‘Democracy Dies Behind Closed Doors’

The Homeland Security Act and Corporate Accountability

by Rena Steinzor
Professor, University of Maryland School of Law,

on behalf of the

Center for Progressive Regulation

Washington, D.C.
March 12, 2003

‘Democracy Dies Behind Closed Doors’* The Homeland Security Act and Corporate Accountability

by Rena Steinzor
Professor, University of Maryland School of Law,

on behalf of the

Center for Progressive Regulation

This paper will be published in a forthcoming issue of
The Kansas Journal of Law & Public Policy

Washington, D.C.
March 12, 2003

U.S. Sixth Circuit Court of Appeals Judge Damon Keith, writing in Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002).

The Center for Progressive Regulation

Founded in 2002, the Center for Progressive Regulation is a nonprofit research and educational organization of university-affiliated academics with expertise in the legal, economic, and scientific issues related to regulation of health, safety, and the environment. CPR supports regulatory action to protect health, safety, and the environment, and rejects the conservative view that government's only function is to increase the economic efficiency of private markets. Through research and commentary, CPR seeks to inform policy debates, critique anti-regulatory research, enhance public understanding of the issues, and open the regulatory process to public scrutiny.

Center For Progressive Regulation
P.O. Box 76239
Washington, DC 20013-1293
www.progressiveregulation.org

Media inquiries to:
CPR Media Office
Matthew Freeman
301-762-8980
CPRMedia@earthlink.net

To contact Professor Steinzor:
(410) 706-0564
rstein@law.umaryland.edu

TABLE OF CONTENTS

Overview

The Homeland Security Act (HSA), enacted into law during an unusual, lame-duck session of the 107th Congress, accomplished the most significant reorganization of the federal government in several decades. At nearly 500 pages, the legislation contained dozens of new provisions, addressing everything from the transfer of existing agencies to the new Department of Homeland Security (HSD) to the creation of several "directorates" to enhance domestic security.[1] A handful of opponents argued that Congress should not rush to judgment on a bill that was so lengthy and contained so many profound changes.[2] Confronted by painful memories of September 11, 2001, intense pressure from President Bush, and the public's anxiety about terrorism, a large majority persevered.

This telescoped and highly politicized process resulted in the enactment of dramatic changes in the law that could have important, yet unintended, consequences. Among the most serious is the "Critical Infrastructure Information Act of 2002" (CIIA). Barely mentioned during the truncated congressional debate on the Bush Administration's version of the legislation, the CIIA offers corporations the opportunity to win confidentiality and civil liability immunity with respect to "critical infrastructure information" that they submit "voluntarily" to the new Department. Critical infrastructure information (CII) includes virtually any information about physical or cyber infrastructure that could prove useful to terrorists or others intent on causing damage to the facility. Unless they obtain the written consent of the company, ***no one*** may use it in ***any civil*** action arising under federal or state law.

Companies act "voluntarily" so long as HSD has not exercised legal authority requiring them to produce the information. They may designate any submission as CII that could lead to harm to interstate commerce if revealed, so long as the information is not "customarily in the public domain." Government officials who knowingly disclose voluntarily submitted critical infrastructure information face *criminal* liability, with a maximum sentence of one year in prison.

Since "information" is covered, as opposed to specific "records" (the term used throughout the Freedom of Information Act), companies may assert that documents containing the same information are also covered, whether or not they submitted this particular paperwork to the government.[3] This assertion will almost certainly spawn

---

[1] For easy access to the full text of the Homeland Security Act, see http://thomas.loc.gov/ .

[2] See, e.g., Gail Russell Chaddock, *Bush spurs lame-duck session to action*, Christian Science Monitor, Nov. 18, 2002, at 2 ("For heavens sake, we have a right to know what is in this 484-page bill, and as of this moment we do not," Senator Byrd said on the floor of the Senate.).

[3] FOIA defines "record" as "any information that would be an agency record subject to the requirements of this section when maintained by an agency in any format, including an electronic format." 5 U.S.C. § 552(f)(2).

widespread litigation because the submission of a single piece of information could invalidate the use of the same information memorialized in countless other formats.

The CIIA was born in the immediate aftermath of collaboration between the federal, state, and local governments and the computer industry to address the so-called "Y2K" problem: the fear of widespread failure of computer systems when the new millennium arrived. Government and private industry participants freely exchanged information about software problems behind closed doors, without any of it falling into the hands of computer hackers or others with criminal motivations.[4] With Y2K problems solved, cyber companies began to worry about the consequences of terrorist attacks through cyberspace and approached Senators Robert Bennett (R-UT) and Jon Kyl (R-AZ) to introduce legislation authorizing a second round of secret consultations.

At some point in its development, the rolling stone that was the Bennett/Kyl legislation began to gather large amounts of moss. The definition of critical infrastructure information was expanded beyond cyber systems to include physical aspects of important facilities. Immunity from civil liability was added to the mix, presumably so that companies would have no fear that if a cyber or physical system failed before they could fix it, their customers could collect billions of dollars in damages. Amazingly enough, to this day, these changes in the laws governing corporate accountability and open government have received very little attention. Instead, the CIIA is described by the White House as a relatively innocuous change in the Freedom of Information Act (FOIA) necessary to protect the national security in these troubled times.[5]

Because the CIIA represents such a significant departure from existing law, those unfamiliar with its provisions may have difficulty believing descriptions of what it says. Therefore, the full text of the new Act is set forth in Appendix A to this paper and its core provisions are examined in detail below. (See "CIIA under a Microscope," below.) Of course, as is the case with most new federal statutes, the CIIA's language is susceptible to different interpretations. How the Act plays out in practice depends largely on how

---

[4] Vernon Loeb, *Cyber-Security Plans go Begging on Hill; Little Funding for $138 Million Proposal*, Wash. Post, Oct. 16, 2000, at A-25 (explaining that President Clinton was having difficulty persuading Congress to fund a "cyber corps" of computer security experts who would "maintain the momentum" established by the "government's successful response to fixing large-scale Y2K software problems last year.").

[5] The FOIA appears at 5 U.S.C. §§552 et seq. For prime examples of the gross mischaracterization of the CIIA's import, see "Analysis of the Homeland Security Act of 2002: Title II," *available at* http://www.whitehouse.gov/deptofhomeland/analysis/title2.html; "Homeland Security Law Contains New Exemption 3 Statute," *available at* http://www.usdoj.oip/foiapost/2003foispost4.htm . Even the press has been misled. See, e.g., *Fix This Loophole*, Wash. Post, Feb. 10, 2003, at A20 (urging Congress to repeal the CIIA because of its effect on "public access to information" without mentioning its civil immunity provisions).

federal courts react to the Department of Justice's (DOJ) characterizations of its true meaning.

A narrow reading of the statutory language would apply the CIIA only to a discrete universe of information that would not otherwise be available to the government. This reading of the FOIA is already the law in states covered by the federal Court of Appeals for the D.C. Circuit. In *Critical Mass Energy Project v. Nuclear Regulatory Commission,*[6] the D.C. Circuit Court of Appeals held that when companies turn information over to the government voluntarily – information that the government could not obtain through other legal means – the information is exempt from disclosure under the FOIA. (See "Optimistic View of Implementation," below.)

On the other hand, an expansive reading would transform the CIIA into a radical reversal of common tort liability and open government requirements. Under this scenario, the CIIA would immunize corporations and their employees from malfeasance in routine activities, from discrimination on the basis of race in the workplace, to embezzlement, to violations of environmental laws, to negligence that harms the general public financially or physically. Not incidentally, these interpretations would also immunize corporations that proved negligent in the face of terrorist threats, allowing them to avoid accountability for endangering their fellow citizens. (See "Pessimistic View of Implementation," below.)

The CIIA was strongly supported not just by corporations that do business in cyber-space, but also by representatives of the traditional manufacturing sector, such as the Edison Electric Institute (EEI), a trade association for large, privately owned electric utilities. EEI's advocacy was so pronounced that, during a fall 2001 visit to the office of Senator Robert Bennett (R-UT), a key co-sponsor of the legislation, I was startled to discover that an EEI lobbyist named Larry Brown had been invited to the meeting to explain how the prospective law was intended to operate. Although Mr. Brown assured me that my concerns about the legislation's overly broad language were "paranoid," it rapidly became clear that none of the bill's industry supporters had any interest in making revisions to address such concerns. (See "Legislative History vs. Lobbyists' Intent," below.)

In May 2002, the Senate Committee on Governmental Affairs held a hearing on these issues where my colleague, David Sobel, senior counsel for the Electronic Privacy Information Center, and I were offered an opportunity to present our concerns more formally.[7] After the hearing, staff for Senators Bennett, Leahy, and Levin negotiated bi-partisan, compromise legislation that eliminated civil immunity and clarified the bill's

---

[6] 975 F.2d 871 (D.C. Cir. 1992).

[7] U.S. Senate, Comm. on Governmental Affairs, hearing on "Securing Our Infrastructure: Private/Public Information Sharing," May 8, 2002 [hereinafter *Senate Hearing on CII*].

narrow scope.[8] Unfortunately, this language was replaced by the original, more extreme text when the House-passed Homeland Security Act legislation became the vehicle for the final vote in Congress.

Unwilling to leave the resolution of these crucial issues up to decades of costly litigation with uncertain and inconsistent results, Senators Patrick Leahy (D-VT) and Carl Levin (D-MI) have pledged to push legislation that will make it absolutely clear that the CIIA was intended as a narrow exemption from FOIA, repealing its civil liability immunity protections. The legislation will be modeled on the compromise negotiated with Senator Bennett. (See "Leahy/Levin Fix," below.)

The remainder of this paper considers the wording of the CIIA, suggesting the contours of narrow and expansive interpretations of the new law and presenting case studies to illustrate the implications of an expansive interpretation. It then examines the context in which the CIIA was passed, including the Bush Administration's secrecy policies, industry's long-standing campaigns to pass tort reform and self-audit privilege legislation at both the federal and state levels. The paper analyzes the arguments of the Act's proponents, especially the questionable assertion that secrecy and civil immunity will enhance national security. It concludes with a discussion of the alternative legislation sponsored by Senators Leahy and Levin.

CIIA under the Microscope

The basic structure of the CIIA is relatively simple. It says that:

When corporations submit

> "critical infrastructure information"
>
> "voluntarily"
>
> to the Department of Homeland Security,

The information

> shall never be disclosed by the government;
>
> cannot be used by the government for "any other purpose;" and
>
> cannot be used to hold companies liable for civil damages or penalties under federal, state, or local law.

---

[8] For the text of that amendment, see http://www.senate.gove/~gov_affairs/073002s2452index.htm

Unauthorized disclosure by a government official triggers criminal penalties.

Conflicting federal, state, and local laws are preempted.

The Act contains a savings clause providing that anyone can use "independently obtained" CII in a manner authorized by other laws.

Important procedural provisions include:

- Submitters must consent in writing to release of the information.

- CII may be used in criminal investigations and prosecutions, may be disclosed to Congress, and may be used to fulfill the "purposes" of the CIIA.

- The Federal Advisory Committee Act (FACA) does not apply to deliberations involving CII.

- Unlike the treatment of "confidential business information" under the FOIA and related executive order, there are no provisions authorizing the government to require companies to show that their submissions qualify for treatment as CII. This provision is very significant because, as a practical matter, HSD may not have the resources to conduct its own independent inquiries, making the corporate claim the beginning and the end of the matter.

Definitions

As in many federal statutes, much of the action in the CIIA takes place in the law's definitions.

Critical Infrastructure Information:

The definition of "critical infrastructure" is not defined, but HSD and the courts will likely borrow the definition of the term from the Patriot Act, section 1016(e):

> 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.

Obviously, this definition focuses on infrastructure that, if attacked by terrorists, could have a debilitating impact on the economy. It suggests that only the most vital infrastructure is covered by the CIIA. After all, even the most vicious attack, one that demolished a facility, presumably would not have a debilitating effect on the ***national*** economy. Either the Executive Branch (HSD or DOJ), or the federal courts, have the task of establishing criteria for sorting "critical" from "non-critical" facilities.

Complicating the interpretation of this aspect of the CIIA's language, however, is considerably broader language used to define the term "critical infrastructure information" (CII). Under this language, if information is not "customarily in the public domain," it qualifies for the protections afforded by the Act, if it "relates to":

- "actual, potential, or ***threatened*** interference" with critical infrastructure by either "physical or computer-based attack or similar conduct" that "violates federal, state, or local law," "harms interstate commerce," ***or*** "threatens public health or safety;" ***or***

- the "***ability***" of critical infrastructure to "***resist***" such interference, including "security testing, risk evaluation thereto, risk management planning, or risk audit;" ***or***

- any "***planned or past operational problem*** or solution regarding critical infrastructure" including "repair, recovery, reconstruction, insurance, or continuity;" ***or***

- the "security of protected systems," which include any "service, physical or computer-based system" that "***directly or indirectly affects the viability***" of a critical infrastructure facility.

While the first two criteria bear at least some relationship to terrorist threats, the third and fourth criteria are sufficiently broad to suggest that more than national security is at stake. Under a literal reading of the third criterion, for example, decisions by companies in the heavy manufacturing sector to repair or replace pollution-generating units could be covered by the law. Since such decisions often trigger additional legal obligations under such laws as the federal Clean Air Act, the third criterion could end up as a leading source of the unintended consequences of the Act. (See "Pessimistic View of Implementation," below.) The fourth criterion – any "system" that directly or indirectly affects the viability of a critical infrastructure facility – could mean the cafeteria, health benefits office, vehicle maintenance shop, or any one of countless other service centers that support in some minor way the operation of any physical plant. If interpreted broadly, this language would expand the scope of the CIIA to virtually any aspect of a company's operations that it wished to describe to HSD in order to receive the protections afforded by the Act.

In sum, if the submitter does not make information available to the public as a matter of custom, and the information concerns a flaw or malfunction that may affect industrial and other business facilities in some economically harmful way, the information falls within the ambit of the Act.

Voluntarily Submitted:

The CIIA's other crucial term of art is "voluntary," used to modify "submittals" of covered critical infrastructure information. This definition is more straightforward

than the convoluted definition of the information itself, and means a "submittal" made "in the absence of [HSD's] exercise of legal authority to compel access to or submission of such information." [9]

The only categories of information specifically excluded from the definition are:

1. information filed with the Securities and Exchange Commission (SEC) or disclosures made when offering securities for sale; and

2. information submitted or relied upon as a basis for making licensing or permitting decisions, or during regulatory proceedings.

The specific exemption for statements filed with the SEC is odd because many, if not most, such statements are "customarily within the public domain" and outside the scope of the CIIA in any event. This targeted exemption has the effect of emphasizing the possibility that the law could be interpreted to cover information filed or retained pursuant to other legal mandates, requirements, or prohibitions. On the other hand, the second exclusion would apply to a broad range of material necessary to operate everything from a television station to a large, pollution-generating industrial facility, and could become a saving grace for the CIIA.

Use of CII by Agencies and in Civil Court Actions

The most egregious aspects of the CIIA are the "protections" it confers on those who voluntarily share covered information with HSD. It is inevitable that corporations concerned not just about security but also about enforcement actions and other forms of civil liability will work hard at the administrative level and in the courts to expand the scope and effect of this section. If HSD officials and the courts listen to these arguments, and overlook or narrowly interpret the Act's savings clause (see "Independently Obtained Information," below), the CIIA will become the powerful tool feared by its critics and ostensibly disclaimed by its proponents. Two categories of protections are the most important: the first bars the use of CII in civil actions and the second bars its use for "any other purpose" by the government.

Civil Actions:

The CIIA blocks the "direct use" of protected information by any party (including all three levels of government and any third party) in any "civil action arising under Federal or State law" so long as the submittal was made in "good faith." Neither term is defined in the law.

---

[9] The provision states that the submission must be made in the absence of the exercise of legal authority by a "covered federal agency," and this term is in turn defined as the Department of Homeland Security. Homeland Security Act of 2002, P.L. 107-296, sec. 212(2), 116 Stat. 2135, 2151 (2002).

It is likely that when the time comes for the federal courts to divine the meaning of "direct use," litigants will direct their attention to interpretations of similar terms in a criminal context because DOJ attorneys repeatedly mentioned such cases when they discussed the draft legislation with congressional staff.[10] Under the Supreme Court decision in *Kastigar v. United States*[11] and its progeny, prosecutors are barred from using information that is directly linked to the testimony of a witness granted "use immunity," and must instead show that they had independent sources for the material. While far from a simple undertaking, *Kastigar* inquiries focus on whether witnesses, or, in the context of the CIIA, submitters, had a reasonable expectation that the information they provided would not be used against them either directly or indirectly as a way of finding out other, equally damaging data. Information obtained from unrelated sources remains available to prosecutors or plaintiffs in civil actions.

A second case that should provide guidance to the courts in interpreting this provision is *Pierce County v. Guillen*.[12] The case involved safety reports required as a condition of receiving federal highway money. The governing statute states that such reports "shall not be subject to discovery or admitted into evidence in a Federal or State court proceeding or considered for other purposes in any action for damages arising from any occurrence at a location mentioned or addressed in such [reports]."[13] Predictably, tort litigation arose and the Supreme Court decided to rule on the meaning of this prohibition. The Court began by emphasizing the rule that "statutes establishing evidentiary privileges must be construed narrowly because privileges impede the search for truth."[14] The Court then held that information compiled initially for the purpose of complying with the federal reporting law was subject to the exclusion, but information initially compiled for other purposes (e.g., a police accident investigation) was not covered by the exclusion. Under this reasoning, only information prepared initially for the purpose of submitting CII to the government would be entitled to confidentiality and civil liability immunity.

Other Purposes:

Although the bar on use of CII in civil actions deprives federal, state, and local officials of a good deal of their enforcement authority, the CIIA does not stop there. Rather, it gilds the lily of confidentiality by prohibiting federal government disclosure or use of such information, without the consent of the submitter, for "purposes other than the purposes of this subtitle." The only exceptions are:

- use of the information in the investigation or prosecution of a criminal act; or

---

[10] I base this statement on my own conversations with congressional staff at the time.

[11] Kastigar v. U.S., 408 U.S. 931 (1972) (holding that prosecution has burden of proving that the evidence proposed to be used is derived from a legitimate source independent of compelled testimony).

[12] Pierce County v. Guillen, 123 S. Ct. 720 (2003).

[13] 23 U.S.C. §409.

[14] 123 S. Ct. 720, 730 (citations omitted).

- disclosure of the information to congressional committees or to the General Accounting Office. (It is worth noting that the Act's failure to allow disclosure to individual members may end up frustrating their efforts to solve constituent problems and exercise oversight over agencies and departments.)

Of course, if this provision is to have much impact as a practical matter, HSD must play a proactive role in policing how other agencies and departments handle CII. The Act provides that to receive protection, CII must be submitted to HSD and marked as confidential. If another unit in the vast federal bureaucracy obtains similar information, how will its employees know that they are prohibited from using or disclosing it? The mind boggles at the expensive, time-consuming, enervating coordination that will be necessary to implement these protections as they appear to be written. Perhaps those practical considerations will encourage a more sensible interpretation of the Act's savings clause.

Independently Obtained Information

The CIIA contains an all-important savings clause designed to preserve the ability of all three levels of government and third parties to obtain "independently obtained information" under "applicable law." In an exercise of ambiguous drafting of the type that exasperates federal judges, such authority is preserved only to the extent that those entities seek to obtain the information "in a manner not covered by" the CIIA's core provisions. As discussed further below, this language could be read to allow access and use so long as the requester discovers the availability of the information through independent means. Or it could be read to mean that once information is labeled CII, no one can obtain it again in any format. (See "Optimistic View of Implementation" and "Pessimistic View of Implementation," below.)

Criminal Penalties

Federal employees who knowingly disclose protected CII are liable for fines and imprisonment up to one year. Such penalties are nothing new; federal law already applies similar penalties to other unauthorized disclosures, although the federal government has never brought such a prosecution.[15] Nevertheless, the message sent by the inclusion of criminal penalties, especially in the context of other Bush Administration policies strongly favoring secrecy, is that bureaucrats act at their peril if they disclose information in controversial cases. (See "Secrecy and the Bush Administration," below.)

[15] 18 U.S.C. §1905 (imposing penalties on federal employees who disclose trade secrets).

Exemptions from the Federal Advisory Committee Act and Ex Parte Rules

The CIIA states that any communication of CII is not covered by the requirements of the Federal Advisory Committee Act (FACA).[16] FACA requires that whenever a federal agency or department convenes a group of outside, private sector advisors, it must publish notice of that fact; announce all meetings of the group in advance; make those meetings open to the public; and ensure that the group itself reflects a balance of different viewpoints. The provisions ensure that the government does not engage in secret consultations with groups biased in one direction or another. The elimination of this open government protection is consistent with the policies of the Bush Administration in other arenas. (See "Vice President Cheney's Energy Taskforce, below.)

In a further effort to circumvent the normal due process afforded to participants in the administrative process, the CIIA also allows CII to be communicated to any decision-maker without regard to traditional "ex parte" rules. Those rules require that every communication be "on the record," or memorialized in writing, so that everyone can see what kinds of pressure were brought to bear on regulatory officials. Dispensing with such rules is directly analogous to the unthinkable prospect that judges could be lobbied in secret by one party or another, and that the other side would never know such contacts took place.

Optimistic View of Implementation

During confirmation hearings for Governor Thomas Ridge, appointed by President Bush to head the new Department of Homeland Security (HSD), Sen. Carl Levin engaged the nominee in a discussion of the CIIA, motivating the new Secretary to make the following pledge:

> It certainly wasn't the intent, I'm sure, of those who advocated the Freedom of Information Act exemption to give wrongdoers protection or to protect illegal activity. And I'll certainly work with you to clarify that language.[17]

Taking Ridge at his word, what is an optimistic scenario for implementation of the Act's broad language?

Three scenarios form the basis for an optimistic view of how the CIIA will be implemented. The first is that federal authorities (HSD and DOJ) and the courts will read the operative language narrowly, circumscribing the reach and therefore the implications of the law. The second is that federal authorities and the courts will view the Act

---

[16] 5 U.S.C. App. 2.

[17] Senate Governmental Affairs Committee Hearing on the Nomination of Tom Ridge to Be Director of Homeland Security, 108th Cong. (Jan. 17, 2003) (statement of Tom Ridge), *available at* 2003 WL 133596; *see* 149 Cong. Rec. S1463-01 (daily ed. Jan. 23, 2003) (statement of Sen. Jeffords).

primarily as a codification of the *Critical Mass* decision. The third is that industry owners and operators of critical infrastructure will not invoke its protections very often.

Narrow Reading

A strict construction of the CIIA would limit its reach to CII that pertains to a small subset of critical physical and cyber infrastructure, the destruction of which would have catastrophic effects on the security and the stability of the economy at the national level. CII would encompass factual material or expert assessments of that material that could play a role in actually assisting terrorists intent on launching such attacks. Further, information would only qualify for protection if it had never before been in the public domain, except by accident. If the submitter had ever disclosed it to outsiders in any other context, the information would not constitute CII.

A second key component in the strict construction of the statute is giving full effect to the savings clause excluding from coverage any information that was "independently obtained." If the material was compiled pursuant to a federal, state, or local legal requirement, mandate, or prohibition, even if it had never been made public, it would not constitute CII, whether or not HSD had ever gone so far as to subpoena it. Data deemed to be legitimate CII could nevertheless be released, or used in a civil action in court, if the party possessing the information had obtained it through sources and methods outside the HSD unit officially assigned to process CII. Conversely, federal, state, and local government agencies and departments would retain their extensive legal authority to require the generation, production, and submittal of any information that is relevant to their missions.

Finally, to deter bogus confidentiality claims and to conserve HSD resources for the fight against terrorism, HSD would issue a rule requiring submitters of CII to produce evidence justifying their confidentiality claims as soon as a request for the information was received.

Codification of Critical Mass

DOJ's Office of Information and Privacy recently posted a statement on the FOIA portion of its website describing the CIIA as providing protection from disclosure under section 552(b)(3) of the FOIA.[18] The statement never mentions the civil immunity provisions of the CIIA. DOJ's focus on the FOIA provision is consistent with the view that the CIIA was never intended as anything more than a codification of an important court opinion expanding exemption 4 of the FOIA, *Critical Mass Energy Project v. Nuclear Regulatory Commission* (*Critical Mass)*.[19] Indeed, some elements of the CIIA's language closely track *Critical Mass*, lending substantial credence to this narrow interpretation.

---

[18] http://www.usdoj.gov/oip/foiapost/2003foiapost4.htm

[19] 975 F.2d 871 (D.C. Cir. 1992).

Critical Mass involved access to safety reports prepared by the Institute for Nuclear Power Operations (INPO), a nonprofit corporation formed in the wake of the 1979 Three Mile Island accident with a membership that consists of all operators of nuclear power plants in the United States.[20] The safety reports were sought by the Critical Mass Energy Project, a watchdog public interest group committed to ensuring nuclear plant safety. The Nuclear Regulatory Commission (NRC) sought to withhold the documents under FOIA exemption 4, which authorizes the withholding of "*trade secrets and commercial or financial information* obtained from a person and privileged or confidential."[21] Notably, the FOIA also allows the government to keep information secret "*in the interest of national defense*" so long as such documents are "*properly classified*" by a presidential Executive Order, but this authority was not invoked by the court.[22]

The case was heavily litigated, bouncing up and down from the trial court level to the D.C. Circuit Court of Appeals three times.[23] The D.C. Circuit ultimately heard the case *en banc*, meaning that every judge sitting on the court participated in producing the opinion. Since most federal appellate cases are decided by three-judge panels, cases decided by the full bench after three of its colleagues have ruled are very unusual, and, for the region of the country covered by "circuit" in which the court sits, represent the definitive word on a topic unless the Supreme Court considers the case.

A divided court (seven judges were in the majority and four in the minority) held that:

> [FOIA] Exemption 4 protects any financial or commercial information provided to the Government on a *voluntary* basis if it is of a kind that the provider would not *customarily release* to the public.[24]

It is clear from the court's opinion that the crucial interest addressed by this categorical rule was that the government must continue to have access to information provided voluntarily, and that this interest was more important than public access to the information under the FOIA. The majority stated in several places, however, that if submitters like the nuclear power plant operators in *Critical Mass* were *otherwise required by law* to submit the information, the government would *continue to have access* to it, whether or not the government had actually gotten around to exercising such authority. Therefore, the court announced somewhat impatiently, watchdog groups like CMEP need have no fear that bureaucrats would "conspire to keep information from the

---

[20] 975 F.2d at 874.
[21] 5 U.S.C. §552(b)(4) (emphasis added).
[22] 5 U.S.C. §552(b)(1) (emphasis added).
[23] See *Critical Mass Energy Project v. Nuclear Regulatory Comm'n* , 931 F.2d 939 (D.C. Cir. 1991); *Critical Mass Energy Project v. Nuclear Regulatory Comm'n*, 830 F.2d 278 (D.C. Cir. 1987); and *Critical Mass Energy Project v. Nuclear Regulatory Comm'n*, 644 F. Supp. 344 (D.D.C. 1986).
[24] 975 F.2d 880.

public by agreeing to the *voluntary submission* of information that the agency has the *power to compel*."[25]

Critical Mass was a bitter loss for consumer and public interest groups because it was viewed as major surgery cutting back disclosure under the FOIA. Indeed, this reality – that disclosure advocates had already lost a significant amount of access – as well as senators' willingness to accept additional FOIA exemptions in a post-September 11 environment, arguably made enactment of the CIIA possible, at least from the perspective of moderates like Senator Bennett. If DOJ and the courts limit the reach of the CIIA to truly voluntary submissions, and exclude all information covered by other legal mandates, requirements, or prohibitions, the new law is far more likely to serve an appropriate purpose.

Industry Reluctance to Submit

A final optimistic scenario for implementation of the CIIA is that private owners and operators of critical infrastructure will not take advantage of its provisions, preferring to solve their own problems rather than seek government assistance. The calculus for any company considering whether to submit information pursuant to the CIIA must begin with the immediate advantages of giving the government access to the information. If the government had experts who could provide valuable advice to companies with vulnerable cyber or physical systems, these incentives would be obvious. They would be offset, of course, by the fear that the government would interfere with the company's internal efforts to address the problem, or that the information would leak.

In hearings on the Senate version of the CIIA,[26] no witness was able to make a convincing case that the government had useful expertise or that consulting with government officials would prove valuable to companies in such plights. In fact, Allan Paller, a leading expert on cyber security, testified:

> Companies are just as reluctant after the attack as they are during the attack, to take the chance that information about their security breach would be made public. They act as if experiencing a security breach is similar to contracting a social disease.[27]

The possibility that information may leak increases as the information becomes more sensational and the vulnerability more threatening. While those possibilities are not necessarily related to whether the government could help address the vulnerability or must know that it exists, they are likely to deter some companies from submitting information to HSD.

---

[25] 975 F.2d 880.

[26] *See Senate Hearing on CII*, *supra*, note 6.

[27] Id. (statement of Alan Paller, Dir. of Research, the SANS Institute, *available at* http://govt-aff.senate.gov/050802paller.pdf).

Ironically, the one obvious situation where it would serve a company's interest to take advantage of CIIA protections is when the information is about to leak anyway and civil liability is a major threat to the company's profitability. Enough such cases are likely to arise that the courts will end up ruling on issues of statutory intent. If the question of the CIIA's true intent ends up in litigation before a judge in the context of a suit for civil damages, including a government enforcement action for civil penalties, two questions are likely to determine the outcome of the case:

1. whether the information, once submitted to the government, is forever off limits even if it is contained in a different document obtained by the plaintiff; and

2. whether the information was "independently obtained" by the plaintiff.

Pessimistic View of Implementation

The pessimistic view of CIIA implementation depends on how seriously the federal government and the courts take the submitters' arguments that national security demands an unequivocal, far-reaching extension of the Act's secrecy provisions. Unfortunately, government officials weighing CII claims are unlikely to have much evidence regarding their validity, making it more likely that they will accept bogus claims.

Government Processing of CII

The closest analogy to the new category of CII in existing law is the protection of trade secrets under FOIA Exemption 4; this, after all, was the provision under which *Critical Mass* was litigated. But there is one crucial difference in the process that governs requests for such information and the process that will ostensibly apply to CII: who bears the burden of demonstrating whether the information is in fact entitled to protection.

Under Executive Order 12600, those who submit information stamped "confidential business information" (CBI) are asked to demonstrate why the information must be withheld by the government prior to its release.[28] If the requester of the information is persistent, these justifications are eventually reviewed by government attorneys who specialize in the application of the FOIA, serving as a deterrent against extravagant, groundless confidentiality claims.

---

[28] Executive Order 12600 of June 23 1987, *Predisclosure Notification Procedures for Confidential Commercial Information*, 52 Fed. Reg. 23781 (June 25, 1987), *available at* http://www.cftc.gov/foia/foieo12600.htm.

In contrast, the CIIA was styled as free-standing law, not as an expansion of Exemption 4, and it will almost certainly be viewed as a new "Exemption 3" exception.[29] Exemption 3 protects from disclosure any information that is "specifically exempted by [a] statute" other than the FOIA, as long as the statute "establishes particular criteria for withholding or refers to particular types of matters to be withheld." Consequently, unless and until the President issues a new Executive Order requiring submitters to bear the burden of proving that information is in fact CII, or HSD promulgates regulations to that effect, it is unclear how the government will determine whether a confidentiality claim is justified.

Again, the CIIA potentially applies to an extremely broad scope of information – virtually anything that pertains to the possibility that either critical physical or cyber infrastructure could be damaged. (See "Critical Infrastructure Information," above.) Companies may well argue that they submit CII voluntarily whenever they hand it over without the compulsion of an actual exercise of government authority to obtain it. Voluntarily submitted CII is protected from disclosure unless a company, as a matter of routine custom, makes such information available to the public. To be sure, the government – or anyone else for that matter – may disclose and use CII that was independently obtained. But application of that savings clause could be read to depend on whether the information has already been submitted voluntarily at the time that it is independently obtained. If the savings clause is read to apply only in the event that information was obtained independently *before* it was filed as CII, the universe of information rendered off limits will expand exponentially.

Because the stakes are so high – immunity from civil liability to those winning CII status – issues of interpretation are very likely to end up in the federal courts, where readings of the statute will be heavily influenced by the facts of the case.

Court Interpretations

Submitters who are parties in cases involving CII are likely to argue that if the courts allow other parties to use sensitive CII in subsequent enforcement actions or tort cases, the incentives to submit information voluntarily are undercut, if not rendered meaningless. They will ask why Congress would have gone to the lengths of criminalizing improper disclosure if it anticipated that third parties could easily use information to harm not only the originating company but the economy as a whole. As evidence of the legislative intent to provide the strong incentive of permanent civil immunity, submitters will note that the CIIA has no time limits on the confidentiality of information, such as a provision sunsetting protections after a vulnerability of critical infrastructure has been resolved.

Given the level of the nation's anxiety about terrorism, courts may be sorely tempted to read the Act expansively in cases involving truly sensitive information, especially where the corporation sharing the information with the government has not yet

[29] 5 U.S.C. §552(b)(3).

had an opportunity to solve the problem and prevent a terrorist attack. Yet because the statute's protections are not limited to such situations, expansive interpretations could have profound unanticipated consequences. Consider the following examples.

Case Studies: From Air Safety to Enron

Air Safety

A company that does background checks for the federal employees who work as security guards at the nation's airports falls behind in its work. Under pressure to make its quota and finish enough background checks to clear candidates in a timely fashion, the company begins to cut corners, omitting criminal background checks in jurisdictions that the applicant lived in more than two years previously. The president of the company retires and his successor is hired from a competitor. Upon discovering the practice, the new president voluntarily notifies the HSD, labeling the disclosure, sent in an e-mail, "critical infrastructure information," or CII. Nevertheless, the practice continues, HSD does nothing to address it, and several people with histories of violent crimes are hired to work at Washington's Ronald Reagan International. When a series of muggings and rapes occurs at the airport, its management asks HSD for any assistance in determining the cause of the outbreak. HSD is aware of the security failure, but says nothing, and the problem continues for several months. Under an expansive reading of the CIIA, none can be held accountable for their actions and omissions.

Software Failure

A large computer company discovers a flaw in the software it sells to connect to the worldwide web. The flaw could cause catastrophic failure of the SCADA computer systems that run power grids throughout the country. The company works for several weeks to correct the problem, to no avail. Eventually, it decides to voluntarily report the flaw to the cyber security office of HSD. At around the same time, its engineers develop changes in the software that correct the problem. The changes cannot be retrofitted on existing systems, but the company includes them in a new operating system it markets the same month. It does not notify its customers of the flaw or the fix.

The flaw then causes the failure of an electric utility serving a mid-sized Midwestern city. The system is down for three days, costing business and residential customers millions of dollars. A government official mentions the cause of the failure to the utility, and it seeks access to the documents filed with HSD. The documents are turned over to the utility by mistake, and the responsible government official is prosecuted criminally. When the utility seeks damages from the software developer, the court grants the developer's motion to dismiss on the basis of its immunity under the CIIA.

Light Truck Brakes

Now consider the same facts with one change: the flaw involves the brake system on a series of light trucks marketed to the military and local police forces. The manufacturer

contemplates a recall, but voluntarily consults with the Department of Homeland Security, which advises against such a step because the trucks are being deployed to the Persian Gulf and a recall would wreak havoc with force readiness and morale. Two dozen service personnel and first responders are killed in accidents caused by the flaw, but their families never discover the cause of their injuries because the information remains buried in the bowels of the bureaucracy.

Pension Fraud

A large pension fund covering employees of a major defense contractor has unscrupulous managers who have used a series of accounting tricks to embezzle millions. After months of warning signs, the contractor's Chief Executive Officer fires the wrongdoers and installs new leadership. On the advice of counsel, it voluntarily reports the results of an internal audit documenting the problems to HSD, which informs the Department of Defense (DOD) of the problem. DOD is unable to take action to terminate the company, however, because doing so would require using CII to justify the decision, an action prohibited under the CIIA.

Workplace Accidents

A company manufactures resins used in spare parts for aircraft. Its internal records indicate that a crucial chemical used in the process is both flammable and can cause acute respiratory distress. It reports this information voluntarily to HSD and redoubles its efforts to enforce a "no smoking" rule within its plants. A freak accident produces a spark that causes an explosion killing 10 workers, and sending 50 to the hospital with acute burns to the lungs and nasal tract. Companies that use the same chemical ask the Occupational Safety and Health Administration (OSHA) to investigate the accident and issue recommendations on how workplace safety can be improved. An OSHA employee, contacted by the original manufacturer and threatened with criminal prosecution for disclosing CII, calls HSD for advice. HSD issues an internal directive ordering government employees not to discuss the situation with outside groups or individuals.

Air Polluters

A large Midwest utility decides that it will change out one coal-burning electric generation unit for another. The new unit, much larger than the first, will produce significantly greater emissions than the unit it replaces. The company could mitigate these increases by installing additional pollution control equipment, but decides it does not wish to shoulder the expense. It begins construction and simultaneously reports these plans to HSD, so that security experts will know about its increased capacity to generate electricity.

An HSD employee, visiting the plant to consult on government purchases of power during emergency situations, notices readings on internal gauges reflecting the dramatically increased emissions. She telephones EPA anonymously to report the situation. EPA issues a Notice of Violation to the company, and threatens to bring an

action for civil penalties, but is instructed to back off by worried HSD officials who want to list the company as an emergency supplier in an upcoming report to Congress. EPA drops its enforcement action, and the HSD employee not only loses her job but is prosecuted criminally. Rumors of these results circulate throughout the industry. In subsequent prosecutions of the utility's competitors, they defend on the basis that EPA has not exercised its prosecutorial discretion fairly.

Port Sabotage

The state of New York suspects that terrorists are smuggling arms into American ports on ships chartered in the Middle East. The state's attorney general seeks access to the shipping manifests kept by American importers in order to spot discrepancies. The American companies refuse, claiming that the information is CII duly submitted to HSD. The New York attorney general does not have enough evidence to assert that he has commenced a criminal investigation of the American companies. Without that evidence, HSD refuses to cooperate with the investigation. A federal court also refuses to order either HSD or the companies to turn over the information, concluding that the attorney general does not have subpoena authority over such materials because the information is CII, as opposed to "independently obtained" information.

Lobbying Improprieties

Lobbyists representing companies that provide goods and services to HSD routinely submit materials describing their companies' products in glowing, even hyperbolic, terms. They arrange repeated trips for government purchasing agents to exotic locations under the guise of briefing them regarding the technical aspects of the products. All of this information is designated as CII by the companies, and is therefore protected from disclosure and oversight by the media or individual members of Congress.

Legislative History vs. Lobbyists' Intent

Although the CIIA's ambiguous language is susceptible to interpretations that would have diametrically different effects, the expansive view of the law's intent is consistent with two ideological crusades supported by the Bush Administration: the first to curb openness in government and the second to reform the nation's tort laws. Viewed from this longer perspective, the CIIA is the outcome of opposition to the FOIA by such powerful officials as Vice President Richard Cheney and Defense Secretary Donald Rumsfeld, who believe that excessive disclosure weakens the presidency. The Act's civil liability immunity provisions can be traced to a two-decade effort by manufacturers of consumer products to roll back statutory and common laws imposing liability for personal injury suffered by their customers. This history demonstrates that the CIIA has little to do with the nation's acute and understandable concerns about terrorism, and has everything to do with fulfillment of an agenda that would not be popular in its own right.

While a comprehensive analysis of the Bush Administration's secrecy policies is well beyond this paper, the most relevant and troubling examples are briefly described below so that readers will grasp the heavily politicized context in which the CIIA became law. For more information about the full range of initiatives, see a related paper entitled *Withhold and Control*, written by Patrice McDermott, Assistant Director, Office of Government Relations, American Library Association.

Secrecy and the Bush Administration

The Ashcroft Memorandum

The FOIA, enacted on July 4, 1966, represented a sea change in federal open government policy. The FOIA shifted the burden placed on people requesting government records to justify why they need the documents onto the government, requiring it to disclose *unless* the information was covered by one of nine specific exemptions.[30] Any decision by an agency to withhold a document was subject to challenge in federal court.[31]

In 1974, in reaction to the Watergate scandals, Congress strengthened the Act, allowing federal courts to order the release of documents over the President's objections. President Gerald Ford vetoed the legislation, at the urging of his chief of staff, Donald Rumsfeld, and deputy chief of staff, Richard Cheney.[32]

DOJ is generally responsible for defending the government in cases challenging decisions to withhold government records under the FOIA. To ensure a consistent approach to such cases, attorneys general often issue memoranda explaining how agencies and departments should interpret the Act. Under the leadership of Attorney General Janet Reno, the Clinton Administration followed a policy of interpreting the Act to facilitate disclosure. Attorney General Reno's memorandum to federal agencies and departments stated that DOJ would only defend an agency's refusal to disclose information when it could be argued that releasing the information would result in "foreseeable harm."[33] Reno could not guarantee that her policy was implemented aggressively by the vast federal bureaucracy, but it set a strong tone favoring disclosure.

When President George W. Bush was elected in 2000, Attorney General John Ashcroft, reversed Reno's approach by 180 degrees, encouraging a presumption of *non-*

---

[30] 5 U.S.C. §552(b).

[31] 5 U.S.C. §552(a)(4)(B).

[32] Shelly Strom, *Freedom of Info Attack Directed from the Top,* The Portland Business Journal, May 10, 2002, available at http://portland.bizjournals.com/portland/stories/2002/05/13/newscolumn2.html (quoting Thomas Blanton, director of the National Security Archive as stating, "President Ford vetoed the Freedom of Information Act as we know it today. And he vetoed it because he and Rumsfeld and Cheney believed that it took away too much presidential power.").

[33] For a copy of Reno's memorandum, see http://www.fas.org/sgp/clinton/reno.html.

disclosure.[34] In October 2001, he issued a memorandum informing federal agencies and departments that DOJ will defend any decision to *withhold* so long as the decision rests on a "sound legal basis," clearly a much easier standard to meet than Reno's demand that agencies demonstrate "foreseeable harm" if records *are* released. The memorandum urges agencies and departments to be creative in their use of FOIA exemptions authorizing refusals to disclose, such as national security considerations, effective law enforcement, and the protection of sensitive business information. The Ashcroft memorandum also changed the tone of government disclosure policies, although it is still too early to document its full effects.

Vice President Cheney's Energy Taskforce

Early in the Bush Administration, Vice President Richard Cheney was placed in charge of national energy policy. He immediately convened a task force that received advice from a wide variety of energy industry representatives.[35] The worst fears of environmentalists and other public interest groups were confirmed when the Bush energy policy was released, demonstrating the overwhelming influence of industry recommendations.

In April 2001, Democratic Members of Congress John Dingell and Henry Waxman asked the General Accounting Office (GAO), Congress' independent investigative arm, to review the deliberations of the Cheney Energy Task Force, including the sources of its recommendations.[36] The White House refused to cooperate with the inquiry. For the first time in its history, GAO went to court to challenge this decision. On December 9, 2002, federal district Judge John Bates, a Bush appointee and former deputy to the Clinton special prosecutor, Kenneth Starr, ruled against GAO.[37]

---

[34] For a copy of the Ashcroft memorandum, see http://www.usdoj.gov/04foia/011012.htm.

[35] For descriptions of the taskforce and how it operated, see Damian Whitworth, *Fresh row over Bush's links to gas companies*, The Times (London), April 5, 2002 (describing the relationship between the Bush Administration's energy policy proposals and the recommendations of the industry representatives on the taskforce); Bennett Roth, *Energy task force releases some files; Conoco Enron lobbied on policy*, Houston Chronicle, March 26, 2002, at A-1 (describing high-level consultations with industry groups and the concerns of environmentalists and other public interest groups about being shut out of the process).

[36] For a description of the Bush Administration's policies on secrecy, including the showdown over the GAO request for records, see Adam Clymer, *Government Openness at Issue as Bush Holds on to Records*, N.Y. Times, Jan. 3, 2003, A-1.

[37] Jim VandeHei, *Officials See Bush Insulated from Hill Probes*, Wash Post, Dec. 15, 2002, at A-18 (describing outcome of lawsuit); E.J. Dionne Jr., *Payback in Judges*, Wash. Post, Jan. 10, 2003, at A-10 (explaining the judge's political connections and the implications of his decision).

Other cases brought by public interest groups sought the same and similar documents not from the Vice President, but from the Department of Energy and other federal agencies.[38] Those cases resulted in the release of thousands of pages regarding the deliberations of the Taskforce.

Presidential Records

In 1978, as another phase of its reaction to the Watergate scandals, Congress passed the Presidential Records Act of 1978, requiring the preservation and disclosure of presidential records by the Archivist of the United States.[39] The first presidential records covered by the Act were those produced by former President Ronald Reagan. In November 2001, in an effort to block release of the Reagan records, President Bush issued an Executive Order that dramatically expanded the scope of prior interpretations of the doctrine of executive privilege as it applies to presidential records.[40] Among other provisions, this Executive Order extends the privilege to Vice President Cheney, a decision without legal precedent. Following litigation by Public Citizen, a nonprofit public interest group, and intense public criticism from academic historians, among others, the Administration ultimately decided to release most, but not all, of the Reagan papers originally identified by the Archivist.[41]

In an effort to forestall other episodes of Executive Branch resistance to the disclosure of presidential records, the 107th Congress' House Committee on Government Reform unanimously approved bipartisan legislation instructing the Executive Branch to implement the Presidential Records Act.[42] In a letter to the Committee, the White House attacked the bill as "unnecessary and inappropriate, and, more importantly, unconstitutional."[43] The bill was introduced by Congressman Stephen Horn and co-sponsored by Congressman Dan Burton, a very conservative Republican from Indiana who proudly advertises on his web site links to like-minded think tanks such as the Competitive Enterprise Institute, the Heritage Foundation, and the Mercatus Center.[44]

Congressman Burton became infuriated with the Bush Administration when the President invoked executive privilege to block a congressional subpoena for information

---

[38] Don Van Natta Jr. & Neela Banerjee, *Top G.O.P. Donors in Energy Industry Met Cheney Panel*, NY Times, March 1, 2002 at A1.

[39] 44 U.S.C. §§2201 et seq.

[40] Executive Order 13233, Further Implementation of the Presidential Records Act, Nov. 1, 2001, *available at* http://www.fas.org/irp/offdocs/eo/eo-13233.htm.

[41] National Archives and Records Administration News Release, *MEDIA ALERT: Additional Reagan Presidential Materials to be Released*, March 12, 2002, available at http://www.fas.org/sgp/news/2002/03/nara031202.html. Approximately 60,000 of 68,000 pages of withheld records were made available to the public.

[42] Adam Clymer, *House Panel Seeks Release of Presidential Papers*, New York Times, Oct. 10, 2002 (*available at* http://www.nytimes.com/2002/10/10/politics/10RECO.html).

[43] Id.

[44] http://www.house./gov/burton/Issues.htm

indicating that the Boston office of the FBI withheld material that would have exonerated Joseph Salvati, a suspected organized crime figure who, as a result, spent 30 years in jail for a crime he did not commit.[45] "You tell the President there's going to be war between the President and this committee," Burton told Carol Thorsen, a DOJ deputy assistant attorney general, right before a hearing before his Committee. "His dad was at a 90 percent approval rating and he lost, and the same thing can happen to him. We've got a dictatorial President and a Justice Department that does not want Congress involved. Your guy's acting like he's a king." [46]

Representative Burton's involvement with issues of open government and corporate accountability demonstrates that these values are not merely the preoccupation of those on the other side of the political spectrum, who are often portrayed as irretrievably alienated from government. In fact, on this issue as on many others, the right and the left ends of the political spectrum end up in the same place on these core principles.

Tort Reform

Tort reform has been a priority for a large group of companies and their trade associations for many years. While it is risky to generalize, the arguments in favor of reform are that the American courts, and especially juries, make extravagant awards to sympathetic plaintiffs in cases where no reasonable manufacturers could anticipate or prevent the harm. Imposing liability in such cases is an unwarranted drag on the economy. The focus of such campaigns has been changes in state law that cap or eliminate categories of damages, especially punitive damages; set standards for determining whether and when a defendant is held liable; and establish administrative alternatives to resolving such cases in court (e.g., arbitration, mediation, or an administrative process for hearing evidence and determining damage awards).

The Bush Administration strongly supports tort reform, vowing to make it a political and policy priority.[47] If one believes that damage awards are often unjustified, and one thinks that the existing system unfairly burdens business, it is not a huge leap to conclude that companies are entitled to the incentive of receiving immunity from civil liability if they are engaged in the patriotic activity of cooperating with the government to enhance national security.

---

[45] A description of the controversy appears at Glen Johnson, *Bush Denies Congress Papers for FBI Probe Panel Denounces Claim of Executive Privilege*, Boston Globe, Dec. 14, 2001, at A-2.

[46] Id.

[47] See Anne E. Kornblut, *Bush Wants Cap on Malpractice Awards Partisan Issue Touches '04 Presidential Race*, Boston Globe, Jan. 16, 2003, at A3 ("Bush is determined to transform soaring jury awards into a potent campaign issue. . .").

The introduction of civil liability immunity distorts the intended incentives in some peculiar, and probably unintended, ways. As discussed earlier, companies may well hesitate to turn CII over to the government for fear it will leak, or that the government will interfere in their efforts to fix the problem. (See "Industry Reluctance to Submit," above.) If they manage to fix the problem, the entire incident will never reach public attention. On the other hand, if they are unable or unwilling to resolve the vulnerability, and if the vulnerability ultimately leads to the failure of systems and equipment, the incentive to submit the incriminating evidence as CII would be very high.

The ostensible goals of the CIIA – to coordinate an effective response through the government's auspices and to make sure that solutions are disseminated to those who need them – are defeated if information is not submitted when vulnerabilities are first discovered. Allowing companies who defy these goals to take advantage of the relief the statute offers is within the letter of the law, but clearly contrary to its purpose.

Self-Audit Privilege

Companies heavily regulated under federal environmental laws have long urged that they should be allowed to initiate voluntary self-audits to determine whether they are in compliance with detailed federal and state mandates. They further request immunity from prosecution if they (1) turn those reports over to the government and (2) initiate efforts to bring themselves back into compliance. About 17 states have enacted some form of self-audit "privilege" law, with some going so far as to excuse criminal violations.[48] That number would undoubtedly be higher if EPA had not strenuously opposed such laws.[49]

EPA opposes audit privilege laws on the grounds that they allow companies and regulators to hide the details and resolution of incidents that should be enforcement matters from public view.[50] Such laws give violators two "bites at the apple," allowing them to commit the violation in the first place, discover it, fix it, and yet escape liability. Especially in cases where compliance costs are high, this result gives an unfair advantage to firms that delay compliance for significant periods, and then pretend to discover their errors late in the day, after their competitors have already paid to operate legally.

"Risk audits" are specifically mentioned in the definition of CII, although this term was probably intended to refer to internal audits of the risk to facilities posed by

---

[48] See Jeffrey C. Fort, Corporate Compliance Series: Designing an Effective Environmental Compliance Program, §2:7 (2002) (reporting that the 17 states are Arkansas, Colorado, Idaho, Illinois, Indiana, Kansas, Kentucky, Michigan, Minnesota, Mississippi, New Hampshire, Oregon, South Dakota, Texas, Utah, Virginia, and Wyoming).

[49] *State Immunity, Privilege Laws Examined for Conflicts Affecting Delegated Programs*, Daily Env't Rep. (BNA), Sept. 18, 1996, at AA-1, 7.

[50] U.S. EPA, Incentives for Self-Policing: Discovery, Disclosure, Correction, and Prevention of Violations, 60 Fed. Reg. 66,706 (Dec. 22, 1995).

terrorist attacks, as opposed to the relatively routine possibility that legal violations may occur. On the other hand, the use of the word audit is sufficiently reminiscent of the other type of document that corporations may well try to invoke the CIIA's protection in states that do not have self-audit laws. Of course, the CIIA does not impose the *quid pro quo* that companies must repair their violations before invoking its protections, although this minimum condition is a core feature of state self-audit laws.

National Security and Secrecy: Safer or Sorrier?

Often, the best way to test the validity of a new idea is to consider the arguments offered by its supporters. Supporters of the CIIA offer two arguments to justify its broad scope and profound consequences.[51]

First, CIIA supporters contend that unless critical infrastructure information is protected from disclosure – *and* the imposition of liability following disclosure – corporations will not share it with the federal government. If the information is not shared, the government will be unable to monitor threats to national security, including attacks on cyber systems and on critical facilities such as power plants, the electric grid, and factories manufacturing essential goods. Without government involvement and a centralized forum for sharing information about these frightening vulnerabilities, private industry will be unable to take effective steps to resolve them.

The second justification appears even more compelling: confidentiality must apply in *any* context, including judicial proceedings, when disclosure would result in the information falling into terrorist hands.

Inevitably, we confront the need to reconsider the openness of our society as terrorism remains a threat. When asked point blank, most members of the public are more than willing to sacrifice the satisfaction of their native curiosity for the sake of enhanced safety.[52] After all, if publicizing information will give terrorists the tools they need to attack us, aren't we better off to keep the information secret? Indeed, long before September 11, 2001, the advent of the Internet provoked such questions. This extraordinarily powerful tool makes the world – and the threats it contains – seem much closer.

Yet, like many other overly simplistic ideas, there is a fatal flaw in the notion that we can simply stuff the Internet genie back into its bottle and also suppress all other methods for communicating information. Even if one pushes aside all the other reasons

---

[51] See, e.g., Sen. Robert Bennett, Closing Remarks, Internet Security Policy Forum II, "Understanding Risk and U.S. Economic Security," U.S. Chamber of Commerce, March 22, 2001, *available at* http://www.senate.gov/~bennett/internet_security_forum.html.

[52] Ken Paulson, *Too Free?*, American Journalism Review (Sept. 2002) at 30 ("roughly half of those surveyed said the American press has been too aggressive in asking government officials for information about the war on terrorism").

why disclosure of information is helpful in an open, democratic society, it is far from clear that suppressing information will make us safer for two reasons.

First, disclosure leads to accountability not just for information but for eliminating the vulnerability the information describes. As a matter of human nature, the absence of this powerful incentive for action will lead to failures to address security problems, ultimately making people less, not more, safe. These outcomes will occur even if the individuals who know about a vulnerability are well-meaning and patriotic because it is so very difficult for good people to combat institutional inertia from a wide variety of sources. The FBI agents who discovered that suspicious men had enrolled in flying schools were unable to persuade their superiors to authorize even a visit to the school to interview its staff.[53] Corporate management worried about the financial bottom line may fail to remedy problems that could prove catastrophic in the event of criminal attack.

Thus, the dilemma is not whether information will fall into terrorist hands, but rather whether suppression of such information, partnered with civil immunity for the consequences of inaction, will lead to even graver outcomes. If we want America to be safer, we cannot afford to suppress information and eliminate liability blindly, hoping that, as large and complex institutions inspired primarily by the profit motive, corporations will voluntarily hold themselves accountable.

The second reason secrecy makes people less safe is that information is necessary for the public to understand how to protect itself. If only a centralized bureaucracy in Washington, D.C. has information about the hazards posed by a potential attack on a given manufacturing facility, how will local responders and the elected officials to whom they are responsible, be able to gauge what steps must be taken to prevent, much less address, those consequences? The predictable and significant risk that information needed by local officials will get lost in the shuffle of the challenges confronting HSD should be unacceptable to anyone sincerely concerned about national security.

As for the assumption that companies would, in fact, respond to the dual incentives provided by non-disclosure and civil immunity and turn over information about their *pending* vulnerabilities voluntarily, no one has offered convincing evidence that this outcome is assured. At a Senate hearing held to examine this and other aspects of the secrecy and security issues, a prominent industry expert named Allan Paller stated unequivocally that companies were unlikely to turn over such information voluntarily in any event.[54] (For more information on this likely outcome, see "Industry Reluctance to Submit," above.)

---

[53] Ron Taylor, *Homeland Security: Facts, coincidences hard to ignore*, Atlanta Journal-Constitution, June 9, 2002, at 4F ("The clues were there, including a seven-year plot to blow up U.S. jetliners. Connecting the clues was the problem. . . . [Congress] is focusing on whether the FBI and the CIA adequately shared intelligence that would have derailed the plot.").

[54] Senate CII hearing, supra note 7 (statement of Allan OPaller). See also, Nick Anderson, *Some Businesses Balk at Giving Secrets for U.S. Terrorism Fight, Security:*

But perhaps the most telling flaw in the law is its prohibition on the use of the information at any time, no matter how far in the future, in a civil action. Presumably, such immunity is only valuable to companies that have done something sufficiently wrong that they face civil liability. If critical infrastructure is operated in full compliance with the law, or if companies have done everything they reasonably can to prevent failure of such systems or facilities, lawsuits may be brought, but they are unlikely to be successful. Viewed from this perspective, the CIIA is more akin to a Trojan horse that, in the name of national security, carries within it far more profound implications.

Leahy/Levin Fix

On March 12, 2003, Senators Leahy and Levin plan to announce that they will push legislation that would prevent the unintended and inappropriate consequences of the CIIA. That legislation would make the following changes to the law:

- The FOIA exemption would cover specific "records" not the information contained in those records, in line with the FOIA's traditional terminology, so that its protections do not encompass any document that includes the information, whether or not it was submitted under the CIIA.

- Covered records must contain information addressing the vulnerability of critical infrastructure, as opposed to any information that could harm interstate commerce.

- "Voluntary" submission is limited to situations where the records at issue cannot be obtained pursuant to the legal authority of regulatory agencies, even where the government has not yet acted to compel it.

- The legislation would not provide civil immunity to submitters of covered information.

- The legislation would not impose criminal liability on government officials who disclose the information.

- The legislation would not preempt state and local laws.

Utilities and high-tech firms are reluctant to turn over information about their operations for fear that it could be compromised, L.A. Times, July 6, 2002, at A-1 ("[R]epresentatives of banking, information technology, utilities and other industries in recent months have declined to share crucial details of how their systems work and where they might be compromised.").

Conclusion

By portraying permanent confidentiality and civil immunity as necessary to enhance national security, the CIIA's proponents sidestepped, at least for the moment, the serious questions that have been raised about whether such proposals are in the public interest. In the aftermath of a major law passed in a panic, with too little consideration of the fine print, Congress should reconsider these conclusions or we will experience years of contentious, draining litigation asking the courts to determine whether Congress really intended such a drastic departure from open government, tort, and enforcement law.

Other changes in federal law enacted soon after September 11 are just now making their way through the federal courts. Considering another such measure, the exclusion of the press from deportation hearings of suspected terrorists, Judge Damon Keith, writing for the U.S. Sixth Circuit Court of Appeals, warned:

> No one will ever forget the egregious, deplorable, and despicable terrorist attacks of September 11, 2001. These were cowardly acts. In response, our government launched an extensive investigation into the attacks... As part of this effort, immigration laws are prosecuted with increased vigor...
>
> Today, the Executive Branch seeks to [place these] actions beyond public scrutiny.... Democracies die behind closed doors. The First Amendment, through a free press, protects the people's right to know that their government acts fairly, lawfully, and accurately . . . When government begins closing doors, it selectively controls information rightfully belonging to the people.[55]

Consider this stirring admonition as it could be applied to the secrecy and civil immunity provisions of the CIIA:

No one can question that recent attacks on America, from assaults on the military and our embassies abroad to the slaughter of thousands on September 11, 2001, have changed forever the nation's willingness to provide opportunities for terrorists to wreak havoc on our democratic way of life. Extraordinary times require extraordinary efforts. In the wake of those attacks, the federal government is determined to ensure that the freedom of our society is not used to sabotage it.

Yet as we fight the terrorist threat, we must ensure we do not play into the hands of those who would destroy us. America is the greatest democracy the world has ever known in large measure because we embrace free and open markets that enable business and industry to flourish. These free markets rest on two premises. First, we believe that the government should not interfere with commerce unless absolutely necessary. Second, we believe that open disclosure of information to investors, lenders, consumers, workers, and others with a stake in a company's future is indispensable to maintaining an economy

---

[55] Detroit Free Press v. Ashcroft, 303 F.3d 681, 683 (6th Cir. 2002).

that will reach its full potential, free of the corruption and graft that have debilitated other economic systems.

Allowing corporations to operate in the shadows will return us to the harsh days of robber barons and *caveat emptor* (let the buyer beware), laying the groundwork for terrorists to gain an advantage without another shot being fired. Rather than making our country safer and more secure, secrecy and immunity will have an increasingly corrosive affect, giving unscrupulous and careless corporations advantages they most certainly do not deserve and sabotaging the efforts of others to do business both honestly and well.

Appendix A: Text of Critical Infrastructure Information Act

H.R.5005 -- Homeland Security Act of 2002 (Enrolled as Agreed to or Passed by Both House and Senate)

Subtitle B--Critical Infrastructure Information

SEC. 211. SHORT TITLE.

This subtitle may be cited as the ‘Critical Infrastructure Information Act of 2002.

SEC. 212. DEFINITIONS.

In this subtitle:

(1) AGENCY- The term ‘agency’ has the meaning given it in section 551 of title 5, United States Code.

(2) COVERED FEDERAL AGENCY- The term `covered Federal agency’ means the Department of Homeland Security.

(3) CRITICAL INFRASTRUCTURE INFORMATION- The term `critical infrastructure information’ means information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

(A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including the misuse of or unauthorized access to all types of communications and data transmission systems) that violates Federal, State, or local law, harms interstate commerce of the United States, or threatens public health or safety;

(B) the ability of any critical infrastructure or protected system to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection, or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or

(C) any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

(4) CRITICAL INFRASTRUCTURE PROTECTION PROGRAM- The term ‘critical infrastructure protection program’ means any component or bureau of a covered Federal agency that has been designated by the President or any agency head to receive critical infrastructure information.

(5) INFORMATION SHARING AND ANALYSIS ORGANIZATION- The term `Information Sharing and Analysis Organization’ means any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of--

(A) gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof;

(B) communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or a incapacitation problem related to critical infrastructure or protected systems; and

(C) voluntarily disseminating critical infrastructure information to its members, State, local, and Federal Governments, or any other entities that may be of assistance in carrying out the purposes specified in subparagraphs (A) and (B).

(6) PROTECTED SYSTEM- The term ‘protected system’ --

(A) means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and

(B) includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

(7) VOLUNTARY-

(A) IN GENERAL- The term ‘voluntary,’ in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency’s exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

(B) EXCLUSIONS- The term ‘voluntary’—

(i) in the case of any action brought under the securities laws as is defined in section 3(a)(47) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(47))—

(I) does not include information or statements contained in any documents or materials filed with the Securities and Exchange Commission, or with Federal banking regulators, pursuant to section 12(i) of the Securities Exchange Act of 1934 (15 U.S.C. 781(I)); and

(II) with respect to the submittal of critical infrastructure information, does not include any disclosure or writing that when made accompanied the solicitation of an offer or a sale of securities; and

(ii) does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

SEC. 213. DESIGNATION OF CRITICAL INFRASTRUCTURE PROTECTION PROGRAM.

A critical infrastructure protection program may be designated as such by one of the following:

(1) The President.

(2) The Secretary of Homeland Security.

SEC. 214. PROTECTION OF VOLUNTARILY SHARED CRITICAL INFRASTRUCTURE INFORMATION.

(a) PROTECTION-

(1) IN GENERAL- Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)--

(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act);

(B) shall not be subject to any agency rules or judicial doctrine regarding ex parte communications with a decision making official;

(C) shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith;

(D) shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States or purposes other than the purposes of this subtitle, except--

(i) in furtherance of an investigation or the prosecution of a criminal act; or

(ii) when disclosure of the information would be--

(I) to either House of Congress, or to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee thereof or subcommittee of any such joint committee; or

(II) to the Comptroller General, or any authorized representative of the Comptroller General, in the course of the performance of the duties of the General Accounting Office.

(E) shall not, if provided to a State or local government or government agency--

(i) be made available pursuant to any State or local law requiring disclosure of information or records;

(ii) otherwise be disclosed or distributed to any party by said State or local government or government agency without the written consent of the person or entity submitting such information; or

(iii) be used other than for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act; and

(F) does not constitute a waiver of any applicable privilege or protection provided under law, such as trade secret protection.

(2) EXPRESS STATEMENT- For purposes of paragraph (1), the term 'express statement', with respect to information or records, means--

(A) in the case of written information or records, a written marking on the information or records substantially similar to the following: `This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002.'; or

(B) in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

(b) LIMITATION- No communication of critical infrastructure information to a covered Federal agency made pursuant to this subtitle shall be considered to be an action subject to the requirements of the Federal Advisory Committee Act (5 U.S.C. App. 2).

(c) INDEPENDENTLY OBTAINED INFORMATION- Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.

(d) TREATMENT OF VOLUNTARY SUBMITTAL OF INFORMATION- The voluntary submittal to the Government of information or records that are protected from disclosure by this subtitle shall not be construed to constitute compliance with any requirement to submit such information to a Federal agency under any other provision of law.

(e) PROCEDURES-

(1) IN GENERAL- The Secretary of the Department of Homeland Security shall, in consultation with appropriate representatives of the National Security Council and the Office of Science and Technology Policy, establish uniform procedures for the receipt, care, and storage by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government. The procedures shall be established not later than 90 days after the date of the enactment of this subtitle.

(2) ELEMENTS- The procedures established under paragraph (1) shall include mechanisms regarding—

(A) the acknowledgement of receipt by Federal agencies of critical infrastructure information that is voluntarily submitted to the Government;

(B) the maintenance of the identification of such information as voluntarily submitted to the Government for purposes of and subject to the provisions of this subtitle;

(C) the care and storage of such information; and

(D) the protection and maintenance of the confidentiality of such information so as to permit the sharing of such information within the Federal Government and with State and local governments, and the issuance of notices and warnings related to the protection of critical infrastructure and protected systems, in such manner as to protect from public disclosure the identity of the submitting person or entity, or information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is otherwise not appropriately in the public domain.

(f) PENALTIES- Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this subtitle coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than 1 year, or both, and shall be removed from office or employment.

(g) AUTHORITY TO ISSUE WARNINGS- The Federal Government may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other governmental entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the federal Government shall take appropriate actions to protect from disclosure

(1) the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning; or

(2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

(h) AUTHORITY TO DELEGATE- The President may delegate authority to a critical infrastructure protection program, designated under section 213, to enter into a voluntary agreement to promote critical infrastructure security, including with any Information Sharing and Analysis Organization, or a plan of action as otherwise defined in section 708 of the Defense Production Act of 1950 (50 U.S.C. App. 2158).

SEC. 215. NO PRIVATE RIGHT OF ACTION.

Nothing in this subtitle may be construed to create a private right of action for enforcement of any provision of this Act.