Testimony
before the
Committee on Governmental Affairs
U.S. Senate
regarding
Critical Infrastructure Information
Submitted by
Rena Steinzor
on behalf of the
Natural Resources Defense Council
May 8, 2002

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?