REFJ

The Real Estate Finance Journal

A THOMSON/WEST PUBLICATION

FALL 2007

THOMSON WEST

REFJ

The Real Estate Finance Journal

A THOMSON/WEST PUBLICATION

FALL 2007

Mat #40477635

Recent Developments in Critical Infrastructure Protection

Joe D. Whitley, George A. Koenig, and Steven Roberts*

As the authors explain, critical infrastructures continue to be the object of terrorist plots — and, increasingly, the subject of new legislative and regulatory initiatives.

Economic prosperity and physical security rely on the effective functioning of the nation's 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 impact on security, national economic security, national public health or safety, or any combination of those matters.''[1] More simply put, critical infrastructures are the processes that enable 21st century life: among others things, power plants, transportation systems, financial networks and communications capabilities. In many cases, critical infrastructures are interdependent, and a substantial decrease in capacity in one critical infrastructure sector may have a catastrophic ripple effect regionally or nationally. For these reasons and others, critical infrastructures continue to be the object of terrorist plots — and, increasingly, the subject of new legislative and regulatory initiatives.

History and Background

Although September 11 heightened the importance of critical infrastructure protection, efforts to safeguard them are more than a decade old. After the 1993 World Trade Center attack and the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City, the Clinton administration began to address security concerns related to critical infrastructures.[2] These efforts continued under the Bush administration. Following September 11, the White House published Homeland Security Presidential Directive 7 (''HSPD-7''). HSPD-7 establishes the U.S. policy for ''identify[ing] and prioritiz[ing] United States critical infrastructure and key resources...'' and mandates a national plan to achieve that policy.[3]

Pursuant to the requirements of HSPD-7, the Department of Homeland Security (''DHS'') released the National Infrastructure Protection Plan (''NIPP'') on June 30, 2006. The NIPP underscores the importance of protecting critical infrastructures and establishes the goal of

> [b]uild[ing] a safer, more secure, and more resilient America by enhancing protection of the Nation's [critical infrastructures] to prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency.[4]

The NIPP creates the framework for unifying critical infrastructure protection efforts across the nation and seeks to mitigate risk by deterring threats, mitigating vulnerabilities and minimizing consequences associated with a terrorist attack or other incident.[5] Because the private sector controls 85 percent of the nation's critical infrastructure, industry's voluntary participation in the NIPP's risk management process is critical.[6]

The NIPP embraces a risk-based philosophy to produce a comprehensive, roadmap of national or sector-specific factors that influence critical infrastructure protection activities. This ''risk management framework is tailored and applied on an asset, system,

Joe D. Whitley, a partner in the Washington, D.C., office of Alston & Bird LLP, can be reached at joe.whitley@alston.com. George A. Koenig, counsel in the firm's Washington office, can be reached at george.koenig@alston.com. Steven Roberts can be reached at SRoberts@seroberts.com.

network, or function basis, depending on the fundamental characteristics of the individual [critical infrastructure/key resource] sectors.''[7] For example, critical infrastructure sectors primarily dependent on fixed assets and physical facilities may require a bottom-up, asset-by-asset approach while sectors with diverse and logical assets (i.e., telecommunications and information technology) may require a top-down, business or mission continuity approach that focuses on networks, systems and functions.[8]

Further Defining Critical Infrastructures and Key Resources

As previously noted, critical infrastructures may be defined 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.''[9] Specifically, there are 12 critical infrastructure sectors in the United States:

- Defense Industrial Base
- Food & Agriculture
- Public Health and Healthcare
- Postage and Shipping
- Energy
- Transportation Systems
- Banking and Finance
- Information Technology
- Telecommunications
- Drinking Water and Water Treatment Systems
- Chemicals
- Postal and Shipping[10]

For important sites/resources either not classified directly as a critical infrastructure or for which additional security considerations must be addressed, there are five categories of key assets:

- National Monuments and Icons
- Commercial Nuclear Reactors, Materials and Waste
- Dams
- Emergency Services
- Commercial Facilities (such as prominent commercial buildings, hotels and sports stadiums)[11]

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.[12] To accomplish this, the federal government must acquire information regarding all aspects of critical infrastructure operations.

While laws and regulations permit the government to access critical infrastructure information in some instances, DHS, as a general matter, must rely on the private sectors' willingness to provide information voluntarily. Yet, absent protection from the disclosure requirements of the Freedom of Information Act (''FOIA''), the private sector has been unwilling to share this information with the federal government. Private industry is worried that competitors, litigants seeking to end-run the discovery process or even terrorists and criminals could use FOIA to compel the federal government to share what would not have been in the public domain but for voluntary disclosure.[13]

Recognizing the private sector's resistance to divulge business information, Congress offered a remedy. The Homeland Security Act of 2002 statutorily exempts critical infrastructure information from FOIA when provided voluntarily by the private sector.[14] When information is designated as Protected Critical Infrastructure Information (''PCII''), government disclosure is limited to authorized parties for specific homeland security purposes.

PCII offers significant benefits. DHS has identified some of them, including:

> 1. Proprietary, confidential or sensitive infrastructure information can now be shared with governmental entities who share the private sectors commitment to a more secure homeland;
>
> 2. Information sharing will result in better identification of risks and vulnerabilities, which will help industry partner with others in protecting their assets;
>
> 3. By voluntarily submitting [critical infrastructure information] to the federal government, industry is helping to safeguard and prevent disruption to the American economy and way of life; and
>
> 4. Private industry is demonstrating good corporate citizenship that may save lives and protect communities.[15]

PCII can be used for many homeland security purposes, including analyzing and securing critical infrastructure and protected systems, risk vulnerability assessments and assisting with recovery. DHS published the PCII Interim Rule — the first series of regulations implementing the PCII program — in February 2004.[16]

Despite protection from FOIA offered by the PCII Interim Rule, information flow from the private sector to DHS has been slower than anticipated. Generally, critical infrastructure owners and operators continue to withhold homeland security information from DHS for two reasons. First, while FOIA protection is available, it is not automatic. To obtain the protection, the submitting party must take a series of regulatory steps. Second, even with a statutory exemption from FOIA, many remained concerned that the submitted information may get into the wrong hands. Information that is shared and then released accidentally, for example,

could harm or embarrass the submitting party who offered the information to DHS in good faith with the expectation of protection.

Seeking to improve the PCII Interim Rule, DHS published the PCII Final Rule on September 1, 2006.[17] The PCII Final Rule establishes the scope of the PCII program and submission procedures. Information will be protected from unauthorized disclosure when, among other things:

1. Such information is voluntarily submitted, directly or indirectly, to the PCII Program Manager or the PCII Program Manager's designee;[18]

2. The information is submitted for protected use regarding the security of critical infrastructure or protected systems, analysis, warning, interdependency study, recovery, reconstitution or other appropriate purposes including, without limitation, for the identification, analysis, prevention, preemption, disruption, defense against and/or mitigation of terrorist threats to the homeland;[19]

3. The information is properly labeled; and[20]

4. The submitted information additionally is accompanied by a statement, signed by the submitting person or an authorized person on behalf of an entity identifying the submitting person or entity, containing such contact information as is considered necessary by the PCII Program Manager, and certifying that the information being submitted is not customarily in the public domain.[21]

Furthermore, ''[a]ll submissions seeking PCII status shall be presumed to have been submitted in good faith until validation or a determination not to validate....''[22] And, as such, the information will be protected from public disclosure under FOIA, state and local sunshine laws[23] and in civil litigation.[24]

Equally importantly, the PCII Final Rule streamlines the process for submitting critical infrastructure information and addresses administrative and procedural concerns that frustrated information sharing under the PCII Interim Rule. In particular, DHS emphasized several key points:

1. A submittal validated as protected critical infrastructure information will not lose its protected status except under a narrow set of circumstances;[25]

2. Protected critical infrastructure information will be shared only for the homeland security purposes specified in the statute and not for other collateral regulatory purpose;[26]

3. In order to accelerate the validation process, the Protected Critical Infrastructure Information Program Manager is given flexibility to designate certain types of infrastructure information as presumptively protected;[27]

4. Provides that submissions not validated as protected critical infrastructure information be returned to the submitter or destroyed;[28]

5. Provides for submission of critical infrastructure information through DHS field representatives;[29]

6. Identifies procedures for indirect submissions to DHS through other federal agencies;[30] and

7. Asserts that the PCII Final Rule simplifies the information submission process.[31]

What Should the Private Sector do Now?

With the release of the NIPP and the clarification of the information protection regulations, the private sector has increased responsibility to safeguard its critical infrastructure. Without continuous input from the private sector, DHS will be unable to develop a comprehensive protection plan that correctly allocates finite resources. Indeed, the risk management process underlying the NIPP assumes that everything cannot be protected; therefore, it is imperative that the private sector cooperate with DHS to develop a national plan that accounts for all stakeholders. Among other things, collaboration includes gathering and submitting critical infrastructure information to DHS.

Collaboration also means working with government stakeholders to develop Sector Specific Plans (''SSPs'') to supplement the NIPP. 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).

Among other responsibilities, SSAs ''shall collaborate with all relevant Federal departments and agencies, State and local governments, and the private sector....''[32] Working cooperatively, SSAs and the private sector continue to develop SSPs to provide a more detailed view of each sector's unique characteristics and protection profile. Each sector's SSP has been completed, though not approved. While some SSPs will not be public, at least one — the SSP for the Financial Services Sector — has been released publicly.

The formation of the Critical Infrastructure Partnership Advisory Council (''CIPAC'') is another example of ongoing 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.[33] According to the CIPAC's *Federal Register* Notice, because of the highly-sensitive and often confidential nature of CIPAC subject matter, CIPAC will be exempt from certain public disclosure laws. Many of the meetings will be private but some ''meetings will be open [to the public] as feasibly consistent with security objectives.''[34]

What Does the Future Hold for Critical Infrastructure Protection?

DHS does not possess regulatory authority to enforce security practices or uniform security standards among most of the nation's critical infrastructure sectors, and there is concern that some critical infrastructure owners and operators will not comply with the voluntary processes outlined in the NIPP.[35] If DHS experiences difficulty obtaining private sector support, regulation may be necessary. The recent regulation in the chemical sector is a likely harbinger of what is to come. Indeed, it is conceivable that Congress will begin regulating other high consequence and high vulnerability industries (e.g., rail) in the near future.

On April 9, 2007, DHS published its Interim Final Rule on Chemical Facility Anti-Terrorism Standards (the "Rule"), which establishes risk-based performance standards for the security of high-risk chemical facilities.[36] Other than Appendix A (discussed below) the Rule became effective on June 8, 2007, and makes revisions and other policy changes to the Chemical Facility Anti-Terrorism Standards Proposed Rule (Proposed Rule) published at the end of 2006.[37] The most significant change to the Proposed Rule is the inclusion of a proposed appendix entitled "DHS Chemicals of Interest" ("Appendix A").[38] Appendix A addresses a perceived weakness in the Proposed Rule, as the Proposed Rule did not specifically identify the chemical substances that DHS considered potentially dangerous. At the time of the submission of this article for publication, DHS had not yet released the Final Appendix A.

Chemical facilities that meet the threshold requirements of Appendix A or are otherwise identified by DHS as potentially high-risk, must complete a questionnaire.[39] 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...."[40]

Depending upon the perceived risk, Covered Facilities will be placed in one of four risk tiers with commensurate security obligations. While DHS will provide the specific tier requirements to Covered Facilities in forthcoming guidance documents, Covered Facilities will be required to prepare Security Vulnerability Assessments ("SVAs") and SSPs that must be approved by DHS. In short, SVAs identifies facility security vulnerabilities. The SSP includes 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, SSP or both.

The Rule also contains provisions concerning inspections, audits, recordkeeping and the protection of sensitive information. It also grants DHS enforcement authority, including assessment of fines and, in extreme cases, the issuance of an order for the cessation of operations. The Rule has a section addressing the review and preemption of state and local law and prohibits third party actions.

While Section 550 of the recently passed Department of Homeland Security Appropriations Act of 2007[41] provides the statutory authority for the Rule, members of the 110th Congress have already proposed amending last year's chemical security legislation. For example, Section 1501 of the Conference Report to the 2007 Emergency Supplemental Appropriations Act for 2007 (H.R. 1591) contains a provision amending Section 550 to allow state and local governments to adopt more stringent chemical security regulations. Regardless of whether H.R. 1591 becomes law, it will be important to monitor legislative developments that may impact the Rule as currently drafted. Additionally, Section 550 has a three year sunset provision and will need to be reauthorized either by this Congress or the 111th Congress.

Conclusion

Although DHS does not generally possess regulatory authority to enforce the procedures outlined in the NIPP, it is important for critical infrastructure owners and operators to understand the important role they play in the nation's security. Members of the private sector must assist the federal government. This means sharing pertinent critical infrastructure information and working to develop plans to ensure the nation's critical infrastructures are protected. If the private sector fails to do its part, it is quite possible that prescriptive legislation will mandate compliance.

---

* The authors are thankful to Les Reese, a third-year law student at Georgetown University, for his invaluable assistance in preparing this article.

[1] 42 U.S.C.A. § 5195c(e).

[2] See generally The Report of the President's Commission on Critical Infrastructure Protection, Critical Foundations Protecting America's Infrastructure (1997); see also Presidential Decision Directive/NSC-63 (May 22, 1998) available at http://www.fas.org/irp/offdocs/pdd/pdd-63.htm.

[3] The White House, Homeland Security Presidential Directive/HSPD-7 (December 17, 2003) available at http://www.fas.org/irp/offdocs/nspd/hspd-7.html.

[4] The U.S. Department of Homeland Security, National Infrastructure Protection Plan 1 (2006), available at http://www.dhs.gov/nipp.

[5] Id.

[6] Matthew E. Berger, *DHS, Private Sector Teamwork Required to Implement Infrastructure "Playbook,"* Cong. Q., June 30, 2006, available at http://homeland.cq.com/hs/

display.do?docid=2319613&sourcetype=31&binderName=news-all; also see 2006 WLNR 11605895 (Westlaw).

[7] *Supra* note 4 at 30.

[8] Id.

[9] *Supra* note 1.

[10] *Supra* note 4 at 3.

[11] Id.

[12] *Supra* note 4 at 32-33.

[13] Steven E. Roberts, *Keeping Corporate Secrets*, Nat'l L.J., May 26, 2003, at 26.

[14] Homeland Security Act of 2002, Pub. L. No. 107-296, § 214, 116 Stat. 2125 (2002).

[15] Dep't of Homeland Security, Protected Critical Infrastructure Information Program, available at http://www.asisonline.org/newsroom/pcii.pdf.

[16] Procedures for Handling Critical Infrastructure Information; Interim Rule, 6 C.F.R. § 29 (2004).

[17] Procedures for Handling Critical Infrastructure Information; Final Rule, 6 C.F.R. § 29 (2006).

[18] Id. at § 29.5(a)(1).

[19] Id. at § 29.5(a)(2).

[20] Id. at § 29.5(a)(3).

[21] Id. at § 29.5(a)(4).

[22] Id. at § 29.5(d).

[23] Id. at § 29.8(g).

[24] Id. at § 29.8(i).

[25] Id. at § 29.6(g). For instance, once information is validated only the PCII Program Office may change the status of PCII to non-PCII. Additionally, the submitter must be notified before a final determination of change in status is made.

[26] Id. at § 29.3(b). It can only be used for collateral regulatory purposes with the written consent of the Program Manager *and* the submitter.

[27] Id. at § 29.6(f). Information that is considered as part of a categorical inclusion will be considered validated upon receipt by the Program Office — without further review.

[28] Id. at § 29.6(e)(2)(i)(F).

[29] Id. at § 29.5(a)(1). PCII shall receive protection if it is voluntarily submitted *directly* or *indirectly* to the Program Manager or his or her designee. (Emphasis added.)

[30] Id. at § 29.2(f); Id. at § 29.5(a)(1); Id. at § 29.6(b), (d).

[31] Id. at § 29.6.

[32] *Supra* note 3 at (19)(a).

[33] Critical Infrastructure Partnership Advisory Council, 71 Fed. Reg. 14930 (Mar. 24, 2006).

[34] Id. at 14932.

[35] Berger, *supra* note 6.

[36] Chemical Facility Anti-Terrorism Standards; Final Rule 72 Fed. R. 17688 (April 9, 2007) (to be codified at 6 CFR Part 27).

[37] Chemical Facility Anti-Terrorism Standards; Proposed Rule, 71 Fed. Reg. 78,276 (Dec. 28, 2006). The ANRM is the subject of a previous Alston & Bird advisory available at http://www.alston.com/files/Publication/ca7d4ff0-8642-4910-89e3-025c33b0cc0d/Presentation/PublicationAttachment/d37632a1-4cde-49fe-ae1a-0685795d7c25/Anti-Terrorism%20Standards.pdf.

[38] DHS looked to existing sources of information in compiling Appendix A: (1) chemicals contained on the EPA's RMP list; (2) chemicals from the Chemical Weapons Convention; and (3) Hazardous Materials that the Department of Transportation regulates. *Supra* note 26 at 17696.

[39] 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. Id. at 17731.

[40] Id. at 17730.

[41] Department of Homeland Security Appropriations Act of 2007, Pub. L. No. 109-295, 120 Stat. 1355 (2006).