Statement of
David L. Sobel
General Counsel
Electronic Privacy Information Center

Before the
Senate Committee on Governmental Affairs

Hearing on
"Securing Our Infrastructure: Private/Public Information Sharing"

May 8, 2002
Washington, DC

Mr. Chairman and Members of the Committee:

Thank you for providing me with the opportunity to appear before the Committee to address the role that information sharing plays in the protection of our nation's infrastructure. The Electronic Privacy Information Center (EPIC) has a longstanding interest in computer and network security policy, emphasizing full and informed public debate on matters that we all recognize are of critical importance in today's inter-connected world.

While my comments will focus primarily on proposals to create a new Freedom of Information Act (FOIA) exemption for information concerning critical infrastructure protection, I would like to share with the Committee some general observations that I have made as this debate has unfolded over the past few years.

· There appears to be a consensus that the government is not obtaining enough information from the private sector on "cyber security" risks and vulnerabilities that could adversely affect the critical infrastructure. I hasten to add that citizens – the ones who will suffer the direct consequences of infrastructure failures – are also receiving inadequate information on these vulnerabilities.

· There has not yet been a clear vision articulated defining the government's proper role in securing the critical infrastructure. While there has been a great deal of emphasis on finding ways to facilitate the government's receipt of information, it remains unclear just what the government will do with the information it receives. In fact, many in the private sector advocate an approach that would render the government powerless to correct even the most egregious security flaws.

· The private sector's lack of progress on security issues appears to be due to a lack of effective incentives to correct existing problems. Congress should consider appropriate incentives to spur action, but secrecy and immunity, which form the basis for many of the proposals put forward to date, remove two of the most powerful incentives – openness and liability. Indeed, many security experts believe that disclosure and potential liability are essential components of any effort to encourage remedial action.[1]

· Rather than seeking ways to hide information, Congress should consider approaches that would make as much information as possible available to the public, consistent with the legitimate interests of the private sector.

As indicated, I would like to focus my comments on proposals to limit public access to information concerning critical infrastructure protection. EPIC is a strong advocate of open government, and has made frequent use of the FOIA to obtain information from the government about a wide range of policy issues, including (in addition to computer security) consumer privacy, electronic surveillance, encryption controls and Internet content regulation. We firmly believe that public disclosure of this information improves government oversight and accountability. It also helps ensure that the

public is fully informed about the activities of government.

I have personally been involved with FOIA issues for more than twenty years and have handled information requests on behalf of a wide range of requesters. In 1982, I assisted in the preparation of a publication titled *Former Secrets*, which documented 500 instances in which information released under the FOIA served the public interest. I am convinced that an updated version of that publication would today yield thousands of examples of the benefits we all derive from the public access law that has served as a model for other nations around the world.

EPIC and other members of the FOIA requester community have, for the past several years, voiced concerns about various proposals to create a broad new FOIA exemption, such as the one contained in S. 1456, for information relating to security flaws and other vulnerabilities in our critical infrastructures. We collectively believe this exemption approach is fundamentally inconsistent with the basic premise of the FOIA, which, as the Supreme Court has recognized, is "to ensure an informed citizenry, vital to the functioning of a democratic society, needed to check against corruption and to hold the governors accountable to the governed."[2] To accomplish that end, "[d]isclosure, not secrecy, is the dominant objective of the Act."[3]

It is clear that, as we enter a new century and move further into the electronic age, the federal government increasingly will focus on the protection of critical infrastructures. It is equally apparent that government policy in this emerging field will become a matter of increased public interest and debate. EPIC has monitored developments in this area since the creation of the President's Commission on Critical Infrastructure Protection (PCCIP) in July 1997. After the Commission issued its report, EPIC published an analysis of the PCCIP's proposals (*Critical Infrastructure Protection and the Endangerment of Civil Liberties*[4]) which identified a number of Commission recommendations that could threaten privacy, extend the reach of federal law enforcement agencies, limit mechanisms for government accountability and increase the level of information classification and secrecy. While reasonable observers can disagree over the merits of such initiatives, I believe we all agree that critical infrastructure protection raises significant public policy issues that deserve full and informed public discussion.

Increasingly, government activity in this area will be conducted in cooperation with the private sector and, accordingly, will involve extensive sharing of information between the private sector and government. To facilitate the exchange of information, some have advocated enactment of an automatic, wholesale exemption from the FOIA for any "cyber security statements" or other similar information provided by a private party to a federal agency. Given the breadth of the proposed definitions of the categories of information to be exempted, I believe such an exemption would likely hide from the public essential information about critically important – and potentially controversial – government activities undertaken in partnership with the private sector. It could also adversely impact the public's right to know about unsafe practices engaged in by the private operators of nuclear power plants, water systems, chemical plants, oil refineries, and other facilities that can pose risks to public health and safety. In short, critical infrastructure protection is an issue of concern not just for the government and industry, but also for the public – particularly the local communities in which these facilities are located.

If the history of the FOIA is any guide, a new exemption would likely result in years of litigation as the courts are called upon to interpret its scope. The potential for protracted litigation brings me to what I believe is the most critical point for the Committee to consider, which is the need for the proposed critical infrastructure exemption. FOIA caselaw developed over the past quarter-century makes it clear that existing exemptions contained in the Act provide adequate protection against harmful disclosures of the type of information we are discussing. For example, information concerning the software vulnerabilities of classified computer systems used by the government and by defense contractors is already exempt under FOIA Exemption 1. Most significantly, Exemption 4, which protects against disclosures of trade secrets and confidential information, also provides extensive protection from harmful disclosures. Because I believe that Exemption 4 extends to virtually all of the material that properly could be withheld from disclosure, I would like to discuss briefly the caselaw that has developed in that area.

For information to come within the scope of Exemption 4, it must be shown that the information is (A) a trade secret, or

(B) information which is (1) commercial or financial, (2) obtained from a person, and (3) privileged or confidential.[5] The latter category of information (commercial information that is privileged or confidential) is directly relevant to the issue before the Committee. Commercial or financial information is deemed to be confidential "if disclosure of the information is likely to have either of the following effects: (1) to impair the government's ability to obtain the necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained."[6] The new FOIA exemption that has been proposed seeks to ensure that the government is able to obtain critical infrastructure information from the private sector on a voluntary basis, a concern which comes within the purview of Exemption 4's "impairment" prong. The courts have liberally construed "impairment," finding that where information is voluntarily submitted to a government agency, it is exempt from disclosure if the submitter can show that it does not customarily release the information to the public.[7] In essence, the courts defer to the wishes of the private sector submitter and protect the confidentiality of information that the submitter does not itself make public.

In addition to the protections for private sector submitters contained in FOIA Exemption 4 and the relevant caselaw, agency regulations seek to ensure that protected data is not improperly disclosed. Under the provisions of Executive Order 12600 (*Predisclosure Notification Procedures for Confidential Commercial Information*) issued by President Reagan in 1987, each federal agency is required to establish procedures to notify submitters of records "that arguably contain material exempt from release under Exemption 4" when the material is requested under the FOIA and the agency determines that disclosure might be required. The submitter is then provided an opportunity to submit objections to the proposed release. The protections available to private sector submitters do not end there; if the agency determines to release data over the objections of the submitter, the courts will entertain a "reverse FOIA" suit to consider the confidentiality rights of the submitter.[8]

In light of the substantial protections against harmful disclosure provided by FOIA Exemption 4 and the caselaw interpreting it, I believe that any claimed private sector reticence to share important data with the government grows out of, at best, a misperception of current law. The existing protections for confidential private sector information have been cited repeatedly over the past two years by those of us who believe that a new FOIA exemption is unwarranted. In response, exemption proponents have not come forward with any response other than the claim that the FOIA creates a "perceived" barrier to information sharing.[9] They have not provided a single example of voluntarily submitted information that would not fall within the protection of Exemption 4.

Frankly, many in the FOIA requester community believe that Exemption 4, as judicially construed, shields far too much important data from public disclosure. As such, it is troubling to hear some in the private sector argue for an even greater degree of secrecy for information concerning vulnerabilities in the critical infrastructure. As I have noted, shrouding this information in absolute secrecy will remove a powerful incentive for remedial action and might actually exacerbate security problems. A blanket exemption for information revealing the existence of potentially dangerous vulnerabilities will protect the negligent as well as the diligent. It is difficult to see how such an approach advances our common goal of ensuring a robust and secure infrastructure.

In summary, the Freedom of Information Act has worked extremely well over the last 25 years, ensuring public access to important information while protecting against specific harms that could result from certain disclosures. After monitoring the development of critical infrastructure protection policy for the last several years, I have heard no scenario put forth that would result in the detrimental disclosure of information under the current provisions of the FOIA. Overly broad new exemptions could, however, adversely impact the public's right to oversee important and far-reaching governmental functions and remove incentives for remedial private sector action. I urge the Committee and the Congress to preserve the public's fundamental right to know.

David L. Sobel is General Counsel of the Electronic Privacy Information Center in Washington, DC, a non-profit research

organization that examines the privacy implications of computer networks, the Internet and other communications media. He has litigated numerous cases under the Freedom of Information Act (FOIA) seeking the disclosure of government documents on privacy policy, including electronic surveillance and encryption controls. Among his recent cases are those involving the Digital Signature Standard, the Clipper Chip and the FBI's Carnivore Internet surveillance system. Mr. Sobel also served as co-counsel in *ACLU v. Reno*, the successful constitutional challenge to the Communications Decency Act decided by the U.S. Supreme Court in 1997.

Mr. Sobel has a longstanding interest in civil liberties and information access issues and has written and lectured on these issues frequently since 1981. He was formerly counsel to the National Security Archive, and his FOIA clients have included Coretta Scott King, former Ambassador Kenneth Rush, the Nation magazine and ABC News.

Mr. Sobel is a graduate of the University of Michigan and the University of Florida College of Law. He is a member of the Bars of Florida, the District of Columbia, the U.S. Supreme Court and several federal Courts of Appeals.

Disclosure

Neither Mr. Sobel nor the Electronic Privacy Information Center has received any federal grants and/or contracts during the current fiscal year or either of the two previous fiscal years.

---

[1] *See, e.g.*, "Counterpane CTO Says Insurance, Liability to Drive Security," InfoWorld (February 20, 2002), <http://www.inforld.com/articles/hn/xml/02/02/20/020220hncounterpane.xml> (According to security expert Bruce Schneier, "[t]he challenges and problems of computer and network security won't be adequately addressed until companies can be held liable for their software and the use of their computer systems").

[2] *NLRB v. Robbins Tire & Rubber Co*., 437 U.S. 214, 242 (1978).

[3] *Department of the Air Force v. Rose*, 425 U.S. 352 (1976).

[4] http://www.epic.org/security/infowar/epic-cip.html

[5] *Getman v. NLRB*, 450 F.2d 670, 673 (D.C. Cir. 1971), *stay denied*, 404 U.S. 1204 (1971).

[6] *National Parks and Conservation Association v. Morton*, 498 F.2d 765, 770 (D.C. Cir. 1974).

[7] *Critical Mass Energy Project v. Nuclear Regulatory Commission*, 975 F.2d 871 (D.C. Cir. 1992) (*en banc*), *cert. denied*, 113 S.Ct. 1579 (1993).

[8] *See GTE Sylvania, Inc. v. Consumers Union*, 445 U.S. 375 (1980).

[9] *See, e.g.*, Letter from Daniel P. Burnham, Chair, National Security Telecommunications Advisory Committee to the President, June 28, 2001 ("*Real or perceived*, barriers to [information] sharing must be removed. Among those barriers are the Freedom of Information Act and potential legal liabilities") (emphasis added).