the NRF lays out roles and responsibilities for key personnel in government agencies as well as in the private sector. Through this public-private coordination, the NRF seeks to improve emergency response and recovery. To do this, the NRF calls for leaders at all levels to create management plans for potential emergencies, as well as response plans that incorporate governmental and private sector actions. The NRF also calls for information sharing, resource allocation, and response integration in the event of a terrorist attack or natural disaster. After the initial emergency response, the NRF calls for planning to meet basic needs and returning to self-sufficiency.

(i) Role of the Private Sector

The NRF specifically addresses the role of the private sector:

> "Private sector organizations play a key role before, during, and after an incident. First, they must provide for the welfare and protection of their employees in the workplace. In addition, emergency managers must work seamlessly with businesses that provide water, power, communication, networks, transportation, medical care, security, and numerous other services upon which both response and recovery are particularly dependent."[52]

The NRF identifies seven critical planning and preparedness responsibilities for the private sector:

- "Planning for the protection of employees, infrastructure, and facilities.
- Planning for the protection of information and the continuity of business operations.
- Planning for responding to and recovering from incidents that impact their own infrastructure and facilities.
- Collaborating with emergency management personnel before an incident occurs to ascertain what assistance may be necessary and how they can help.

[52] NRF, p. 18.

- Developing and exercising emergency plans before an incident occurs.

- Where appropriate, establishing mutual aid and assistance to provide specific response capabilities.

- Providing assistance (including volunteers) to support local emergency management and public awareness during response throughout the recovery process."[53]

The NRF core document is a detailed ninety pages; however, it does not include the additional annexes which collectively add up to almost 300 pages.[54] We will briefly focus on two annexes which have particular relevance to the private sector.

(ii) Critical Infrastructure and Key Resources Support Annex (CIKR Annex)

The Critical Infrastructure and Key Resources Support Annex ("CIKR Annex")[55] describes the processes through which the principles of the NRF will be implemented to assess, prioritize, protect, and restore critical infrastructure and key resources. The Annex describes the roles and responsibilities, establishes a concept of operations, and outlines incident related actions for CIKR preparedness, protection, response, recovery, restoration and continuity of operations. Among other things, the Annex provides for the process for requesting CIKR-related federal assistance and public-private coordination.

(iii) Private Sector Annex

The Private Sector Coordination Support Annex ("Private Sector Annex")[56] describes the policies, responsibilities, and operations for emergency management activities involving the private sector. In the event of an emergency, DHS will coordinate communications with the private sector and utilize a private sector advisory group to provide advice on incident management. While the CIKR Annex focuses on the CIKR efforts of the private sector, the Private Sector Annex deals with the remaining portion of the private sector. This Annex provides specific guidance for incidents that require a coordinated federal response and which involve the private sector, whether in impacts, resources, regulations, or emergency management.

h. National Incident Management System (NIMS)

In February of 2003, President Bush published Homeland Security Presidential Directive 5 (''HSPD-5''). HSPD-5 directed the Secretary of Homeland Security to establish a national

[53] NRF, pp. 19-20.
[54] NRF Annexes are available at http://www.fema.gov/pdf/emergency/nrf/nrf-annexes-all.pdf
[55] Available at http://www.fema.gov/pdf/emergency/nrf/nrf-support-cikr.pdf
[56] Available at http://www.fema.gov/pdf/emergency/nrf/nrf-support-private.pdf

incident management system.[57] While the NRF provides the structure and mechanisms for the development of nationwide policy, the National Incident Management System ("NIMS")[58] provides a consistent template for all levels of government, the private sector, and nongovernmental organizations to work together in the management of incidents. The original version of NIMS was announced in March of 2004 and an updated version was published in December 2008.

NIMS is not an operational plan, but rather a comprehensive framework for emergency response that identifies the key principles, best practices, roles, and structures culled from existing emergency management. By using a single incident management framework, NIMS will give emergency management and response personnel a standardized system that has the flexibility to be adapted for emergency management and incident response at all levels. NIMS focuses on five areas: preparedness, communications and information management, resource management, command and management, and ongoing management and maintenance. Within each of these areas, NIMS supplies concepts and principles to be used in emergency management and incident response.

According to NIMS because "[t]he private sector plays a vital role in emergency management and incident response [it] should be incorporated into all aspects of NIMS."[59] Many private sector entities will be involved in "critical aspects of emergency response and incident management" and governments at all levels should work closely with the private sector to develop a "common set of expectations" regarding roles and responsibilities.[60] NIMS also looks to the private sector as a possible source of best practices for emergency management and incident response.[61]

B. Federal Regulation of Critical Infrastructure

While most of the policy and strategy development of CIP has been largely voluntary and collaborative in nature, in recent years Congress has begun to look increasingly at regulation of critical infrastructure sectors. Since 9/11, Congress has passed several pieces of security legislation that directly impact CIKR sectors including the Aviation and Transportation Security Act, the Maritime Transportation Security Act, Electricity Modernization Act of 2005, The Security and Accountability for Every (SAFE) Port Act of 2006, The bulk of CIP/sector specific security regulation has been in the areas of transportation and chemical security.

The new chemical security regulation may become the standard for future security regulations in other sectors. On April 9, 2007, DHS published its Interim Final Rule on Chemical Facility Anti-Terrorism Standards (CFATS) (the ''Rule''), which establishes risk-based

[57] HSPD-5 is available at http://www.dhs.gov/xnews/releases/press_release_0105.shtm
[58] National Incident Management System (hereinafter "NIMS"); available at http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf
[59] NIMS at p.15.
[60] *Id.*
[61] *Id.*

performance standards for the security of high-risk chemical facilities.[62] Risk-based performance standards seek a specific result or outcome, but do not direct the manner or means of achieving it; therefore, precise security measures are not mandated. For instance, where CFATS sets as an outcome to "secure and monitor the perimeter of the facility"; DHS is prohibited from mandating that only an electric fence and closed-circuit camera system can be used to achieve this outcome. Instead, DHS using its discretion might accept motion detectors and a patrolling security guard as a method of securing the required outcome.

The Rule also includes an appendix entitled ''DHS Chemicals of Interest'' (''Appendix A'**),**[63] which is a list of chemical substances that DHS considers potentially dangerous. Chemical facilities that possess a listed chemical and meet the threshold requirements of Appendix A or are otherwise identified by DHS as potentially high-risk, must complete a questionnaire.[64] The questionnaire elicits information to help DHS determine whether a chemical facility needs to meet the additional requirements of the Rule. If DHS determines that a facility is high-risk, it will be regulated. As such, it will be referred to as a ''Covered Facility,'' which the Rule defines as ''a chemical facility determined by the Assistant Secretary to present high levels of security risk, or a facility that the Assistant Secretary has determined is presumptively high risk....''[65]

Depending upon the perceived risk, Covered Facilities will be placed in one of four risk tiers with commensurate security obligations. DHS provides specific tier requirements in guidance documents. Covered Facilities are required to prepare Security Vulnerability Assessments (''SVAs'') and Site Security Plans ("Site Plans') that must be approved by DHS. In short, SVAs identifies facility security vulnerabilities. The Site Plans include measures that satisfy the identified risk-based performance standards. In certain circumstances, Covered Facilities are permitted to submit Alternate Security Programs, rather than an SVA, Site Plans or both.

CFATS may be a model for how other CIKR will be regulated in the future. Both Congress and DHS recognized that there is no cookie-cutter approach to CIP. Each industry and each company has a unique set of vulnerabilities. In theory, risk-based performance standards are an effort to reach a goal of greater preparedness and protection without mandating the precise method to achieve it. Because the CFATS program is still in the process of being implemented, it is uncertain whether this security regulation scheme will achieve the results that Congress desires or whether a similar security program would work with other industries.

III. The Private Sector and Information Sharing

[62] Chemical Facility Anti-Terrorism Standards; Final Rule 72 Fed. R. 17688 (April 9, 2007) (to be codified at 6 CFR Part 27)(hereinafter "CFATS Rule"); *available at* http://edocket.access.gpo.gov/2007/E7-6363.htm; for a more detailed discussion of this rule see New Federal Rule Dictating Anti-terrorism Standards for Chemical Facilities by Joe Whitley and Ava Harter; *available at* http://www.wlf.org/upload/WhitleyCLN.pdf

[63] Chemical Facility Anti-Terrorism Standards; Final Rule Appendix A, 72 Fed. R. 65396 (November 20, 2007); *available at* http://www.dhs.gov/xlibrary/assets/chemsec_appendixafinalrule.pdf

[64] DHS may determine at any time that a chemical facility presents a high level of security risk based on any information that, in the DHS Secretary's discretion, indicates the potential that a terrorist attack involving the facility could result in significant adverse consequences for human life or health, national security or critical economic assets. CFATS at 17731.

[65] *Id.* at 17730

One of the clear failings of September 11, 2001, was inadequate information sharing regarding potential terrorist threats. Developing an environment where useful and actionable information is shared with appropriate persons and entities has become a top priority for policymakers. A top down only approach does not work. Emergency planners need private sector entities to share information about vulnerabilities and potential consequences resulting from a disaster. Recognizing that such private sector information must be protected, the government has developed several programs to give assurances that the information will not fall into the wrong hands or be used for unintended purposes.

A. Information Sharing Environment

Congress passed and the President signed the Intelligence Reform and Terrorism Prevention Act of 2004 (hereinafter "IRTPA").[66] Section 1016 of IRTPA directed: (i) the establishment of the Information Sharing Environment ("ISE"); (ii) designation of a Program Manager and (iii) creation of an Information Sharing Council. It specifically includes the private sector as part of the ISE.[67] The Program Manager has developed a website[68] and prepared an ISE Implementation Plan (hereinafter "ISE Plan")[69] that explains ISE goals and roles. According to the ISE Plan, a trusted partnership is required:

> among all levels of government in the United States, the private sector, and our foreign partners, in order to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States by the effective and efficient sharing of terrorism and homeland security information.[70]

The ISE Plan lists six information sharing objectives[71] of the private sector[72] – these primarily fall into two areas: (i) ensuring that the private sector obtains risk-oriented and actionable information from the government; and (ii) ensuring that there are protections for information that the private sector provides the government (including liability limitations for private sector entities that provide the information).

In October 2007, the *National Strategy for Information Sharing* (hereinafter "*Information Sharing Strategy*") was published.[73] The *Information Sharing Strategy* once again emphasizes the important role that the private sector plays in protecting critical infrastructure and the federal government's efforts to developing a networked approach to information sharing:

---

[66] Intelligence Reform and Terrorism Prevention Act of 2004 (hereinafter ("IRTPA"), Pub. L. 108-458, 118 Stat. 3638; *available at* http://www.ise.gov/docs/guidance/irtpa.pdf
[67] *Id.* at § 1016 (b)(2).
[68] *See* http://www.ise.gov
[69] ISE Implementation Plan (November 2006) *available at* http://www.ise.gov/docs/reports/ise-impplan-200611.pdf
[70] *Id.* at Executive Summary (xiii).
[71] *Id.* at 20.
[72] *Also* see http://www.ise.gov/pages/partner-private.html
[73] The National Strategy for Information Sharing (October 2007) (hereinafter "Information Sharing Strategy"); *available at* http://www.ise.gov/docs/nsis/nsis_book.pdf.

> Efforts to improve information sharing with the private sector have initially focused on sharing with the owners and operators of our Nation's [CIKR]. In accordance with the [NIPP], **we are currently implementing a networked approach to information sharing that allows distribution and access to information both horizontally and vertically using secure networks and coordination mechanisms, allowing information sharing and collaboration within and among sectors.** It also enables multi-directional information sharing between government and industry that focuses, streamlines, and reduces redundancy in reporting to the greatest extent possible.[74]
>
> (emphasis added)

The *Information Sharing Strategy* identifies several mechanisms that CIKR operators can utilize for information sharing, including:

> Sector Coordination Councils, Government Coordination Councils, National Infrastructure Coordinating Center, Sector-level Information Sharing and Analysis Centers [ISACs], DHS Protective Security Advisors, the DHS Homeland Infrastructure Threat and Risk Analysis Center (HITRAC), and State and major urban area fusion centers.[75]

Of these it should be noted that according to the ISE Program Manager, federal departments and agencies will primarily provide terrorism-related information to State, local, and tribal authorities primarily through major urban area fusion centers.[76] According to the ISE website, there are 66 of these fusion centers operating or are being established in States and localities across the country.[77]

B. Protected Critical Infrastructure Information

Although some information relating to homeland security and infrastructure is properly classified, much of it is not. This is recognized in the HSA, which called for new designations and processes in dealing with information relevant to homeland security.[78] DHS has three unclassified programs for protecting sensitive information: (i) Protected Critical Infrastructure Information ("PCII"), which was created by the HSA; (ii) Sensitive Security Information ("SSI"), with its roots in the Air Transportation Security Act of 1974; and (iii) chemical vulnerability information ("CVI"), which was first introduced in the CFATS final rule.[79] The designation and sharing of all other controlled unclassified information ("CUI") is addressed in a memo issued by President Bush on the subject – all three of the DHS programs are exempt.[80]

[74] *Id.* at 21.
[75] *Id.*
[76] *See* http://www.ise.gov/pages/partner-fc.html
[77] *Id.*
[78] Homeland Security Act of 2002, *supra* at § 214
[79] *See* 72 Fed.Reg. 72,737 (April 9, 2007)
[80] Presidential Memorandum for the Heads of Executive Departments and Agencies regarding "Designation and Sharing of Controlled Unclassified Information" (May 7, 2008) *available at* http://www.fas.org/sgp/bush/cui.html

Although a detailed discussion of the three DHS programs is beyond the scope of this chapter,[81] we will briefly discuss PCII, the program that provides the strongest protections.

Historically, the private sector has been very hesitant to share sensitive business and vulnerability information with the government. Absent protection from the disclosure requirements of the Freedom of Information Act (''FOIA''), State and local disclosure laws and discovery in private litigation, the private sector has resisted sharing sensitive information with the federal government. Recognizing this private sector concern, Congress developed a program to protect information that is voluntarily provided. HSA provides a critical infrastructure information exemption from FOIA when private companies provide it voluntarily.[82] When information is designated as PCII, government disclosure is limited to authorized parties for specific homeland security purposes. By participating in the PCII program,[83] the private sector will be helping government better identify risks and vulnerabilities in particular sectors or industries, thereby helping to safeguard and prevent disruption to the American economy and way of life.

IV. Private Sector Preparedness

> Terrorism forces us to make a choice. We can be afraid. Or, we can be ready.[84]
>
> - Secretary Tom Ridge

Both government and the private sector have a responsibility to plan for disasters. We have already discussed a number of the strategies, planning directives/documents and regulations that the federal government has developed that impact the private sector. Now let's focus specifically on what individuals and companies in the private sector can do.

A. Individuals

Disaster planning begins with individuals and families. If citizens in the private sector take personal responsibility for their own safety and welfare, then in the event of a disaster, emergency responders can direct their efforts to those in extraordinary situations: the elderly, the poor, people requiring medical attention or people with physical disabilities, etc.[85] DHS has developed a national public service advertising campaign that focuses on readiness – the main themes are "Prepare, Plan and Stay informed."[86] Ready.gov, the featured website, provides information about a readiness kit, a family emergency plan, information about some of the potential threats (e.g., pandemic flu). It also provided links to sites with state and local information. According to DHS,

---

[81] For a detailed discussion of information sharing and protections for private sector information *see* Joe Whitley, et al. *Homeland Security Information Sharing: Protection for Private Sector Information;* Privacy & Data Security Law J. (Sep. 2007), p. 871; *also see* James Conrad, *Protecting Private Security-Related Information from Disclosure by Government Agencies*, 57 ADMIN. L. REV. 715 *(Summer 2005).*

[82] Homeland Security Act of 2002, *supra* at § 214.

[83] For details on the PCII Program *see* http://www.dhs.gov/xinfoshare/programs/editorial_0404.shtm

[84] *See* http://www.ready.gov/america/_downloads/ready_trifold_brochure.txt

[85] A useful book for individuals is Nancy Harvey Steorts, *Safe Living In A Dangerous World: An Expert Answers Your Every Question from Homeland Security to Home Safety.*

[86] *available at* www.ready.gov

individuals should have at a minimum sufficient food and water for three days. DHS makes recommendations for other materials to be included in a readiness kit including: a first aid kit, flash light, radio, cell phone, money etc. As to an emergency plan, DHS makes recommendations regarding out of town contacts, communications in an emergency, sheltering-in-place, etc.

B. Business Continuity Planning (BCP)

As mentioned at the beginning of this chapter, the 9/11 Commission declared that private sector preparedness "is not a luxury; it is a cost of doing business in the post-9/11 world."[87] Because the private sector provides the majority of goods and services in the United States, it is imperative that it be prepared and resilient; otherwise, extended business closures could lead to dangerous shortages threatening the nation's health and welfare. The keys to being prepared are to: (i) develop a business continuity plan (BCP) that addresses a company's vulnerabilities and disaster contingencies; (ii) to coordinate the BCP with state and local authorities; (iii) to educate executives and employees about the BCP; and, (iv)regularly practice the BCP and revise it accordingly with "best practices" as they evolve. There is no one-size fits all approach. The smaller an organization, the less complicated the plan should be. The larger a company the more people and segments of the organization should be involved in preparing the BCP: (i) operations; (ii) human resources; (iii) legal; (iv) financial services; (v) security; (vi) environmental, health and safety; (vii) public affairs; (viii) logistics and technical support, to name a few.

By being prepared, businesses help keep the country safer and more secure. But while private sector preparedness may be a matter of good corporate citizenship, it is also becoming an issue of potential legal liability and there truly is a "cost of doing business in the post-9/11 world."

(i) Potential Legal Liability for Businesses that Fail to Prepare

Emerging law and developing standards suggest an increased legal obligation to plan for emergencies and disasters. It is well established that a corporation's board has an affirmative, fiduciary duty to protect corporate assets.[88] For events occurring after 9/11 and Hurricane Katrina, it will be difficult for the private sector to argue that it is not on notice of the potential for man-made or natural disasters and that such events are not foreseeable.

On April 29, 2008, the New York Supreme Court[89] issued a significant ruling that has gotten the attention of many in the business community. The decision involves a finding of liability arising out of the 1993 terrorist bombing of the World Trade Center ("WTC"). The Court held that the Port Authority had a duty to minimize the risk of harm from a terrorist attack.

[87] The 9/11 Commission Report, *supra.* at 398.
[88] *See In re Caremark Derivative Litigation*, 698A.2d 959, 971 (Del. Ch. 1996); Directors and officers must act in good faith, with the level of care that an ordinarily prudent person would exercise in like circumstances, and in a manner they reasonably believe is in the best interest of the corporation.
[89] *Nash v. Port Authority of New York and New Jersey*, 51 AD 3rd 337, 856 N.Y.S. 2d 583 (N.Y. App. Ct. 2008)

This duty is an outgrowth of a landlord's recognized duty to take reasonable measures to minimize foreseeable danger on his premises from third-party criminal activity. In such cases, the Court explained, the duty does not hinge on likelihood or previous experience, but on notice to the landlord. Prior to the bombing in 1993, the Port Authority had hired several consultants to conduct vulnerability assessments which raised concerns about the security of the parking garage and identified the WTC as a high-profile target. The court found that this constituted notice to the Port Authority, but that the Authority failed to take even minimal corrective action. In so concluding, the Court upheld a jury verdict which found the terrorists only 32% liable and the owner of the WTC (Port Authority of New York and New Jersey) 68% liable – the owner of the WTC is more liable than the terrorists who detonated a bomb in the building's parking garage.

Even before this recent court decision, standards for business continuity have been evolving since 9/11. For instance, the New York Stock Exchange (NYSE) and the National Association of Security Dealers (NASD) have mandated specific business continuity practices for their members. The Securities and Exchange Commission (SEC) in April 2004 approved NASD Rule 3510 and 3520 and NYSE Rule 446[90]. The rules require broker-dealer members to develop BCPs that include at least ten essential elements:

- Data back-up and recovery (hard copy and electronic)
- Mission critical systems;
- Financial and operational risk assessment;
- Alternate communications between consumers and members;
- Alternate communications between members and employees;
- Alternate physical location of employees;
- Critical constituent, bank and counter party impact;
- Regulatory reporting;
- Communication with regulators; and
- Prompt access to customer funds and securities in the event that the member determines that it is unable to continue its business functions.[91]

Some homeland security experts have argued that proper compliance with SEC reporting requirements can create incentives for better security. Public companies that are registered with the SEC are required to file periodic reports that disclose material matters to investors. The purpose of these reports is to ensure that investors have a true picture of a company's strengths

[90] Securities and Exchange Release No. 34-49537 (April 7, 2004); *available at* http://www.sec.gov/rules/sro/nasd/34-49537.pdf
[91] *Id.*

and weaknesses before they invest or to help them decide whether they should remain invested. Proponents of homeland security reporting believe that disclosure of vulnerabilities, risks, and strategies in terms of terrorism are clearly material matters and therefore should be included in any filing.[92] By addressing these matters in public filings, the market will more efficiently address disaster preparedness: companies that don't address their vulnerabilities and risks will become disfavored. So far, the evidence is that this type of vulnerability and preparedness reporting has not become standard for public companies.

(ii) NFPA 1600 – Standard for Preparedness

The 9/11 Commission identified three main elements of preparedness: (1) a plan for evacuation, (2) adequate communications capabilities, and (3) a plan for continuity of operations.[93] The 9/11 Commission was concerned that the private sector remains largely unprepared for another attack and asked the American National Standards Institute (ANSI) to develop a consensus on a "National Standard for Preparedness."[94] A voluntary standard was developed known as "NFPA 1600".[95] Secretary Ridge endorsed the standard and the 9/11 Commission recommended that NFPA 1600 become the national standard.[96] NFPA 1600 establishes a "common set of criteria for disaster/emergency management and business continuity programs" and is intended to "provide disaster and emergency management and business continuity programs, the criteria to assess current programs or to develop, implement and maintain aspects for prevention, mitigation, preparation, response, and recovery from emergencies."[97]

The program elements are addressed in Chapter 5 of NFPA 1600. The key elements of the program are:

- risk assessment
- incident prevention
- mitigation
- resource management and logistics
- mutual aid and assistance
- planning

[92] *See* Robert Housman, et al., *New Strategies to Protect America: A Market-Based Approach to Private Sector, available at* http://www.americanprogress.org/kf/fecreport.pdf

[93] *Id.*
[94] *Id.*
[95] *2007 edition available at* http://www.nfpa.org/assets/files/pdf/nfpa1600.pdf
[96] The 9/11 Commission Report, *supra.*
[97] NFPA 1600 §§ 1.1 and 1.2, respectively.

- incident management
- communications and warning
- operational procedures
- facilities
- training
- exercises, evaluations, and corrective actions
- crisis communication and public information
- finance and administration[98]

The concept of risk management is central to an organization being prepared for a disaster. According to NFP 1600, each entity[99] should conduct a "risk assessment" by identifying "hazards, monitor[ing] those hazards, the likelihood of their occurrence, and the vulnerability of people, property, the environment, and the entity itself to those hazards."[100] There are three types of hazard to be evaluated: (i) natural disasters (geological, meteorological, and biological); (ii) human-caused events (accidental and intentional); and (iii) technological caused events.[101] Finally, each entity is to "conduct an impact analysis to determine potential detrimental impacts of the hazards" on key assets or conditions.[102]

To date, NFPA 1600 is the single most significant preparedness standard that has been developed. It is updated on a periodic basis to include the newest preparedness best practices. However a new federal voluntary preparedness program is seeking additional input on how best to develop a preparedness standard.

(iii) FEMA and Private Sector Preparedness

The Federal Emergency Management Agency (FEMA) has an entire division dedicated to private sector preparedness. Its website provides useful and up-to-date information about private sector preparedness; including, hurricane awareness, emergency management guides, funding opportunities, and the new Voluntary Private Sector Preparedness Program (PS-Prep).[103]

[98] *Id.* at § 5.1, et al.
[99] "Entity" is defined as "[a] governmental agency or jurisdiction, private or public company, partnership, nonprofit organization, or other organization that has emergency management and continuity of operations responsibilities." *See* NFPA 1600 § 3.3.5.
[100] *Id.* at § 5.3.1
[101] *Id.* at § 5.3.2
[102] *Id.* at § 5.3.3
[103] *See* http://www.fema.gov/privatesector/index.shtm

In August of 2007, President Bush signed into law the "Implementing Recommendations of the 9/11 Commission Act of 2007" (Public Law No. 110-53).[104] In Section 901(d) of Title IX of that law, Congress specifically identifies NFPA 1600 as being a "voluntary preparedness standard." Title IX also calls for a "Voluntary Private Sector Preparedness Accreditation and Certification Program" (hereinafter "PS-Prep") PS-Prep would be used to designate readiness standards and then to certify compliance. The Secretary has designated the FEMA Administrator as the responsible officer for the program. As such, the FEMA Administrator (currently Craig Fugate) chairs a Private Sector Preparedness Coordination Council, which includes DHS officials from the Science & Technology Directorate, Office of Infrastructure Protection, and Private Sector Office who provide advice regarding development of the program, including the "business case" for why the private sector should work towards certification. Additionally, DHS retained ANSI-ASQ National Accreditation Board (ANAB) to "develop and oversee the certification process, manage the accreditation, and accredit qualified third parties to carry out the certification in accordance with the accepted procedures of the program."[105]

In January of 2009, DHS received comment on a Federal Register Notice (the "Notice"), that sought public feedback on PS-Prep, including: (i) scope of the Program; (ii) content of the voluntary "preparedness" standards to be designated; (iii) existing standards that should be considered; (iv) target criteria for evaluation of comprehensive voluntary preparedness standards; and (v) particular considerations for small businesses.[106] On October 15, 2009, Secretary Napolitano announced new proposed standards for the private sector to improve preparedness for disasters and emergencies and asked for public comment.[107] The proposed standards were prepared by the National Fire Protection Association, the British Standards Institution, and the ASIS International. According to DHS, the proposed standards "were selected based on their scalability, balance of interest and relevance to PS-Prep from a group of 25 standards proposed for consideration . . .."[108] In addition, DHS announced that it is establishing classifications and methods of certifications that focus on the unique circumstances of small businesses. Once DHS receives public comment on the proposed standards during November 2009 and has a chance to evaluate those comments, we can expect the final rule to be published shortly thereafter.

Over time, NFPA 1600 and the PS-Prep may have an impact on developing standards for negligence in disaster litigation.

(iv) Terrorism Risk Insurance Act (TRIA)

One important element in a company's preparedness plan is to have insurance to cover losses as a result of a disaster. However, shortly, after 9/11 many insurance companies began petitioning state insurance commissioners to exclude from insurance policy coverage "acts of terrorism." Policymakers realized that there would be no market for terrorism insurance unless the Federal government was willing to temporarily reinsure against catastrophic loss. Congress

[104] *Available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_public_laws&docid=f:publ053.110.pdf
[105] *Available at* http://www.fema.gov/media/fact_sheets/vpsp.shtm
[106] *Id.*; *available at* http://www.fema.gov/pdf/business/certification/122408_frn.pdf
[107] *See* http://www.dhs.gov/ynews/releases/pr_1255621627246.shtm
[108] *Id.*

enacted the Terrorism Risk Insurance Act (TRIA)[109] as a temporary program until the insurance industry settled down and identified a programmatic market solution. The program is now semi-permanent having been extended several times and most recently was extended through December 31, 2014.[110]

V. The Future Role of the Private Sector In Emergency Preparedness, Planning and Response

Although there have been substantial developments in private sector preparedness, planning, and response, there is still much to be done.

During the 2008 Presidential Campaign, then Senator Barack Obama, published his campaign's plan for homeland security entitled "Strengthening Homeland Security," which among other priorities, discussed in broad terms how an Obama Administration will protect critical infrastructure.[111] In January 2009, the Obama Administration and Secretary Janet Napolitano took over the leadership of DHS. President Obama has announced in general terms his goals and guiding principles.[112] To date, it appears that one of President Obama's top infrastructure preparedness priorities will be securing the nation's communications and information infrastructure (i.e., cyberspace)."[113] President Obama also has been actively engaged in pandemic influenza planning and in October of 2009 signed an emergency declaration for H1N1 flu.[114] This will allow the Secretary of Health and Human Services to waive federal regulatory requirements governing healthcare facilities in response to the flu emergency.

In many regards, Secretary Napolitano has endorsed much of the homeland security strategy and initiatives to date. However, the Secretary has a reputation as a hands-on manager and changes and new programs in the weeks and months ahead can be expected. For instance, in July 2009, Secretary Napolitano announced the formation of a bi-partisan task force to review the controversial Homeland Security Advisory System (HSAS). HSAS is the system that informs the public about terrorist threats and communicates appropriate protective measures within government and throughout the private sector.[116] In September, the Secretary received the task force's

[109] Terrorism Risk Insurance Act, 15 U.S.C. § 6701 (2002).
[110] *See* Terrorism Risk Insurance Extension Act of 2005, Pub. L. No. 109-144 (December 22, 2005); *also see* http://www.ustreas.gov/offices/domestic-finance/financial-institution/terrorism-insurance/
[111] *Available at* http://www.barackobama.com/pdf/issues/HomelandSecurityFactSheet.pdf, p.10.
[112] *See* White House, Homeland Security and Counterterrorism Webpage; *available at* http://www.whitehouse.gov/issues/homeland_security/
[113] *See* White House, Press Statement on Conclusion of the Cyberspace Review; *available at* http://www.whitehouse.gov/the_press_office/Statement-by-the-Press-Secretary-on-Conclusion-of-the-Cyberspace-Review/; A Copy of the Cyberspace Policy Review is available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf
[114] *See* http://www.whitehouse.gov/blog/2009/10/25/president-obama-signs-emergency-declaration-h1n1-flu
[115] Remarks by President Barack Obama regarding the development of a Cybersecurity Strategy *available at* http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/
[116] *See* Press Release Announcing Formation of Task Force to Study HSAS; *available at* http://www.dhs.gov/ynews/releases/pr_1247586668272.shtm

recommendations and is currently working with the President and other Cabinet Secretaries on appropriate follow-up action.

In late July, Secretary Napolitano gave a comprehensive speech to the Council on Foreign Relations regarding the threat of terrorism and some of the Obama Administration's top priorities. The Secretary spoke of our nation's need to make counter-terrorism a more shared endeavor and that we must be in a "constant state of preparedness and not a state of fear."[117] It is clear from her remarks that the Secretary believes that the private sector's capacity to contribute to the nation's preparedness and security has not been fully leveraged. The Secretary reemphasized the Department's "all-hazards approach to preparedness, meaning we prepare for natural disasters as well as terrorist attacks" and she is committed to developing a "culture of preparedness in our communities."[118] Napolitano reiterated the centrality of critical infrastructure protection and the need for DHS to be "more effective at defining our critical assets and providing our private sector and their leaders with the knowledge and technical assistance to help them secure these assets."[119] She specifically highlighted the increasing cyber threat and the Obama administration's new cyber plan to combat that threat. Earlier this summer, she had published a description of DHS focused efforts on cyber security.[120] For instance, the Secretary has specifically tasked the Deputy UnderSecretary for National Protection and Programs Directorate (NPPD) with cyber security responsibilities.

Finally, another critical review process is currently underway which will likely underscore the nation's readiness, infrastructure protection and preparedness priorities is the Department's first ever Quadrennial Homeland Security Review ("QHSR"). Upon completion of the review, DHS will submit a report to Congress with its findings by December 31, 2009.[121] DHS has already begun the process of public outreach and dialogue to solicit ideas and suggestions. According to DHS, this "comprehensive examination includes recommendations regarding the goals and objectives for homeland security and guidance on the Department's programs, assets, capabilities, budget, policies, and authorities."[122] The QHSR will focus on a number of principle areas, including "emergency preparedness, response, and recovery, continuity of operations/continuity of government, and individual and community preparedness."[123] The QHSR should provide a comprehensive Federal road map for the future of emergency planning, response, and recovery.

.

[117] *See* Secretary Napolitano's Speech before the Council of Foreign Relations (July 29, 2009); *available at* http://www.dhs.gov/ynews/speeches/sp_1248891649195.shtm
[118] *Id.*
[119] *Id.*
[120] *See* Secretary Napolitano's posting regarding cybersecurity on DHS website's Leadership Journal; available at http://www.dhs.gov/journal/leadership/2009/06/focused-effort-on-cybersecurity.html
[121] *See generally* http://www.dhs.gov/xabout/gc_1208534155450.shtm
[122] *Id.*
[123] *Id.*