PROTECTING THE HOMELAND BY EXEMPTION: WHY THE CRITICAL INFRASTRUCTURE INFORMATION ACT OF 2002 WILL DEGRADE THE FREEDOM OF INFORMATION ACT

To protect against "cyberterror," the House version of the Homeland Security Act exempts information related to the nation's critical infrastructure from the Freedom of Information Act[1] disclosure requirements. The proposed exemption unnecessarily threatens public access to vital information about health and safety information; information the Freedom of Information Act was designed to guarantee.

Introduction – The Threat of Cyberterror

One of the hottest perceived threats to America in this new age of terrorism is "cyberterror" – terrorism via our own electronic infrastructure. Reports indicate that al Qaeda operatives are researching methods to electronically disable or destroy our nation's infrastructure systems, such as dams, communications systems, and other structures.[2] In fact, 74% of IT professionals believe an attack on Wall Street or on large banks will almost certainly occur in the next year.[3] What makes this vulnerability difficult to patch is the nature of our nation's infrastructure. Eighty-five to 90% of America's critical infrastructure is privately owned, and information regarding its capabilities and weaknesses is not automatically available to the government.[4]

According to industry computer experts, businesses that operate our nation's critical infrastructure currently hesitate to share information with the government about previous Internet attacks because they fear disclosure to the public under the Freedom of Information Act ("FOIA").[5] Under the FOIA, most agency records must be made available for public review.[6]

---

[1] 5 U.S.C. § 552 (2002).
[2] Jay Lyman, *Worries Mount Over Terrorist Cyber Assault*, NEWSFACTOR NETWORK, June 27, 2002, *available at* http://www.newsfactor.com/perl/story/18426.html.
[3] *Id*.
[4] *Cf.* 148 CONG. REC. H5633-04 (daily ed. July 25, 2002) (statement of Rep. Watts), 2002 WL 1730173, *with* Jay Lyman, *Homeland Defense Focuses On High-Tech Threats*, NEWSFACTOR NETWORK, July 10, 2002, *available at* http://www.newsfactor.com/perl/story/18549.html.
[5] Ted Bridis, *Computer Secrecy Proposals Debated*, AP Online, July 24, 2002, *available at* 2002 WL 24648022.
[6] *Cf.* 5 U.S.C. § 552(a)(1) ("Each agency shall make available to the public information as follows"), *and* § 552(a)(2) ("Each agency…shall make available for public inspection and copying"), *with* § 552(a)(3) ("each agency, upon any request for records… shall make the records promptly available to any person").

Industry experts claim that public knowledge of previous hacker attacks could lead to liability lawsuits against companies that volunteer information.[7]

To alleviate these fears, Congress is considering the Critical Infrastructure Information Act of 2002 ("CIIA").[8] The CIIA is embedded within the House version of the Homeland Security Act of 2002, a politically charged piece of legislation that would lead to the largest reorganization of the federal government since World War II.[9] To improve information sharing, the CIIA would exempt certain information from being disclosed under the Freedom of Information Act.[10] The CIIA would block requests for information that was voluntarily given by private companies to the government about their own network vulnerabilities and previous hacker attacks.

However, an exemption to the FOIA is unnecessary to improve information sharing. There are already private sector protections embedded in the FOIA, though this is not widely known.[11] In addition, the broad language of the proposed exemption may lead to an unintended lack of access to vital information about public health and safety. Furthermore, it is uncertain that this new exemption will do anything to increase public/private collaboration.

The Critical Infrastructure Information Act of 2002

The CIIA, as written in the House version of the Homeland Security Act of 2002, exempts certain information from disclosure under the Freedom of Information Act.[12] To be exempt, the information must be "critical infrastructure information," which is broadly defined as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems."[13] Examples of critical infrastructure information given in the statute include 1) actual, potential, or threatened interference with critical infrastructure, 2) capabilities and assessments of current systems and their resistibility to attacks, and 3) any operational problems or solutions regarding critical infrastructure.[14] A person or entity must give the information voluntarily to the new Department of Homeland Security to be used by the department for some informational purpose regarding the security of critical infrastructure and

---

[7] Ted Bridis, *Computer Secrecy Proposals Debated*, AP ONLINE, July 24, 2002, *available at* 2002 WL 24648022.
[8] H.R. 5005, 107th Cong. §§ 721-725 (2002).
[9] Press Release from the White House to Congress (June 18, 2002), 2002 WL 1315534.
[10] H.R. 5005, 107th Cong. § 724(a)(1).
[11] 5 U.S.C. § 552 (most significantly, the FOIA exempts 1) trade secrets, and 2) confidential commercial or financial information).
[12] H.R. 5005, 107th Cong. § 722(3).
[13] *Id.*
[14] *Id.*

protected systems.[15] Protected systems include both physical and computer-based systems that either directly or indirectly affect a facility of critical infrastructure.[16]

In addition to being exempt from disclosure under the FOIA, information disclosed under the CIIA cannot be used against the submitter in civil litigation (if submitted in good faith),[17] nor be disclosed by any government employee (except in very narrow circumstances, such as a criminal investigation).[18] The CIIA also applies to information provided to state and local governments, nullifying any state laws requiring disclosure.[19]

The Homeland Security Act of 2002, including the CIIA provisions, passed the House of Representatives by a vote of 295-132. As of the date of publication, it is under consideration by the Senate.

Would the CIIA Achieve Anything New?

The most cogent argument against the CIIA is that the private sector exemptions are redundant and unnecessary. The Freedom of Information Act contains several exemptions that protect information given to the government by private entities. Although the FOIA embodies a "general philosophy of full agency disclosure"[20] in order to create a more informed citizenry,[21] that goal is balanced by nine statutorily delineated exemptions[22] designed to preserve the confidentiality of sensitive information.[23] Included in these exemptions are matters of national defense or foreign policy,[24] trade secrets,[25] and commercial or financial information given by a person that is privileged or confidential.[26]

In a letter to members of the House, eighteen private businesses and associations expressed their current hesitations to share sensitive information with the government.[27] They

---

[15] *Id.* at § 724(a)(1).
[16] *Id.* at § 722(6).
[17] *Id.* at § 724(a)(1)(C)
[18] H.R. 5005, *supra* note 12, at § 724(a)(1)(D).
[19] *Id.* at § 724(a)(1)(E).
[20] U.S. Dep't of Def. v. Fed. Labor Relations Auth., 510 U.S. 487, 494 (1994).
[21] Vigil v. Andrus, 667 F.2d 931, 938 (10th Cir. 1982).
[22] Freedom of Information Act, 5 U.S.C. § 552(b)(1)-(b)(9) (2002).
[23] Adm'r, Fed. Aviation Admin. v. Robertson, 422 U.S. 255, 261 (1975).
[24] 5 U.S.C. §552(b)(1).
[25] *Id.* at §552(b)(4).
[26] *Id.*
[27] Letter from eighteen businesses and organizations to members of the United States House of Representatives, (July 5, 2001) (*available at* http://www.itaa.org/infosec/foialetter.pdf) (the letter was written to support the Cyber Security Information Act, H.R. 2435, 107th Cong. (2001). Its provisions are similar to those in the CIIA of 2002.).

stated that the uncertainty in the law, namely the Freedom of Information Act and antitrust exemptions, creates a "chilling effect" on information sharing efforts.[28]

Although the law surrounding the FOIA is generally well settled, on first glance there appears to be credence to these businesses' concerns. The Supreme Court has said, "disclosure, not secrecy, is the dominant objective of the [Freedom of Information] Act."[29] The courts agree that the FOIA is to be broadly construed in favor of disclosure, while the nine exemptions are to be construed narrowly.[30]

Even more damaging to public/private collaboration is the generally one-sided nature of the FOIA. If a FOIA information request is denied by a federal agency, the requestor can seek a decree in a U.S. District Court to enjoin the agency to disclose the information.[31] However, the FOIA is exclusively a disclosure statute and does not afford any private entity a right of action to enjoin an agency from disclosure.[32] In addition, if a part of a record contains information exempted under the FOIA, the record still must be disclosed with the exempted information redacted.[33]

But, there is a very broad exception to this general rule for information that falls under exemption 4 of the FOIA – trade secrets and confidential commercial or financial information. The Trade Secrets Act[34] prohibits agencies from releasing information that falls within exemption 4.[35] To bar release of the information, the submitter can bring a "reverse-FOIA" suit under the Administrative Procedure Act.[36]

The purpose of exemption 4 is "to encourage individuals to provide certain kinds of confidential information to the Government."[37] If information is disclosed to the government voluntarily (and is financial or commercial in nature, and obtained by a person), then it will be exempted if "it is the kind of information that would customarily not be released to the public by

---

[28] *Id.*
[29] Dep't of Interior v. Klamath Water Users Protective Ass'n, 532 U.S. 1, 7 (2001).
[30] Anderson v. Dep't of Health and Human Services, 907 F.2d 936, 941 (10th Cir.1990); Sharyland Water Supply Corp. v. Block, 755 F.2d 397, 398 (5th Cir.1985).
[31] Freedom of Information Act, 5 U.S.C. § 552(b) (2002).
[32] Chrysler Corp. v. Brown, 441 U.S. 281, 316 (1979).
[33] 5 U.S.C. § 552(b).
[34] 18 U.S.C. § 1905 (2002).
[35] McDonnell Douglas Corp. v. Nat'l Aeronautics and Space Admin., 180 F.3d 303, 305 (D.C. Cir. 1999); Hercules, Inc. v. Marsh, 839 F.2d 1027, 1029 (4th Cir. 1988); Pacific Architects & Engineers, Inc. v. U.S. Dep't of State, 906 F.2d 1345, 1347 (9th Cir. 1990).
[36] 5 U.S.C. § 706(2)(A) (2002) (agency actions will only be overturned if found to be arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with the law).
[37] Critical Mass Energy Project v. Nuclear Regulatory Comm'n, 975 F.2d 871, 873 (D.C. Cir. 1992) (quoting Soucie v. David, 448 F.2d 1067, 1078 (D.C. Cir. 1971)).

the person from whom it was obtained."[38] For instance, in *Critical Mass Energy Project v. Nuclear Regulatory Commission*, the D.C. Circuit Court of Appeals held that safety reports voluntarily transmitted to the Nuclear Regulatory Commission ("NRC") on condition of confidentiality should not be released to the public under exemption 4.[39] The court emphasized that releasing the documents would undermine the purpose of the exemption, which is to encourage cooperation between the government and people with useful information.[40] This exemption has precisely the same goal as does the CIIA.

Fears of the private sector are overstated. Reservations about critical business information being disclosed under the FOIA should not prevent disclosure of information about our fundamental infrastructure to the government. Passage of the CIIA is unnecessary for the private sector to begin assisting the administration in its anti-terrorism efforts.

Is the CIIA Loophole Oversized?

In addition, many are concerned that the language of the CIIA is too broad and goes against the very purpose of the FOIA. Four of the nine members of the Select Committee on Homeland Security conveyed their concerns in a minority opinion regarding the potential reach of the CIIA.[41] In the House report on the Homeland Security Act, these four representatives stated that the broad definition of "critical infrastructure" would cover corporations seeking liability protection, and such a result threatens our country's "tradition of open and accountable government.[42] Ten press organizations have sent their own letter to Congress warning that the proposed exemption "is ripe for misuse and abuse."[43]

Opponents of the proposed exemption fear that reduced accountability will actually lead to weaker protection of our critical infrastructure. Especially in the wake of recent corporate scandals and accounting improprieties, some say that the government should be restricting the

---

[38] *McDonnell Douglas Corp.*, 180 F.3d at 304 (citing *Critical Mass*, 975 F.2d at 873); *but see* McDonnell Douglas Corp. v. Nat'l Aeronautics and Space Admin., 895 F. Supp. 316, 318 (D.D.C. 1995) ("Unlike the NRC in *Critical Mass*, NASA does not need to "encourage cooperation" to receive the information at issue. MDA is not doing the government a favor by providing the most basic information in a contract--price.")

[39] 975 F.2d at 873.

[40] *Id.* at 878.

[41] H.R. Rep. No. 107-609, at 1 (2002), 2002 WL 1634718.

[42] *Id.* ("For example, an energy company could hide from the public information about a leak at its nuclear power plant simply by submitting information, unsolicited, to the [Department of Homeland Security].").

[43] Paul McMasters, *A Protection Ripe for Abuse*, THE RECORD, July 28, 2002, *available at* 2002 WL 4666847.

privacy of corporate America rather than enlarging it.[44] Even members of the current administration have misgivings about the proposed exemption. John Malcolm of the Justice Department's Criminal Division says that the loophole would permit a knowingly at fault company to do a "document dump" on the government and free itself from any potential civil prosecution.[45]

The language in the House version of the CIIA exempts "critical infrastructure information" from the disclosure requirements of the FOIA. Included in that term's definition is "any planned or past operational problem…regarding critical infrastructure or protected systems."[46] Representative Schakowsky (D-Ill.), ranking Democrat on the House Government Reform Subcommittee on Governmental Efficiency, has called this language, "a loophole big enough to drive any corporation and its secrets through."[47]

Theoretically, Schakowsky is correct. As currently written, operators of critical infrastructure will be able to submit any information to the government regarding previous attacks in order to become insulated against civil liability related to those attacks. While this language certainly encourages public/private information sharing, it inhibits the public's ability to hold operators of critical infrastructure accountable for their activities through civil action.

Such a result may, in fact, actually decrease private preparedness for future cyberterror attacks. If an operator of critical infrastructure knows it can avoid civil liability for a cyberterror attack by simply submitting information regarding the attack to the Homeland Security Department, it will have less of an economic incentive to invest in preventing future attacks. A decrease in preparedness implies a decrease in security, and illustrates the need for public scrutiny on the preparedness of our critical infrastructure.

Can the Public & Private Sectors Ever Collaborate Voluntarily?

Even if the CIIA in its current form should become law, the biggest roadblock to public/private information sharing still remains: overcoming business interests. The most

---

[44] *See id.* ("Without access to the kind of information that would be exempted in this proposal, there is no accountability for mistakes and misdeeds, no public pressure to address critical infrastructure vulnerabilities, and no informed discourse on policies that impact dramatically on public life.").

[45] Dan Caterinicchia, *Sharing Seen As Critical For Security*, FEDERAL COMPUTER WEEK, May 9, 2002, *available at* http://www.fcw.com/fcw/articles/2002/0506/web-crit-05-09-02.asp.

[46] H.R. 5005, *supra* note 12, at § 722(3)(C) (2002).

[47] Press Release, Representative Jan Schakowsky, *Schakowsky Condemns Bush Administration Support Of Proposal That Would Grant Corporations Immunity And Deny Information To Public,* (July 24, 2002), *available at* http://www.house.gov/apps/list/press/il09_schakowsky/pr07_24_2002foia.html.

pertinent concerns to members of the corporate sector are those of its shareholders. For a company to use valuable time, resources and manpower to organize its own information regarding infrastructure capabilities, weaknesses, and previous hacks for the benevolent mission to improve our national security is antithetical to the very nature of a profit-driven organization. While increased public/private sharing may prevent cyberterror attacks in the long-term, it will not increase profits in the short-term – such investments may be hard to come by with the current economic slowdown. The government may find its efforts here wasted without providing some incentive for disclosure.

A more radical option to consider is to require by law all critical infrastructure information to be disclosed to the new Homeland Security Department. Such information would still receive the protections under the FOIA[48], and the government would receive unfettered access to the information it needs to protect the homeland. Although this would not be a desired market solution, it deserves discussion, especially in light of our perceived infrastructure vulnerability.

Conclusion

With so many issues facing passage of the Homeland Security Act, the Critical Infrastructure Information Act must not be included in its present form. Glaring issues remain with respect to the right of individuals to know what their government is doing and to hold operators of critical infrastructure accountable for their actions. With protections already in place through the Freedom of Information Act, members of the administration and the public need to pressure operators of private infrastructure to willingly contribute as much information to the homeland security effort as is necessary to protect our nation from future cyberterror attacks. Private owners hold the keys to the safety of our critical infrastructure, and therefore must be convinced or compelled to act. However, removing their flaws from the public eye will decrease public scrutiny and reduce private incentives to improve security. Such a result will hinder the overall effectiveness of the Homeland Security Act.

By: Brett Stohs

---

[48] Even if information is required by the government, it may still fall under exemption 4 if disclosure is likely to (1) impair the government's ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained. Pub. Citizen Health Research Group v. Food and Drug Admin., 185 F.3d 898, 903 (D.C. Cir. 1999).