S. Hrg. 107–550

# SECURING OUR INFRASTRUCTURE: PRIVATE/PUBLIC INFORMATION SHARING

## HEARING

BEFORE THE

## COMMITTEE ON GOVERNMENTAL AFFAIRS UNITED STATES SENATE

ONE HUNDRED SEVENTH CONGRESS

SECOND SESSION

MAY 8, 2002

Printed for the use of the Committee on Governmental Affairs

U.S. GOVERNMENT PRINTING OFFICE

80–597 PDF WASHINGTON : 2003

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENTAL AFFAIRS

JOSEPH I. LIEBERMAN, Connecticut, *Chairman*

CARL LEVIN, Michigan
DANIEL K. AKAKA, Hawaii
RICHARD J. DURBIN, Illinois
ROBERT G. TORRICELLI, New Jersey
MAX CLELAND, Georgia
THOMAS R. CARPER, Delaware
JEAN CARNAHAN, Missouri
MARK DAYTON, Minnesota

FRED THOMPSON, Tennessee
TED STEVENS, Alaska
SUSAN M. COLLINS, Maine
GEORGE V. VOINOVICH, Ohio
THAD COCHRAN, Mississippi
ROBERT F. BENNETT, Utah
JIM BUNNING, Kentucky
PETER G. FITZGERALD, Illinois

JOYCE A. RECHTSCHAFFEN, *Staff Director and Counsel*
LARRY B. NOVEY, *Counsel*
KIERSTEN TODT COON, *Professional Staff Member*
RICHARD A. HERTLING, *Minority Staff Director*
ELLEN B. BROWN, *Minority Senior Counsel*
ELIZABETH A. VANDERSARL, *Minority Counsel*
MORGAN P. MUCHNICK, *Minority Professional Staff Member*
DARLA D. CASSELL, *Chief Clerk*

# CONTENTS



## WITNESSES

### WEDNESDAY, MAY 8, 2002



### ALPHABETICAL LIST OF WITNESSES

APPENDIX

~~fidential private sector information, provides extensive protection. As my written statement explains in detail, I believe that exemption 4 extends to virtually all of the critical infrastructure material that properly could be withheld from disclosure.~~

~~In light of the substantial protections provided by FOIA Exemption 4 and the case law 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 2 years by those of us who believe that a new exemption is unwarranted. Exemption proponents have not come forward with any response other than the claim that the FOIA provides a "perceived" barrier to information sharing. They have not made any showing that Exemption 4 provides inadequate protection.~~

~~Frankly, many in the FOIA requestor 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. 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, overly broad new exemptions could adversely impact the public's right to oversee important and far-reaching government functions and remove incentives for remedial private sector action.~~

~~I thank the Committee for considering my views.~~

Chairman LIEBERMAN. Thanks, Mr. Sobel. And finally, Professor Steinzor.

**TESTIMONY OF RENA I. STEINZOR,[1] ACADEMIC FELLOW, NATURAL RESOURCES DEFENSE COUNCIL AND PROFESSOR, UNIVERSITY OF MARYLAND SCHOOL OF LAW**

Ms. STEINZOR. Mr. Chairman, thank you for the opportunity to appear before you today on behalf of the Natural Resources Defense Council.

The issues before you are both significant and troubling, especially in the wake of the tragedies that began on September 11. Obviously, all Americans recognize the importance of doing whatever we can to improve homeland security. At the same time, as Senator Lieberman said, this country was attacked because we are the most successful democracy the world has ever known. If we overreact to those who attacked us so viciously, and in the process undermine the principles and rule of law that have made us such a hopeful example for the world, terrorists will win the victory that has thus far eluded them.

[1] The prepared statement of Ms. Steinzor with an attachment appears in the Appendix on page 172.

NRDC strongly opposes both the text and the underlying principles embodied in S. 1456, the Critical Infrastructure Information Act, and urges you to consider more effective alternatives to make Americans secure.

We oppose the legislation for four reasons. The legislation has an impossibly broad scope. To the extent that the legislation focuses on cyber systems, and by these I mean systems that are connected to the Internet and therefore are vulnerable to outside disruption, NRDC as an institution has little to add to the debate. Computers are not our area of expertise. In fact some of us are still using the Windows 95 operating system.

Of course, as Senator Thompson has articulated, S. 1456 extends much further than cyber systems, covering not just computers that are connected to the Internet, but also the physical infrastructure used to house these systems. The legislation covers not just physical infrastructure that has or is controlled by computers, but also any physical infrastructure that is essential to the economy and might be damaged by a physical attack. The legislation is not limited to the Freedom of Information Act, but extends to any use by anyone of the information in civil actions. Mr. Malcolm spoke about the government's use of disinformation. I would stress, however, that this applies not just to the government but to the use of the information in a civil action by any party.

And the legislation covers information, not just copies of specific documents. It is a slender reed to rest on the adjective direct use when it covers information so broadly, and information in a different format could still be precluded from use in a civil action.

NRDC is sensitive to the fears all Americans have about our vulnerability to terrorist attacks. We are active participants in the debate about whether information about the operation of facilities during acutely toxic chemicals should be accessible on the Internet. The Environmental Protection Agency is encountering many challenges as it works diligently to sort through these issues.

But these difficult issues are not within the areas of expertise of the government agencies assigned a role in implementing S. 1456. Using legislation of this kind as a vehicle for stressing how information enhances or combats the terrorist threat to physical infrastructure is unwise and duplicative. As Senator Akaka stated so well, the legislation will have a series of disastrous unintended consequences, damaging existing statutory frameworks crafted with care over several decades.

Let me draw in another thread of history. A few years ago major industry trade associations, which had members subject to environmental regulations, began to push the idea of giving companies immunity from liability of the performed self-audits, uncovered violations of the law, took steps to solve those problems and turned the self-audit over to the government voluntarily. The Department of Justice vigorously opposed such proposals and they never made it through Congress. Several States enacted versions of self-audit laws. In the most extreme cases, EPA responded by threatening to withdraw their authority to implement environmental programs and the laws were repealed.

Self-audit bills defeat deterrence-based enforcement, creating a situation where amnesty is available even where a company has

continued in violation for many years and then decided to come into compliance at the 11th hour.

As drafted, S. 1456 is a comprehensive self-audit bill that extends not just to environmental violations but to violations of the Nation's tax, civil rights, health and safety, truth-in-lending, fraud, environmental, and virtually every other civil statute with the exception of the Securities Act. The legislation does not even require that companies cure their violations in order to receive amnesty. Redrafting may help, but it will be very hard to solve the problems as long as the legislation covers physical infrastructure. Secrecy is not the best way to protect critical infrastructure, and this Committee should abandon that approach. Rather, actually requiring changes on the ground is a far preferable solution to the threats we face.

One way to reduce the vulnerability of physical infrastructure is to ensure that employees have undergone background checks and that site security at the fence line of the facility and the area adjacent to vulnerable infrastructure is enhanced.

Another way to protect the public and workers is to eliminate the need for the hazardous infrastructure, for example, a tank holding acutely toxic chemicals. This approach, called Inherently Safer Technologies, is the cornerstone of legislation, S. 1602, now under consideration by the Senate Environment and Public Works Committee.

NRDC has also consulted with EPA officials responsible for coordinating their agency's contribution to strengthen homeland security. EPA has extensive legal authority to take actions against companies that fail to exercise due diligence in protecting such attacks. The combination of the Corzine bill and administrative action will make great strides toward addressing these problems.

As the Committee continues its consideration of these issues, we hope that you will continue to consult with a broad range of experts and stakeholders and allow us to participate in your deliberations. We appreciate the efforts of the Committee staff to undertake these discussions in order for all of us to better understand the policies, goals and implications of the legislation. Thank you.

Chairman LIEBERMAN. Thanks, Professor.

Let me see if I can ask a few of you to give a little more detail, without disclosing exactly what you do not want to disclose, which is what are we talking about here with sensitive information? Mr. Paller, in your testimony you gave us a series of examples. I wonder if any of the rest of you, Mr. Sagalow or Mr. Gent, could give us a little more general information about what we are talking about that people you represent or you yourselves would not want to disclose without this kind of exemption from FOIA?

Mr. GENT. Senator, you might remember back, I believe it was your freshmen year this Committee held hearings, and not much has changed about the electric system vulnerability since then. And one of the problems back then was that they wanted us to build a list of critical facilities, "they" being the government, so that the government could analyze that and be prepared to help us defend at those facilities at that time from physical attack of nations or nation states or terrorists. Not much has changed. We now have the cyber element that goes into this.

So government agencies are asking us to come forth with lists of critical facilities along with their degree of vulnerability and what would happen if this facility were taken out. And we have, for the last 20 years, said that we are not going to build such a list. As others have testified, we have no confidence that the government can keep that a secret.

Chairman LIEBERMAN. Got it. Mr. Miller, do you have an example that comes to mind, generally speaking?

Mr. MILLER. In the information technology industry there might be a product that is developed, a software product, which in most formats works fine, but in conjunction with a certain hardware, which a lot of these things are integrated with, different types of hardware, in fact there is a vulnerability. The software vendor may become aware of that, may decide that it wants to communicate with, however, a very limited audience, for example—just its immediate customers and clients because of that relationship, but would be totally unwilling to share that with the government because it does not want to face the possibility of broad public disclosure of that.

Again, we are talking about limited cases, not a massive virus attack, where as was discussed in the previous panel, everyone wants to work together to get the word out about a Code Red or a Nimda. We are talking about a particular—the technical term is "configuration" of a particular software product, where the impetus is to keep it in a closed community unless otherwise they are incented to do so, and particularly to share it with the government would bring a lot of risk because of this possibility, or Senator Bennett, maybe it is just the paranoia business, the likelihood that if you share it with government it will end up being disclosed.

Chairman LIEBERMAN. Mr. Sagalow.

Mr. SAGALOW. Mr. Chairman, I will give you two examples of information, falling into the areas of best practices that might be shared if there was a FOIA exemption. When it comes to the Nimda virus, Code Red, those massive attacks, that information is being shared. What is not being shared is information on risk management techniques, best practices, corporate governance, and I will give you two examples.

If a corporation becomes dissatisfied with their particular vendor, one antitrust software works very poorly and they end up deciding to terminate that contract and instead incorporate another antivirus software, you would want that information to be shared. A general counsel would be extremely reluctant to give their CEO or CTO permission to share that type of information, fearing potential defamation lawsuits from the vendor that you ended up dropping, as well as from other people for other causes of action like tortious interference with a contractual relationship.

The second example I would give you is potential shareholder actions arising out of disclosure of company practices and technology use. There is a business issue of whether you want to disclose these things since some may regard them as trade secrets. However, if all the CEOs of the world were similar to Mr. Bennett, they would disclose a certain amount of what is arguably a trade secret if it is consistent with protecting our national infrastructure and the good of society, as long as it did not do undue harm to the com-

pany. A general counsel is not going to take that attitude. A general counsel is going to say even though it is the right thing to do, there are professional plaintiff attorneys out there that will start shareholder derivative actions alleging that the act of disclosure itself was a breach of fiduciary duty.

Chairman LIEBERMAN. Thank you.

Mr. Paller made a statement which was very frank and sounded pretty realistic, that even with the exemption proposed, that there will be companies who will not share because they are still concerned in a voluntary system that it will not really be kept confidential, and therefore—not that he was recommending this, maybe he was—but that we may need a mandatory system.

Now, I wonder whether, real quickly because I want to get on to another question, whether the three of you agree or disagree, if we had appropriate exemption from FOIA do you think companies would still withhold information?

Mr. GENT. I think if you made it mandatory, they would not withhold.

Chairman LIEBERMAN. Right. [Laughter.]

Mr. MILLER. I would strongly disagree with Mr. Paller. First of all, I do not know what it would mean to be mandatory and I do not know how you would possibly enforce that, but I think the information sharing is growing. Again, I agree that the FOIA is not the silver bullet, Senator, but for the interest of the industry, yes, there is growing in the communities, electrical, financial services IT, that there is a broader community interest because these people who are American citizens. They want to support the good of the Nation. But they have to be protected on the down side. That is clearly the establishment of the ISACs, the establishment of the partnerships, that sharing of information through InfraGard is a commitment the industry is making.

Chairman LIEBERMAN. Mr. Sagalow.

Mr. SAGALOW. Our members have told us that if these obstacles are removed, there will be a substantial increase in disclosure. Of course some people will never disclose no matter what, but there will be a substantial increase.

Chairman LIEBERMAN. Professor Steinzor, let me ask you your reaction to the conversation on the last panel, which was: Why would not your concerns about the effect of the passage of Senator Bennett's legislation on various environmental laws be eliminated by inserting language that said that nothing in this proposal should diminish any obligation that anyone has under any other system of law?

Ms. STEINZOR. That would go a long way to help, but we would still be required to fight over such issues as whether there was an obligation, there was no obligation, and whether the information was submitted before the government asked for it. The way this bill is drafted it says that information is voluntarily submitted in the absence of such agency's exercise of legal authority. So the agency would have to actually ask for the information in order for it to be submitted non-voluntarily. At the moment, there is a lot of information kept in companies that the government may not have asked for yet, and if it was submitted voluntarily, the protec-

tion could be asserted. That is just one of the kinds of problems that we are concerned about.

Another way to deal with what you are talking about is a savings clause. Such a clause should be something that is dynamic, not just for laws that are on the books today but laws that are added to the books in the future.

And one last thing I would like to add, which is that to the extent that the information we are concerned about here is information that is time-sensitive, one way to approach it would be to say the protection only lasts for a certain limited period of time. We have heard a lot about an attack is ongoing and you need to share the information. Arguably, once you have shared it, once the problem is addressed, as we all assume it will be, you no longer need to make that information secret. Keeping it secret is only important to liability down the line. Again, there would be no liability if the problem was solved. So that is another way to approach this.

Chairman LIEBERMAN. Mr. Sobel, do you have a reaction to that discussion on the first panel? I know is it not directly responsive to your concerns.

Mr. SOBEL. Frankly, Senator, my concern is with this taken in combination, the fact that there would be no possibility of disclosure apparently at any time running into the future, as well as no real governmental ability to address any of the vulnerabilities that are made known to the government, and then there is this provision that I read as a very broad immunity that would also preclude any private actors from seeking corrective action. So what I see, taken as a whole, is this structure that provides information to the government, but then really ties the hands of the government or anyone else to direct and compel corrective action. As I said, I think this approach protects the negligent as well as the diligent, and that is really, I think, the main flaw. Yes, we can certainly assume that many, if not most, of the actors in the private sector are going to be good actors, but it seems to me that this just creates an incredibly large loophole for those companies that frankly are more inclined to be negligent than diligent.

Chairman LIEBERMAN. Thanks. Senator Bennett.

Senator BENNETT. Thank you, Mr. Chairman, and thanks to everyone on the panel including those who were not quite as supportive of my legislation as some of the others, because these are obviously the issues that have to be resolved, that have to be talked about.

I sponsored a bill for a long time on the privacy of medical records, and ran into much the same kind of very firm opinions on all sides of the issue, and I kept saying year after year, this is not an ideological issue, this is not conservatives versus liberals or Republicans versus Democrats. This is a management issue. How do we solve the problem? And my staff got sick and tired of me saying it. I would say, if there is a management problem raised by this objection, let us solve the problem rather than put ourselves into ideological camps and then scream at each other? We do a great deal of that in the U.S. Senate, usually on the floor, less so in committee, but we have a serious challenge here. It is one for which there is, frankly, no historic predicate because the coming of the information age has changed the world as thoroughly and fundamen-

tally as the coming of the Industrial Age did. And if you are going to talk about agricultural age warfare after the invention of the repeating rifle, you are going to be left behind. And the statement by Osama bin Laden is a chilling reminder of the fact that we live in an entirely different world, and we all, on all sides of this issue, need to view that world differently.

Now, if I were someone who wished this country ill, and I have said this before so I am not giving out any secrets, if I were someone who wished this country ill, I would be concentrating on breaking into the telecommunications infrastructure over which the Fedwire functions. If I could shut down the Fedwire, I could bring all activity in the country to a complete stop. No checks would clear. No financial transactions would take place. There could be no clearing at the end of every day for the Federal Reserve system. The Fedwire is the absolute backbone of everything that goes on in the economy. And I have had conversations with Chairman Greenspan about protecting the Fedwire from cyber attack. That specter before us, how do we deal with the challenge of telephone companies, of power companies, of brokerage houses, banks, and the Federal Government itself, that are tied together in this absolutely intricate network of transactions and facilities, and protect the Fedwire from someone sitting in a cave somewhere coming after it?

Now, Mr. Miller could share some information with us, which I have seen, that shows the graphs of the level of attacks that have come against the United States, cyber attacks, and it is a logarithmic scale. It is not just a quiet little incremental increase every year. It is almost Malthusian in terms of the predictions, and it is a hockey stick. And I have stood in the rooms where these attacks are being monitored in real time, second by second, in the Defense Department within the Pentagon. The interesting things is that just as the number of attacks is going up logarithmically, the sophistication of the attacks is going up logarithmically, so that our ability to defend ourselves, which is also going up logarithmically, is just barely keeping up with the sophistication and volume of the challenge that we have.

I first became aware of this with Y2K when I was talking with Dr. Hamre, the Deputy Secretary of Defense, as we were trying to find out in a hearing on S. 407, Mr. Chairman, over in the Capitol, where we can have classified briefings, about the degree of this country's vulnerability, and Dr. Hamre said to me, "We are under attack every day." And this was 3 or 4 years ago. And I said, "Under attack, what are you talking about?"

Well, the attack on the government facilities goes on. My fear, the thing that keeps me awake at night is that if those who are mounting those sophisticated attacks on government facilities—and they are primarily aimed at the Defense Department and the intelligence community, CIA, NSA and others—were to shift their focus onto the private sector and do so in a timing and a circumstance where no one in the government knew that that shift had taken place, how vulnerable are we, and how will we feel if we say, "Well, we did not facilitate the opportunity for people who are the recipients of those attacks to share with the government what was happening." This is not questioning. I am just responding to the panel

and sharing with you my deep, and I hope not paranoid, desire to see to it that we are prepared for this.

So in the one minute left before we go back to the second round, do any of you, recognizing this is a management issue rather than an ideological issue, have any comments across the gap that has occurred within the panel, that are not just, oh, you are wrong, you do not understand. It is easy for you to say that back and forth to each other. Do any of you have any solutions that you could suggest across the divide that has been created here within this panel in the circumstance that I have framed?

Mr. MILLER. Just a brief comment. I thought that Mr. Sobel and Professor Steinzor said that with some of the limitations that Chairman Lieberman suggested, and Mr. Malcolm discussed it in the earlier panel with you as the primary sponsor, that they might see some possibility of bridging the gap. Again, these are technical legal issues beyond my exact area of expertise, but I was pleased to hear that both Mr. Sobel and Professor Steinzor indicated that they might—if the language of the bill was even more clear as not to allow the worst bad actors to use the Freedom of Information Act language to hide behind—that they might be open to some kind of compromise. And I thought that was a very positive statement by both of them from my perspective.

Ms. STEINZOR. Senator, I could not agree with you more that this is an enormous challenge and a grave threat, and I am not by any stretch of the imagination questioning your motives or your sense of urgency about all of this. What is troubling to us is that it would seem as if a more direct way to approach this would be to try and develop technologies like the one Mr. Paller was talking about, to erect firewalls and make cyber systems more secure, rather than simply allowing for a shroud of secrecy to go over them because of the difficulties of drawing lines in this area.

You know the Freedom of Information Act, in our experience, is one of the most ponderous legal tools one can ever use. It takes months, years, to get a request answered. And so we are puzzled why the urgent exchange of information could not be protected in a short timeframe in a different way that does not implicate the Freedom of Information Act, which we do not see as a very grave threat to the immediate exchange of information. People are talking about perceptions on all sides, and we are puzzled by that.

Mr. SOBEL. Senator, if I could just follow up on that, on the FOIA point. I have a real concern that a new exemption approach could actually muddy the waters far more than they are right now. We have heard a lot of concern about the advice that a general counsel might give within a company in terms of whether or not there is adequate protection or not. It seems to me, as an attorney who looks at these issues, that 28 years worth of very clear case law would give me much more comfort in advising a client than a newly-enacted piece of legislation that contains some very broad language. I think if I was that general counsel and this legislation passed, I would say, "Well, you know, this has not yet been judicially construed. We do not know how much protection this is going to provide." I would feel much more comfortable looking at the Critical Mass decision from the D.C. Circuit, where the Supreme

Court denied certiorari, and saying, "This is a pretty good assurance that this information is not going to be disclosed."

So I do not think we are disagreeing about goals, but I think there is a real question in terms of what is the most effective way of providing the assurance that the private sector seems to want.

Mr. MILLER. Maybe that is what the hypothetical general counsel would believe, Senator Bennett. That is not what the real general counsels believe.

Mr. SAGALOW. Senator, let me follow up if I can.

Chairman LIEBERMAN. Mr. Sagalow, let me just interrupt.

Senator Bennett, I do not have any other questions. I have a couple of colleagues waiting to see me. If you are able, I would like to ask you to continue the discussion, and then when you are through, to adjourn the hearing.

Senator BENNETT. That is very dangerous on your part. [Laughter.]

Chairman LIEBERMAN. I do not want you to get comfortable with the gavel though. [Laughter.]

Senator BENNETT. Thank you, Mr. Chairman.

Chairman LIEBERMAN. Not at all. Thank you for your leadership. It has been a very interesting, important, constructive hearing, and I look forward to continuing to work with you, Senator Bennett, and with those who have been before us to see if we can resolve this in the public interest. Thank you.

Senator BENNETT [presiding]. Thank you very much.

Now, having no constraints upon me, I would like to pursue this a little further.

Mr. SAGALOW. Senator, if I could just respond to a couple of the comments that were mentioned earlier. My company created something called a Technology Alliance, which is a group of technology companies that advise us as underwriters on evaluating cyber risk, and we have been literally talking to dozens of technology companies over the last 2 years and we continue to talk to them.

I can tell you, Senator, that without exception there is no technology company that believes that there is a technology silver bullet. There is no super firewall. There is no super anti-virus or intrusion detection system. There is no single technology or combination of technologies that will solve this problem.

On the second issue of the theoretical versus practical general counsel, I agree with the comments of my colleague, Mr. Miller. I do not know what theoretical general counsels say, but I know what they say to me every day. And what they say to me every day is their view of current law and regulation including case law does not give them a sufficient basis to recommend to their CEOs to disclose. More legislation, more action is needed.

Senator BENNETT. Let me follow through on that one.

We have always been under the impression that we were helping FOIA by focusing and defining the exemption which, Mr. Sobel, you indicated has been done by case law so as to make it clear that in this circumstance under these conditions the broad exemption that is already in FOIA would clearly apply and that we were not in any way repealing or destroying FOIA, we were simply focusing the definition.

Now, Mr. Sagalow, let us go back to you—recognizing you have not had this discussion, but your perception of how a general counsel would react. Do you think that the passage of this legislation would be viewed in that regard and therefore make a general counsel more likely to say let us go ahead, or do you think they would react to the legislation somewhat in the way that Mr. Sobel is? You do not have to agree with his opinion of where they are in case law, as to try to say maybe he is right that they would say, "Well, the legislation may sound good, but it is still not going to give me any comfort."

Mr. SAGALOW. I do not know. It is a legitimate issue. I believe that, based upon the conversations that I have had so far, that the majority of general counsels would be looking at it in the first approach. They would be looking at this legislation clarifying existing case law in a way favorable toward disclosure as opposed to a de novo aspect of legislation that they would feel uncomfortable with until years of case law interpretation.

Senator BENNETT. Let us go back to Professor Steinzor's comment about time. I think that is a very legitimate issue that she has raised. I have used the example which, frankly, Professor, you shoot down, that Osama bin Laden would mount an attack and then file a FOIA request to find out how well it worked, and if indeed FOIA would require 4 years before he got the information, the technology would have been about five generations old by the time he got the information.

She has raised an interesting question, gentlemen, about putting a time limit on this, where you say the FOIA request cannot be filed for 3 years, let us say, pick a number. She would probably pick 3 months, but let us pick a number and put a timeframe on this, and talk about what effect that might have in the real world. Mr. Gent.

Mr. GENT. Senator Bennett, there are certain operational information that can be made availble moments afterwards, some hours afterwards, some days afterwards, but when it comes down to the configuration and vulnerability of the electric system, this is something that evolves over decades. So having information, in fact, to be honest with you, some of the information that is now being released to the public is still very dangerous and could be considered as a terrorist handbook. So the configuration has not changed that much. The components that are vulnerable have not changed that much over the last decade. So if you talk about operational information, I would be willing to talk about a shorter timeframe, but physical configuration of a system is still important after decades.

Senator BENNETT. We need to remember, and you have reminded us, that the physical and the cyber are inextricably linked here.

Mr. GENT. We believe that. In fact, Hoover Dam is not going anywhere.

Senator BENNETT. But the ability to break into the computers that are updated that control the sluice gates, somebody could open the sluice gates and drain Hoover Dam without blowing it up. Is that an accurate——

Ms. STEINZOR. But, Senator, that again is a cyber issue which presumably would be addressed by technology evolving within a certain period of time because cyber systems are changing all the

time. I think the emphasis on the physical configuration is exactly what concerns us because a lot of the physical configuration, for example, at a chemical plant, is heavily scrutinized and regulated by the government. And again, this protection does not just apply to Freedom of Information Act, it always applies to use in a civil action which could be either enforcement or some other type of action that would not be able to proceed if the company was not continuing to do something wrong.

So again, my suggestion about the temporal aspect is that the assumption must be that once we discover vulnerability, we are going to address it right away, whether it is in the physical context or the cyber context, that the Freedom of Information Act in civil actions would only be viable if those problems were not addressed, and therefore a temporal limitation might be just the ticket to solve the problem.

If I could just add one more thing. As an educator of young lawyers, let me talk about the theoretical versus the actual general counsel. One of the things we always impress on our students is the need to zealously protect their clients' interests, and while I would sign up tomorrow to be your general counsel, you being the hypothetical CEO——

Senator BENNETT. You might not be in a financially successful institution. [Laughter.]

Ms. STEINZOR. Well, but you were articulating such good ethics and good sense, that I think I might do it. Maybe I could keep my university job.

The problem is that if there is an opportunity to do a document dump, which of course would not be conceived in those pejorative terms, that it is both a theoretical and actual general counsel would be pushing the company to do exactly that. They would say, "Look, CEO, we have vulnerabilities involing our physical infrastructure that are very serious, and we should go contact Governor Ridge about those and get into some conversation with him, and if any agency tries to pursue us through one of the more mundane daily laws, we can fend them off while we address our vulnerabilities." This kind of situation is our concern.

I should have brought a lawyer joke for the occasion.

Senator BENNETT. I have plenty of those.

Ms. STEINZOR. Good.

Senator BENNETT. Anyone want to respond to that? Mr. Miller.

Mr. MILLER. Not so much to that, but your earlier question about time limitations. It is easy for me to say sure, why not in the information technology industry because 3 years is an eternity. But again, it is very much tied to physical issues.

A certain governor of a certain large State just to the north of here, about 4 years ago was very proud to release a document on the Internet that showed where every telecommunications, electrical network, and critical asset in the Commonwealth of his State was located, and it was very public, it was very well known. I am sure Tom Ridge was very proud of that at the time he was governor, because everyone was into disclosure using the Internet. I am sure looking back from his current position, Tom Ridge wonders how he had that crazy idea 4 years ago to make that information public.

So I would think, Senator, we need to consult with a lot more people who are, as Mr. Gent was suggesting, involved in these long-term fixed positions that may or may not be controlled by cyber relationships before we would say that the time limit idea intrinsically is a good idea.

Again, in principle, I do not think the IT industry would be too much concerned about that, but I think a lot of our customers might be because those physical assets do not change and those physical vulnerabilities do not change for long periods of time.

Senator BENNETT. Without treading into classified territory, because in this whole process I have spent an awful lot of time in places that deny that they exist after I leave them, as a general principle, someone who is looking over critical infrastructure needs to know key points. And the key point in the critical infrastructure can be taken out with a kinetic weapon many times more efficiently than it can be taken out with a cyber attack. The interesting thing that comes from those who analyze this—and I must be careful about this—the interesting thing that comes from those who analyze this for a living is that the key points in a critical infrastructure are very often not obvious. There might be a particular switch in a particular pipeline or a particular telecommunications switch, or a substation that for some reason is far more critical than any other in terms of possibly shutting down the power grid. A terrorist would give a tremendous amount to know where those key points are. And I am not sure the people who are giving information to the government, if my bill was to pass, would themselves know how key they are or where they are.

And the question becomes—the government could put that together. The government says, "OK, we have got this from this source. We have got this from this source. Uh-oh." Back to my original analysis if I am going to mix metaphors here. If this particular facility goes down, that is what shuts down the Fedwire. And the people who manage that facility do not know that. If that information—that is the pieces of information that allowed the government to discover that are individually made available with FOIA, and an analyst working for a hostile nation state comes to the same conclusion that our analyst came to, and said, "Aha, this is the one thing which if we shoot down, cuts down the Fedwire." And that become very valuable information, and maybe they make the decision, "We are not going to go after it in a cyber way. We are going to get somebody with a truck full of fertilizer to pull up to the front door of that particular facility and lo and behold everybody is going to be surprised because they think they have all of these technological firewalls everywhere else to protect the Fedwire, and bingo, we can take it out with a fertilizer bomb."

Now, that is obviously a hypothetical and obviously that kind of analysis is going on. But that is the kind of concern that I have about sharing information. And it may well be that we could find a division here between some things that could be disclosed after a 3-year period and some things that could not. I can anticipate some of you are going to say, "Well, you are not going to know that in advance," but let us at least have a quick round on that concern.

Mr. PALLER. I think you go back to the bigger question that your staff got mad at you about, about understanding it is a manage-

ment problem. And what I see happening here is what happens in lots of security conversations, which is different people looking at different parts of the animal. (1) If that is what you are going to disclose, it is terrible, and (2) if that (other thing) is what you are going to disclose, it is fine. I think maybe this is one of those really hard slogging jobs where you have to go systematically through every specific type of data in every specific type of environment and get the answers to the questions of which are going to be disclosed and which are not going to be disclosed if you want to get consensus in the room. I am not sure that the effort is going to be worth the trouble, but I do not see a way, as long as you keep a very broad view of what the "it" is, to get them to agree how long or when or whether to disclose it.

Mr. MILLER. Senator, I do not know whether it has to do directly with FOIA legislation. I mean clearly the issue of saying we do not know what we do not know is a real problem. Let me give you an obvious lesson that was learned on September 11, and that is redundancy in telecommunication systems. A lot of companies had learned over time, as part of business continuity planning, to have redundancy in their telecommunication systems, which meant having two carriers, two switches, and two sets of pipes. But a lot of companies put those switches and those pipes in exactly the same building, the World Trade Center. So when the World Trade Center went down they really did not have redundancy. They ended up not having complete telecommunication systems left. And so that was a lesson that was learned, or at least it was put out there. I am not sure whether it has been completedly learned. We are still having this debate with the Federal Government as you know, and there is legislation in Congress to require Federal agencies to begin to think about having true physical redundancy as opposed to assumed physical redundancy in telecommunication systems.

So frequently we do not know what we do not know, and we have to have a tragedy or a direct experience to learn that lesson.

Would the FOIA exemption you are suggesting help that to come together? Perhaps because who, other than the government, does exactly what you say, which is to look at all of the pieces of the puzzle. At the end of the day, his companies look at the electricity industry, I look at the IT industry, Mr. Sagalow and financial ISAC members look at the ISAC industry. Mr. Paller kind of looks across industries because he has got experts in all of these. But at the end of the day it is only the government that looks at the overall view of how these interdependencies really work in ways that nobody else really can.

Mr. SOBEL. Senator, I just wanted to make the observation that it seems to me that there is a little bit of a disconnect in terms of industry's attitude here. I mean on the one hand we are being told that the agencies that would receive the information are somehow so incompetent that they would be releasing highly sensitive information in response to a FOIA request despite very strong case law supporting withholding, and yet on the other hand industry seems to believe that there is something valuable that the government has to tell them or something valuable the government has to do in the form of coordinating response activity. So I am not getting a clear picture from industry in terms of how they see government.

Is government a competent, useful player here or is it something else, an entity that is going to receive information and very haphazardly release it to the detriment of all of us?

So I really am hearing two things here.

Senator BENNETT. My answer to that question would be yes. [Laughter.]

Mr. SOBEL. Well, then I think it raises——

Senator BENNETT. There is no such thing as industry and there is no such thing as the government. There are a variety of companies in a variety of industries. It is enormously complex, and as you have indicated, the vast majority of them would be very disciplined and act in a responsible way. And there are few, in your opinion, that would not, that would be irresponsible and would try to use this in an improper fashion. There are a variety of people in government who are enormously competent and who would provide the analysis that we need, and there are a variety of people who have demonstrated a regulatory mentality to which I referred earlier, that would use the information in a way just to prove their regulatory muscle that would be irresponsible. You only have to sit in a Senator's office to discover that there is no, "the Government." There are a variety of human beings, some of whom, most of whom, act responsibly and intelligently, and every once in a while there are some regulators who just defy common sense in the way they do their jobs and hang on to the regulations that they have.

So my answer to your question, without being facetious, is yes to both sides of it.

Mr. SOBEL. I think that is very true, but as Mr. Tritak said, if this is a question of trust and establishing trust, I do not understand why that same regulator is suddenly going to be trusted by the industry submitter to comply with your new FOIA exemption if he is not trusted to comply with the existing protections. In other words, if this is an incompetent or malicious bureaucrat, why would this new legislation create any greater trust on the part of the submitter? That is what I am really missing here.

Senator BENNETT. All you can hope for is that you nudge him in the right way.

Mr. SAGALOW. Senator, if I could just emphasize on that last point you mentioned, because that is exactly what is happening. In the real world everything is a gray area and what you need to do is nudge the general counsel in the right way. What I am hoping that you are hearing from at least the majority of people that are speaking on this area is a desire not to throw the baby out with the bath water, that this is a very essential piece of legislation, very important to the national infrastructure and our war against terrorism, and that the people on both sides of the aisle, so to speak, are willing to look at language in the bill consistent with the fundamentals: That data is received through independent use would be exempted, that under certain circumstances criminal prosecution if documented through that independent use would be permitted, that certainly it is not the intention of the legislation, and none of my members are indicating they expect it to be the intention of the legislation, that the legislation will somehow allow a company not to disclose what they would otherwise be obligated

to disclose, whether in the criminal area, the environmental area, or the financial area.

Two other quick comments. My personal belief is that the fear of data dumping or the bad general counsel while not unrealistic, is perhaps overstated. General counsels have a firm belief in the law of unintended consequences. That is why they are hesitating to permit disclosure in the first place. And part of the law of unintended consequences is if you do a data dump thinking that you are going to fool the other side, something is going to go wrong. Very few general counsels take that risk unless it is a matter of utter desperation.

And then finally on this issue of the temporal solution to the problem, I can only echo the point that was made earlier, that this issue of "we do not know what we do not know" is quite important. We really do not know in any set of documents or data what are the fundamental issues that may be completely applicable 5, 6, or 10 years from now.

Senator BENNETT. Well, the audience is voting with their feet in saying that the hearing is over. May I thank all of you for your contribution. This has been a serious discussion rather than a simple venting of opinions, and I am grateful to all of you for your willingness to enter into it in that spirit.

If I were to summarize my attitude, and speaking solely for myself, obviously, and not for any other Member of the Committee, I wish we had the time to go through all of the issues and ultimately come, as has been suggested here, to a final consensus where everybody buys off and agrees, because I think people of goodwill at all aspects of this probably could arrive there.

I must share with you once again, I feel a sense of urgency here which is very powerful, and the more time I spend with the intelligence community, the more time I spend in the Defense Department, the more times I visit that room in the Pentagon, where the attacks on our military infrastructure come in in real time and I see them on the screen, the more sense of urgency I have.

I think we err on the side of exposing our country and really with exposing the American economy, exposing the world to serious damage if we delay too long. And I would rather take steps as quickly as we can that start us down the road and maintain a perfect willingness to change the legislation as we get examples of serious violations of environmental or other circumstances by the small minority of companies that might try to take advantage of that, than delay the legislation until we can theoretically iron out all of the problems.

I do not wish to be an alarmist. I try not to be an alarmist, but I think this is an issue that requires early action. And that is why I am grateful to the Chairman for his willingness to schedule the hearing, and I am grateful to all of you for your willingness to participate.

With that, the hearing is adjourned.

[Whereupon, at 12:30 p.m., the Committee was adjourned.]

**Testimony**

Submitted by

**Rena Steinzor**

on behalf of the

**Natural Resources Defense Council**

Mr. Chairman and members of the Committee, thank you for the opportunity to appear before you today to testify regarding the management of critical infrastructure information on behalf of the Natural Resources Defense Council (NRDC). NRDC is a national, non-profit organization of scientists, lawyers, economists, and other environmental specialists dedicated to protecting public health and the environment. Founded in 1970, NRDC has more than 500,000 members nationwide, and four national offices in New York, Washington, Los Angeles, and San Francisco.

The issues before you are both significant and troubling, especially in the wake of the tragedies that began on September 11, 2001. Obviously, all Americans recognize the importance of doing whatever we can to improve homeland security. At the same time, this country was attacked because we are the most successful democracy the world has ever known. If we overreact to those who attacked us so viciously, and in the process undermine the principles and rule of law that have made us such a hopeful example for the world, terrorists will win the victory that has thusfar eluded them.

In the testimony that follows, I explain NRDC's strong opposition to both the text and the underlying principles embodied in S. 1456, the "Critical Infrastructure Information Act," and our proposals regarding how the problems that underlie the legislation should be handled. Before I launch into that analysis of the legislation's flaws, however, I want to thank Senators Bennett and Kyl for their commitment to work with public interest groups to address these problems. We have received informal assurances that several of our problems will be addressed in subsequent drafts of the legislation. Nevertheless, because no alternative language has yet become available and because certain industry supporters of the legislation have reiterated support for the original language as recently as a few weeks ago, we are compelled to remain forceful, as well as vigilant, in urging you to oppose it.

My testimony addresses the following four central points:

1. ***The legislation has an impossibly broad scope.***
2. ***The legislation will have a series of disastrous, unintended consequences, damaging existing statutory frameworks crafted with care over several decades.***
3. ***Secrecy is not the best way to protect critical infrastructure, and this Committee should abandon that approach. Rather, Congress should require covered industries to conduct assessments of their vulnerabilities and take effective action to eliminate terrorist targets.***
4. ***As the Committee continues its consideration of the legislation, it is vital that a broad range of experts and stakeholders participate in those deliberations.***

I have attached a detailed analysis of S. 1456 to my testimony and ask that it be made part of the record of this hearing.

## Scope

In a sense, S. 1456 is a piece of legislation with multiple personalities, perhaps because it has several, at times inconsistent, goals.

As I understand it, the bill was drafted before September 11, and is an outgrowth of the successful management of the "Y2K" crisis. That is, the central purpose of the bill is to facilitate the collaboration between industry and government that produced the effective response to what could have been a devastating failure of computer systems here and around the world.

To the extent that the legislation focuses on "cyber systems" – and by these I mean systems that are connected to the Internet and therefore are vulnerable to outside disruption -- NRDC as an institution has little to add to the debate. Computers are not our area of expertise. Indeed, some of our computers have not made it past Windows '95 operating systems.

As a consumer of computer products, I must confess that I wonder how companies will

be held accountable for doing everything feasible to prevent cyber-attacks if they are allowed to keep the details of how they responded to notices of such problems secret and are immunized from liability to their customers. But I leave a detailed exploration of the best approaches to these purely cyber problems to other members of this panel.

Of course, S. 1456 extends much further than cyber systems, covering not just computers that are connected to the Internet, but also the physical infrastructure used to house these systems. The legislation covers not just any physical infrastructure that is connected to, and therefore would be affected by a cyber attack through the Internet, but also any physical infrastructure that is "essential" to the "economy" and that might be damaged by a physical attack. Its coverage is so breathtakingly broad that at some point one begins to suspect that simple collaboration to prevent cyber interference may have been where it all started, but that along the way its goals became far more complex and ambitious.

NRDC is sensitive to the fears all Americans have about our vulnerability to terrorist attacks. We are active participants in the debates that continue in other contexts about whether information about the operations of facilities storing acutely toxic chemicals should be accessible on the Internet or in other contexts. On one hand, we understand the need to keep information out of the hands of potential attackers. On the other hand, we believe that the communities that would be directly affected by such catastrophes need access to information necessary to assess and respond to these threats, both before and after they materialize. Suffice it to say that the Environmental Protection Agency (EPA) is encountering many challenges as it works diligently to sort through these issues and made decisions whether to revise our approach to information about chemical use in the "post 9/11" world.

However, with all due respect to this Committee, these difficult issues are not within the areas of expertise of the government agencies assigned a role in implementing S. 1456. Further, this Committee has not focused its resources on examining these questions historically. To the extent that S. 1456 has become a vehicle for addressing how disclosure of information plays a role in enhancing or combating the terrorist threat to physical infrastructure, you have a daunting

and arguably duplicative task before you.

***Consequently, NRDC urges you to eliminate from consideration the security of information pertaining to any aspect of physical infrastructure, even facilities that are connected in some way to cyber systems.***

## Unintended Consequences

Several years ago, major industry trade associations with members subject to environmental regulations began to push the idea of giving companies immunity from liability if they performed "self-audits," uncovered violations of the law, took steps to solve those problems, and turned the self-audit over to the government voluntarily. The Department of Justice vigorously opposed such proposals, and they never made it through the Congress. Several states enacted versions of self-audit laws. In the most extreme cases, EPA responded by threatening to withdraw their authority to implement environmental programs and the laws were repealed.

The reasons cited by the Justice Department and EPA are instructive. Our system of law is based on "deterrence-based" enforcement. Or, in plain English, the prospect of getting caught is sufficiently probable and the consequences sufficiently distasteful that large numbers of regulated entities are reminded of those incentives to comply every time the government brings an enforcement action against one of their number. The government cannot prosecute all violators, and no one expects it to do so. But enforcement is frequent enough to shorten the odds and make compliance the rule, not the exception.

Self-audit bills defeat this dynamic, creating a situation where amnesty is available even where a company has cynically continued in violation for many years, "discovers" its behavior, and does nothing more than come into compliance at the last minute. The large costs avoided by such scofflaw behavior are never recovered and the company, not the government, is in charge of what can only loosely be characterized as an enforcement process.

As drafted, S. 1456 is a breathtakingly comprehensive self-audit bill that extends not just

to environmental violations, but to violations of the nation's tax, civil rights, health and safety, truth-in-lending, fraud, environmental, and virtually every other civil statute with the exception of the Securities Act. (For reasons that have never been explained, the legislation explicitly exempts the Securities Act from its secrecy provisions, setting up an anomaly where wealthy investors will still have access to the courts while all other injured consumers and customers are shut out.) The legislation does not even require that companies cure their violations in order to receive amnesty. Rather, it allows them to simply stamp materials as secret "critical infrastructure information" and turn them over to the officials designated by the Office of Management and Budget, which would have the responsibility of ensuring that the information is never used against the submitter in a civil action in court.

Staff for Senators Bennett and Kyl have explained that these consequences were not intended when they wrote the legislation, and NRDC therefore awaits a new draft of the bill before making a final judgment. But we cannot let this moment pass without expressing our profound doubts that a redraft can solve the problem easily. As long as industry is allowed to assert that information must remain secret without making any showing as to why, and no government officials are assigned to scrutinize and validate such claims upfront, it will be a nightmare to straighten the situation out after the fact, especially if "critical infrastructure information" continues to have such a broad definition.

To illustrate the problem, imagine that a company discovers that it has a tank of acutely toxic chemicals that is old and prone to leaks. The instrument panel for the tank is accessible to even its most casual employees and other visitors to the plant site, but it does not wish to bear the costs of moving the panel or replacing the tank. Someone in the general counsel's office gets the bright idea of taking pictures of this "vulnerable" infrastructure, writing a detailed report, and sending them over to the Homeland Security Office, where they join hundreds of thousands of other documents warehoused throughout the Washington area. Later, an EPA or OSHA safety inspector arrives, notices this dangerous situation, and tries to assess civil penalties against the company. The subsequent litigation turns not on whether the conduct was a violation of the law,

but rather on whether the information is indeed critical infrastructure information. Most importantly, the problem is never fixed and the company is protected from the consequences of its grossly negligent activities.

Does anyone think for even a moment that it is worth setting up such miserable legal stalemate on the off chance that disclosure of this information months or years later, pursuant to a Freedom of Information Act request or civil discovery, might increase the vulnerability of the tank to a terrorist attack? Surely there is a better way.

The next section of my testimony explains how a sister Committee and EPA are working to find a better way, but before I leave the area of unintended consequences, I would like to offer for the record a document I prepared explaining what questions must be considered if the sponsors are intent on redrafting their bill. We are far from convinced that even the best drafters could avoid serious unintended consequences, but if the sponsors are intent on pursuing this course of action, we implore you to use these questions to determine how close you are coming to that mark.

## Secrecy Is Not the Answer

In the eight months since September 11, thousands of people have spent many hours working on policies and requirements that will strengthen homeland security. The scenario I just presented involving the tank storing acutely toxic chemicals is a good vehicle to illustrate the content of those efforts.

One way to reduce the vulnerability of the tank to a terrorist attack is to ensure that only employees who have undergone background checks and are rigorously supervised are allowed in the vicinity of the tank. This approach involves both site security at the fence-line of the facility and in the area adjacent to the tank, as well as greater vigilance in selecting workers. Another way to make the tank more secure would be to move it, the instrument panel that operates it, and – for that matter – the computer system that connect them inside a locked fence or other barrier. But by far the most effective way to protect the public and the workers from the devastating

effects of an equipment failure at a facility capable of releasing gases that kill on contact is to eliminate the need for the chemical and therefore the tank itself.

This approach is called "inherently safer technology" and involves ensuring that everything that can be done is done to eliminate or reduce the storage of acutely toxic chemicals at the site. Inherently safer technology is the cornerstone of legislation introduced by Senators Corzine, Jeffords, Clinton and Boxer now under consideration by the Senate Environment and Public Works Committee. S. 1602, the "Chemical Security Act of 2001," would require EPA to regulate the efforts companies make to enhance site security and eliminate potential targets, efforts that actually solve the problem rather than sweeping it out of public view. Senator Corzine is now in the process of refining the bill to ensure that companies have the flexibility they need to assess the vulnerability of physical infrastructure and take the most effective action to prevent terrorist attacks.

NRDC has also consulted with EPA officials responsible for coordinating their Agency's contribution to strengthened homeland security. EPA has extensive legal authority to take action against companies that fail to exercise due diligence in preventing such attacks, and we are heartened to see that staff appear to be making a comprehensive effort to develop a plan for using that authority most effectively. Hopefully, the combination of the Corzine bill and administrative action will make great strides in the foreseeable future toward addressing the problems I have described above.

***NRDC believes that actually requiring changes, on-the-ground, as required by S. 1602 and EPA's existing legal authority, is a far preferable solution to the threats we face than giving companies and the government an opportunity to sweep such problems under the rug. Further, although cyber systems are not within our area of expertise, we are certain that pursuit of new technologies to forestall or blunt cyber attacks by terrorist or other criminal actors is a far more productive use of the nation's limited resources than bickering endlessly, in and out of court about what information can, should, or would be protected from disclosure.***

**Process**

In the last few weeks, Committee staff, under the direction of Senators Lieberman and Thompson, have undertaken a series of discussions with groups potentially affected by S. 1456 to better understand the policy goals and implications of the legislation. NRDC was included in these discussions, and we appreciate the diligence with which they have been pursued. We hope that this hearing marks the continuation of that kind of collaboration, rather than its end point. For all the reasons stated above: the pressing need to strengthen homeland security, the potential unintended consequences of the legislation as currently drafted, and the availability of far more effective alternatives, we believe that stakeholders with varied expertise must continue to participate in this unfolding legislative process. If NRDC had its druthers, the approach taken in S. 1456 would be dropped in favor of more direct action to solve the problem. Whether or not we get our wish, however, our perspective is an important part of this debate, as are the perspectives of those who disagree with us.

Thank you, Mr. Chairman and members of the Committee. I would be pleased to answer any questions you may have.

November 25, 2001

**Problems with S. 1456**
**Critical Infrastructure Information Act**

*Note: **Problems are listed in the order in which they appear in the draft of the legislation dated November 6, 2001, and not necessarily in the order of their importance.***

**Sec. ___ 02. FINDINGS.**

**FINDING (8): Page 4, lines 15-25 and page 5, lines 1-5:**

These paragraphs indicate congressional intent to apply the legislation as broadly as possible to virtually every sector of the economy. They further state that in order to encourage voluntary submission of any information about any aspect of an industry's physical infrastructure, the government must pledge not to disclose it if disclosure would "result in legal liability or financial harm."

The scope of this language goes far beyond efforts to preserve the security of computer systems or even physical plants in the event of a criminal attack. Rather, the language clearly invites all sectors of the economy to submit any information they would prefer to keep confidential ***in order to avoid legal liability or financial harm.*** Thus, for example, companies could submit information about illegal acts they have committed, from tortious conduct to tax fraud, and be protected from having the information used to hold them accountable.

**FINDING (9): Page 5, lines 6-13:**

This provision compounds the impression that the legislation could be used as a source of amnesty for legal violations by specifically encouraging companies to engage in "risk assessments" and "risk audits," turn such information over to the government, and thereby preclude its use in any subsequent prosecution of the company. In the environmental arena, "risk audit" is a term of art meaning an evaluation of a company's compliance with the nation's environmental laws. For many years, industry has engaged in an ***unsuccessful*** effort to persuade Congress to grant exactly this type of self-audit privilege. Congressional committees have rejected these proposals because they would encourage chronic violators to periodically purge themselves of the consequences of their violations by turning the results of their internal audits over to the government.

**FINDING (13): Page 6, lines 13-17:**

This finding – stating that the information covered by the bill is "not normally in the public domain" -- is clearly erroneous, suggesting that the legislation has a far broader scope than its authors may have intended. A large majority of the information regarding normal industrial operations that would be protected from disclosure if the legislation is enacted into law is routinely in the public domain, and has been for several decades.

**Sec. ___04. DEFINITIONS.**

**Section 04 (4) "Critical Infrastructure": Page 9, lines 3-25, page 10, lines 1-2:**

Paragraph (4)(A) applies the legislation's non-disclosure provisions to virtually any aspect of a company's normal operations by including "physical, information, and data systems and services essential to . . . [the] economy of the United States." The legislation does not require that the impact on the economy be significant or that the damage have some effect on the national security. Under this definition, the smallest, temporary malfunction of any piece of equipment would be covered, even if it caused no lasting damage to a company's performance. Major damage caused by the company's own negligence would be similarly protected.

The definition further encompasses "all types of communications and data transmission systems, electric power, gas and oil production, refining, storage, transportation and distribution, banking and finance, transportation [sic] water supply, emergency services . . . the continuity of government operations, and their associated protected or essential systems." Under this broad language, routine monitoring of emissions of toxic chemicals into the air, discharges of toxic chemicals into water, or the level of toxic chemicals in the ambient air within a workplace could be kept secret if the company claimed that disclosure would "affect" the economy. This extraordinarily broad coverage is far more extensive than critical computer system information necessary to launch a terrorist attack.

Completing the effort to draw as wide a parameter as possible for the scope of the legislation, paragraph 04(b) includes "any industry sector designated by the President pursuant to the National Security Act of 1947 . . . or the Defense Production Act of 1950." These statutes give the President the authority to designate any industry that now sells – or might sell – products to the United States military, encompassing everything from armaments to baseball caps and suntan lotion.

**Section 04 (5) "Critical Infrastructure Information": Page 10, lines 3-25, page 11, lines 1-2:**

This definition continues to define an extremely broad scope for the legislation. The first subparagraph – (5)(A) – covers the information that is the ostensible focus of the bill, namely the ability of critical infrastructure to resist criminal interference. Even in this relatively discrete provision, however, the temptation to extend the legislation's parameters surfaces when it covers "attack[s] or similar conduct" that "harms interstate commerce," whether or not the conduct was criminal. Since "harm" to interstate commerce can include even minor damage, this provision encompasses non-criminal, even inadvertent conduct that causes any temporary interruption of normal business operations.

The next three subparagraphs – (5)(B), (C), and (D) – are even broader in application, extending the legislation's secrecy provisions to "any planned or past assessment . . . of the security vulnerability of critical infrastructure . . . including . . . risk management planning, or risk audit." Since "security" is not defined in the legislation, but commonly means the safety of

a system or set of industrial practices, this provision encompasses any analysis of a company's vulnerability not just to an attack, but to normal malfunctioning of equipment, human operational errors, or system failure. As noted earlier, the manufacturing sector has attempted unsuccessfully for years to persuade Congress to grant ***immunity from civil liability for violations of health and safety regulations, including those issued by EPA or OSHA***, if it conducts risk audits and submits them to the government. This provision would have the same effect as that rejected legislation, circumventing the normal legislative process and bypassing the committees that have considered these proposals and rejected them in the past.

Finally, subparagraph (5)(C) of the legislation protects the confidentiality of information about "any planned or past operational problem or solution, including repair, recovery, reconstruction . . . related to the security of critical infrastructure." This provision, while in certain respects redundant with subparagraph (5)(B), confirms legislative intent to cover the expansion of a facility's operating equipment in order to address past problems, effectively shrouding the unpermitted construction of new sources from EPA review. Thus, a company could replace the equipment of a "major source" as defined by the Clean Air Act, producing a new operating system that discharges twice the emissions, without applying to EPA for a new permit, and EPA could do nothing to enforce the law if information about construction of the new source was submitted "voluntarily" to the government.

### Section 04 (6) "Information Sharing and Analysis Organization": Page 11, lines 3-25, page 12, lines 1-2:

This provision invites the creation of industry trade associations called "information sharing and analysis organizations" (ISAO), for the explicit purpose of gathering and submitting information that would be covered by the confidentiality protections of the legislation. *(See also subparagraph (8)(A), page 12, lines 17-25 and page 13, lines 1-2, explicitly inviting ISAOs to submit information "voluntarily" on behalf of their members.)* Since freedom from civil enforcement would be a tremendous advantage to potential members of such organizations, it is likely that every major corporation will be solicited for membership in an ISAO, and will take full advantage of the bill's protections. Smaller competitors of such large entities may not be solicited, or may conclude that they cannot afford the dues or other fees charged by ISAO, making them targets for frustrated government enforcement programs, an outcome contrary to sound public policy and basic fairness.

### Section 04 (7) "Protected System": Page 12, lines 3-16:

This definition confirms the broad application of the legislation's secrecy provisions to "any service, physical or computer-based system, process or procedure that directly or indirectly affects a facility of critical infrastructure." Under this overreaching language, the malfunctioning of a stove in the corporate cafeteria could fall within the legislation's scope, an absurd but obvious result of such expansive language.

**Section 04 (8) "Voluntary": Page 12, lines 17-25, page 13, lines 1-23, page 14, lines 1-2:**

This crucial provision defines "voluntary" submission to include any conveyance of covered information by a covered entity with respect to a covered facility and a covered threat. The only limitation on this broad scope is that the submittal of the information must be made "in the absence of such agency's exercise of legal authority to compel access to or submission of such information." While this language is admittedly ambiguous, it could be read to include any information submitted by a company that is not already the subject of a subpoena or other access order compelling disclosure of the information. Because the provision uses the present tense, requiring that the agency ***has exercised*** its legal authority, the exclusion it creates is significantly narrower than an exclusion tied to coverage of the information by another legal authority that could be exercised at some time by an agency. Therefore, the definition of "voluntary" explicitly encourages companies to rush to submit information under the legislation in order to avoid some subsequent exercise of subpoena or other legal authority by a regulatory agency. Once covered by the legislation's secrecy provisions, the information could not be disclosed by the agency, to anyone – including a civil court judge – in perpetuity. *(For the text of these sweeping protections, see Section 05, pages 14, lines 4-25, page 15, lines 1-25, page 16, lines 1-25, page 17, lines 1-25, page 18, lines 1-4.)*

The legislation underscores and confirms this excessively broad definition of a "voluntary" submission by specifically excluding from the exclusion information involved in any ***ongoing action*** brought under the Securities Exchange Act. Or, in plain English, even if the SEC has not subpoenaed such information in an action it has already filed, the company is precluded from taking advantage of the legislation's confidentiality provisions and the information can be used to prosecute the civil case. Under standard principles of statutory interpretation, this exclusion will be read to mean that if the IRS, the Departments of Justice or Defense, EPA, OSHA, or any other agency or department is prosecuting a civil action for tax evasion, contractor fraud, violations of environmental permits or workplace safety standards, the company can preclude use of information that was previously submitted "voluntarily" whether or not it receives a government subpoena.

The legislation further excludes from the exclusion "information or statements required as a basis for making licensing or permitting determinations." Or, in other words, information that agencies or departments specifically direct applicants to include in their requests for permits or licenses can be disclosed. Any information submitted voluntarily as part of a permit application, or submitted later to demonstrate compliance with the permit, presumably would be kept confidential.

**Sec. ___ 05. PROTECTION OF VOLUNTARY SHARED CRITICAL INFRASTRUCTURE INFORMATION.**

**Section 05(a) "Protection": Page 14, lines 4-25, page 15, lines 1-25, page 16, lines 1-3:**

This section explicitly repeals all other provisions of law, including state and local laws, that pertain to the information and entities covered by the legislation's provisions, as explained above because it opens with the unequivocal statement "[n]otwithstanding any other provision of law . . ." as an introduction to its confidentiality protections.

The section further provides that "critical infrastructure information . . . that is voluntarily submitted to a covered Federal agency . . . for [any] informational purpose . . . shall be exempt from disclosure" under the Freedom of Information Act. This broad prohibition means that federal agencies will be barred from disclosing unknown quantities of information that they routinely disclosed before to citizens, and to state and local appointed and elected officials, including local prosecutors, and police and firefighting personnel unless some other provision of law other than the Freedom of Information Act authorizes such disclosure.

Even if disclosure to state and local enforcement officials or emergency personnel is authorized by another law, the legislation bars disclosure if the federal agency has not received the "written consent" of the "person or entity" that submitted it. The information covered by this broad prohibition includes not only "critical infrastructure information" itself but also the "identity of the submitting person or entity." Disclosure is barred "in any civil action arising under Federal or State law if such information is submitted in good faith," thereby precluding any and all enforcement actions. Although the legislation does not repeal the enforcement powers of federal agencies and departments, no target of an investigation would voluntarily settle its case if the federal agency or department was legally precluded from bringing the matter to court. The explicit identification of civil actions leaves no doubt that the intent of the legislation is to provide immunity from civil violations.

The legislation would also accomplish an unprecedented preemption of state liability laws, including the common law of tort allowing victims of chemical exposure to recover damages, because it states that "critical infrastructure information . . . shall not, without the written consent of the person or entity submitting such information, be used by any third party in any civil action." This provision could be read to mean that if "critical" information is first submitted to a federal agency, a company need not disclose in any subsequent litigation brought by any private citizen. The sponsors may have intended merely to preclude a private third party from using the ***government's copy of the information*** in a civil action, allowing private parties to gain access to other copies of the information, including copies maintained by the company, through the normal judicial process. However, this limitation is nowhere specified in the legislation, which speaks generally of "critical information" without specifying any particular custodian or version.

Further compounding these problems, the federal agency or department is barred from using or disclosing the information, including the identity of the submitter, without the

submitter's written consent for any other purpose with only two exceptions. Unless disclosure is covered by one of these two exceptions, agencies and departments may not rely on voluntarily submitted information, including the identity of the submitter, when they are crafting regulatory provisions; issuing guidance regarding interpretations of the laws under their jurisdiction; conducting routine inspections of facilities selling food and other products to the public; responding to congressional requests for information; or performing studies and compiling reports not explicitly required by the legislation itself.

It is not an overstatement to suggest that this extraordinarily broad prohibition on disclosure could bring the normal regulatory process to a grinding halt, placing great pressure on those two exceptions.

The first exception permits disclosure during the "proper performance of the official duties of an officer or employee of the United States." *(See section 05(a)(D)(ii) on page 15, lines 8-10.)* The underlined terms have been interpreted by the courts extensively in the context of enforcement of section 1983 of the U.S. Code, which provides for punishment of federal and local officials who abuse civil rights. Such officials may not be held liable if they were performing their official duties properly, and the law has evolved in a manner that takes into account multiple nuances and implications of this ambiguous wording. In any given factual circumstance, extensive legal research and analysis would be necessary to find precedent indicating what those terms mean. If the legislation becomes law, it is entirely possible, even likely, that this exception will be interpreted narrowly and, since the legislation explicitly prohibits any legal challenge to its implementation, the courts will be barred from intervening to assist in the correct application of this language. *(See Section 08, page 26, lines 22-25, barring private rights of action to enforce the legislation's provisions.)*

In sum, the first exception does nothing to narrow the scope of the legislation unless the federal, state, and local officials implementing its provisions decide in their discretion to so limit it. Further, one official might assert that he is exercising his authority appropriately and wishes to disclose information, only to be contradicted by another official with a different motivation to keep the information secret.

The second exception is that information may be disclosed "in furtherance of an investigation or prosecution of a criminal act." *(See Section 05(a)(1)(D)(ii), page 15, lines 11-12.)* This exception is unambiguous and fortunate.

### Section 05(b) "Independently Obtained Information": Page 16, lines 4-12

This crucial provision may have been intended as a "savings clause" to counteract the drastic implications of Section 05(a) discussed immediately above. Unfortunately, the language of the subsection is so garbled that it may well be read to have no effect on the legislation's broad prohibitions on disclosure. The language reads: "Nothing in this section shall be construed to limit or otherwise affect the ability of a state, local, or Federal government entity . . . to obtain critical infrastructure information in a manner not covered by subsection (a) . . . and to use such information appropriately." Read in the context of the other provisions of subsection 05 (a), including and especially the ban on disclosing information unless it was previously subpoenaed,

this provision is likely to be read to mean that any information that ***is*** covered by subsection (a) must be kept confidential. Thus, the savings clause would only cover information that is ***not*** covered by subsection (a): that is, information that was not "voluntarily" submitted to the government. In effect, this provision penalizes companies that are too ignorant to submit sensitive information voluntarily, but fails to preserve the essential government enforcement and rulemaking authorities nullified by subsection (a).

### Section 05(c) "Treatment of Voluntary Submittal of Information": Page 16, lines 13-18:

This provision, potentially another "savings clause" for other provisions of federal law requiring companies to submit information to the government, also fails to circumscribe the legislation's secrecy provisions appropriately. The provision states that voluntary submittal of information to – for example – the White House Homeland Security Office or the Department of Defense – does not "constitute compliance" with other requirements that the covered entity submit the information to another agency or department. The provision does ***not*** say that if the information is submitted to another agency or department, that agency or department may disclose it even if confidentiality has been claimed in the submission to the Homeland Security Office or DOD. Thus, a plausible interpretation of this provision is that a company can submit the information voluntarily first, claiming that it is entitled to confidential treatment, and then resubmit it to a second agency or department, claiming the same right to confidential treatment. The second submission complies with the independent requirement that the information be submitted without jeopardizing the goals of the legislation. Indeed, to read the provision any other way would arguably vitiate the legislation's findings, purpose, and legal effect.

**February 18, 2002**

## Questions to Clarify Intent of S. 1456

Prepared by Rena Steinzor, Natural Resources Defense Council
(202) 289-2364 or rsteinzor@nrdc.org

**Note**: Participants in the debate over the Critical Infrastructure Information Act (S. 1456) have strongly disagreed not only about the policy goals of the legislation, but also with respect to what its key provisions mean. Confusion over the intent of the language has obscured and frustrated the discussion and resolution of legitimate policy disputes. The following questions are an effort to clarify the intent of the language so that perceived drafting problems can be addressed, allowing the debate to focus on those core policy issues.

### Threshold Assumptions:

What evidence exists to document whether and why companies refuse to share sensitive cyber security information with the government?

Why do companies fear that information submitted voluntarily, will be made public under the Freedom of Information Act, given the D.C. Circuit Court of Appeals holding in the Critical Mass case (975 F.2d 871 (1992)) that such materials are exempt from disclosure?

### Circumstances Covered:

Is the legislation intended to cover:

a. attacks from one computer system to another ("cyber attacks") – e.g., hackers send Love Bug to U.S. computers supporting the Pentagon;
b. attacks from one computer system to another that result in damage to physical infrastructure (e.g., hackers send Love Bug to computers controlling the operation of the Power Grid, resulting in black-out that causes heavy machinery to break down); or
c. attacks on physical infrastructure that damage cyber systems (e.g., terrorist plant bomb in building that houses server for power supply company).

### Consequences Covered:

Is the legislation intended to:

a. eliminate use of voluntarily submitted "critical infrastructure information" to support legal liability in civil law cases brought in a public law context (e.g., company X turns in documents labeled "critical infrastructure information" indicating that it has evaded tax laws by depreciating equipment too quickly);

b. eliminate use of critical infrastructure information to support civil liability in a private law context (company X turns in documents indicating that it is aware of weaknesses in a manufacturing process and these weaknesses result in an explosion that badly injures nearby residents, who sue to recover damages);
c. affect the federal government's ability to share information among agencies and departments (e.g., the information described in (a) is turned over to the Homeland Security Office and subsequently requested by the IRS); or
d. affect the federal government's ability to share information with state and local officials (e.g., the information described in (b) is requested by a state environmental agency investigating possible violations of the laws it administers).

**Type of Information Covered:**

The legislation defines "critical infrastructure information" as information "related to the "ability of any critical infrastructure" to "resist interference, compromise, or incapacitation by either physical or computer-based attack or other similar conduct. Is the legislation intended to cover:

a. computer security systems intended to prevent cyber attacks;
b. security systems intended to prevent physical attacks;
c. information regarding the operation of a manufacturing process that could be used to either choose the facility as a target or to promote a cyber or physical attack;
d. information about the company's products or customers that could be used to either chose a facility as a target or to promote a cyber or physical attack;
e. administrative or financial details regarding a company's operation that might suggest that its facilities would make good targets or that would promote a cyber or physical attack (e.g., the company has suspended required maintenance because it has encountered financial difficulties or the company's union contract with operating engineers is about to expire); or
f. vulnerability of any aspect of the company's operation to misconduct attacks by its own employees. For example, misconduct "similar to a cyber or physical attack" might include administrative fraud or omissions or a slow-down in work performance by disgruntled workers.

**Status of Covered Information:**

The legislation's findings state that it is intended to cover information that would not "normally [be] in the public domain," but this caveat is not repeated in the legally operative portions of the bill. Is the legislation intended to cover:

a. information that the law requires companies to keep but that they do not routinely turn over to the government;
b. information that the company elects to keep to demonstrate its compliance with the law; or
c. information that is generated in a self-audit that documents potential law violations.

**Bill Implementation:**

Once a company designates documents as covered by the legislation's confidentiality provisions, does the legislation envision any review of the legitimacy of those assertions by a neutral government official?

If a company designates documents as covered by the bill, a member of the public subsequently requests the information, but the company refuses to give consent to the release of the information, what kind of recourse will be available to the requestor?

What agency or department will serve as the repository of information covered by the legislation, or may any agency or department become a repository?

Under which of the following situations is information protected by the legislation's confidentiality provisions:

a. information stamped confidential is simultaneously submitted to a federal enforcement agency and the Homeland Security Office. It later turns out that the information indicates that the company has committed civil violations of the laws enforced by the agency; or
b. information stamped confidential is submitted to the Homeland Security Office after unstamped information has been submitted to another federal enforcement agency. The enforcement agency is preparing to go to court to seek penalties for conduct documented in the documents.

**Exemptions:**

Would the legislation protect from disclosure information that a federal agency or department could obtain by subpoena or other legally binding information request, whether or not such a subpoena or request has been transmitted to the submitter?

If information is already in the public domain, is it still qualified for confidential treatment under the legislation?

If the same type of information is – or routinely has been – in the public domain, is it still qualified for confidential treatment under the legislation?

What kinds of activities would constitute the "proper performance of official duties" by a government representative sufficient to exempt information from the protections of the bill?