STATEMENT OF
JOHN G. MALCOLM

DEPUTY ASSISTANT ATTORNEY GENERAL
CRIMINAL DIVISION
U.S. DEPARTMENT OF JUSTICE

BEFORE THE COMMITTEE ON
GOVERNMENTAL AFFAIRS
U.S. SENATE

MAY 8, 2002

Mr. Chairman and Members of the Committee, thank you for this opportunity to testify about the Department of Justice's efforts to protect our nation's critical infrastructure and about information sharing related to that protection. The issues before this Committee today are of great importance, and I commend the Committee for holding this hearing.

In my testimony today, I would like to outline briefly the nature of critical infrastructure protection, the information sharing problem and the Department's current efforts to combat that problem. It is clear to the Department that information-sharing is a serious issue, and that its complexity presents a significant challenge to law enforcement.

-

The nature of the issue

The safety of our nation's critical infrastructure is of paramount concern to the Justice Department. As you know, the term "critical infrastructure" refers to both the physical and cyber-based resources that make up the backbone of our nation's telecommunications, energy, transportation, water, emergency services, banking and finance, and information systems.

The problem of ensuring delivery of critical infrastructure services is not new. Indeed, owners and operators of critical infrastructure facilities have been managing risks associated with service disruptions for as long as there have been such facilities. However, the operational challenge of ensuring the delivery of the broad array of services that now depend upon the Internet and other information systems is a challenge that has grown exponentially in the last several years. The burgeoning dependence of the U.S. infrastructure on the Internet has exposed vulnerabilities that have required the U.S. government to mount new initiatives, to create new federal entities to help manage critical infrastructure protection efforts, and to seek prevention, response, and reconstitution solutions.

The safety of our nation is our first and overriding objective. The Justice Department has been working across government to address infrastructure issues for several years. The attacks of September 11 heightened our awareness of these issues and have pushed us closer to resolution on some issues. Following those terrorist attacks, the Congress enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT Act). That Act, which the President signed into law in October 2001, amended U.S. laws to further critical infrastructure protection efforts by increasing sentences for those committing cyber attacks, improving our ability to use procedural tools to track sources, and enabling law enforcement to share wiretap and grand jury information with others responsible for homeland defense when appropriate.

U.S. infrastructure protection efforts are the shared responsibility of many entities, both public and private. Much of this joint effort is based upon the principle that a robust exchange of information about threats to and actual attacks on critical infrastructures is a critical element for successful infrastructure protection efforts. The following are just a few of the entities dedicated to this principle: the National Infrastructure Protection Center, the Department of Justice's Computer Crime and Intellectual Property Section, Information Sharing and Analysis Centers, the Critical Infrastructure Assurance Office, the Office of Homeland Security, and the Federal Computer Incident Response Center

To better protect critical infrastructures, government and the private sector must work together to communicate risks and possible solutions. Acquiring information about potential vulnerabilities from the private sector is essential.

Doing so better equips us to fix deficiencies before attackers can exploit them. For example, a telephone company might discover a vulnerability in a widely used component of our telephone network that makes the network susceptible to disruption by hackers. If we concentrate our time and energy on remediation of terrorist attacks after they occur, we have already lost. Information is the best friend of both prevention and response. We recognize that we can protect the nation only if the private sector feels free to share information with the government.

However, industry often is reluctant to share information with the Federal Government. One reason given by industry for not sharing information is that the government may later have to disclose that information under the Freedom of Information Act, or FOIA. Industry also is

concerned that sharing information among companies will lead to antitrust liability, or that sharing among companies or with government will lead to other civil liabilities (e.g., through a product liability suit or a shareholder suit). Without legal protections regarding information needed by the government in order to safeguard our infrastructure, even the most responsible, civic-minded companies and individuals may hesitate before sharing such crucial information, fearing that competitors may obtain that information and use it to their advantage.

With this in mind, both the Senate and the House of Representatives have actively considered and are currently considering bills that would specifically bar disclosure under the Freedom of Information Act of any information that is voluntarily submitted to government agencies to protect our critical infrastructure. Such a "corporate good Samaritan" law would provide the necessary legal assurance to those parties willing to voluntarily provide sensitive information to the government that they would not otherwise provide.

The Justice Department believes that the sharing of private sector security information on critical infrastructure between private sector entities and with the federal government to avert acts that harm, or threaten to harm, our national security is of the utmost importance. We are prepared to work closely with Congress to pass legislation that provides this important legal protection.

The Freedom of Information Act

Congress passed the Freedom of Information Act more than thirty-five years ago. FOIA established an effective statutory right of access to government information. The principles of government openness and accountability underlying FOIA are inherent in the democratic ideal.

However, achieving an informed citizenry is a goal that is sometimes counterpoised against other vital societal aims. Society's strong interest in an open government sometimes conflicts with other important interests of the public--such as the preservation of the confidentiality of sensitive commercial and governmental information. Though tensions among these competing interests are characteristic of a democratic society, their resolution lies in providing a workable formula that encompasses, balances, and appropriately protects all interests, while maintaining emphasis on the most responsible disclosure possible. It is this accommodation of countervailing public concerns, with disclosure as the predominant objective, that FOIA seeks to achieve.

The Freedom of Information Act generally provides that any person has a right, enforceable in court, to obtain access to federal agency records, except to the extent that one of nine exemptions protects such records (or portions of them) from disclosure or they are protected by one of three special law enforcement record exclusions. Two exemptions are relevant here: 5 U.S.C. §§ 552(b)(3) and (4).

Exemption 4 of FOIA protects "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." The exemption affords protection to those business submitters who are required to furnish commercial or financial information to the government, either directly or indirectly, by safeguarding them from the competitive disadvantages that could result from disclosure. That exemption covers two categories of information in federal agency records: (1) trade secrets; and (2) information that is (a) commercial or financial, and (b) obtained from a person, and (c) privileged or confidential. Exemption (3) of FOIA incorporates the disclosure prohibitions contained in various other federal statutes.

Case Law on Exemption 4

Over the years, a considerable body of law has developed, much of it in the form of decisions of the United States District Court for the District of Columbia and the Court of Appeals for the District of Columbia Circuit. In practice, the great majority of FOIA disputes revolve around whether the submitted information qualifies as "confidential" as that term has been judicially interpreted within the context of Exemption 4. It is important to recognize that the courts have regularly rejected any notion that either an information submitter's request for confidentiality, or an agency's promise that submitted information would not be released, by itself, suffices to insulate such information from disclosure under FOIA.

Under the District of Columbia Court of Appeals decision in Critical Mass Energy Project v. NRC, commercial information or information that is required to be furnished to the Government can be withheld primarily to the extent that the Government can demonstrate that its disclosure would result in "substantial competitive harm." However, where information is "voluntarily" submitted to the government, such information is protected to the extent that it is not "customarily" disclosed to the public by the submitter, a considerably easier standard to satisfy. It is our expectation that most information regarding critical infrastructure vulnerabilities will fall into the "voluntarily" submitted category and will, therefore, readily qualify for Exemption 4 protection under the DC Circuit's Critical Mass decision. At the same time, both we and business submitters are aware that this D.C. Circuit Court precedent might not come to be accepted in all other judicial circuits, which gives rise to reasonable concerns.

Were the decision in Critical Mass a definitive legal principle decided by the United States Supreme Court, concerns regarding protection of this information would be greatly reduced. Since that is not the case, the Department recognizes that the broad protection afforded such information by the District of Columbia appellate court does not provide the complete assurances to the submitters of private sector infrastructure that they seek. Nor will protection be categoric in those instances in which information regarding vulnerabilities are included as part of a submission by state and local government entities.

Other Issues

Although FOIA is a major issue, it is not the only issue here. Some companies also claim that sharing information with the government, or each other, will lead to liability and possible antitrust suits by the government or by their competitors.

Legislative Action

The Department appreciates the continuing interest of the Congress. During the 106th Congress, bills were introduced in both the Senate and the House to address these issues. Both bills focused on protecting critical infrastructure information provided to the government from compelled disclosure under FOIA. Both bills also address the antitrust and liability issues.

Last session, Senators Bennett and Kyl again introduced a bill. Key provisions of their bill:

- shield from disclosure under FOIA, with a specific request by the company that submitted the information, critical infrastructure information voluntarily submitted to certain federal agencies;
- limit use of shared information in civil proceedings; and
- exempt critical infrastructure information-sharing activity from the antitrust laws.

Representatives Davis and Moran also introduced a new version of their bill. Although similar to the Bennett-Kyl bill, it more tightly restricts the government's use of such information. Later in the session, a consensus bill was developed, but not introduced.

Justice Department Concerns

Under the existing case law on Exemption 4 of FOIA, the Justice Department believes that critical infrastructure information submitted to the government should be protectible from disclosure. However, we realize that some in industry disagree or, at least, are lacking the certainty that allows them to comfortably submit information to the government with complete assurance that it will not be disclosed. Since the goal of our information sharing efforts is to increase

information flow to the government, we need to address the concerns of these companies. Indeed, in a letter to the National Security Telecommunications and Advisory Committee last fall the President expressed his support for "a narrowly drafted exception to the Freedom of Information Act to protect information about corporations' and other organizations' vulnerabilities to information warfare and malicious hacking." An important point is that, without such a statutory provision, the government would never obtain the information, and, thus, would not have it to disclose to begin under FOIA. Such a state of affairs, moreover, would not serve our vital national interests.

Scope of the Information Protected

By the same token, it is crucial that any bills be carefully crafted so as not to unnecessarily shield information. Defining critical infrastructure is difficult, and, on balance, the Department believes that a broad definition is better suited to this issue. Our objective is to reassure companies that appropriate information will be protected. Too narrow a definition may leave a company in doubt and result in the information being withheld from the government out of fear of FOIA disclosure, the very result we seek to prevent.

On the other hand, a bill that sweeps in too much information is just as bad. For example, suppose a bill were to protect all information (1) submitted by a person, (2) to a covered Federal agency, and (3) for informational purposes. If that were so, any information obtained by the EPA during a witness interview would likely be covered, since it would constitute information submitted by a person, to a covered Federal agency, for informational purposes. Such a bill would clearly cover too much information, and would not serve our national interests.

Three approaches are available to reduce this problem. First, drafters must make clear that any bill does not cover independently-obtained information. For example, let us suppose that a company submits valid critical infrastructure information to the Office of Homeland Security. Entirely independently, the EPA develops the same information in an investigation. The government should be able to use the EPA's information without restriction. If this were not so, any information sharing bill would quickly turn into a shield, allowing companies to use the protections of the bill to dump information on the government and thus shield it for all time and for all purposes. In a sense, it is important to protect the "copy" of the information submitted to the government, but not the information itself.

Second, resolve the issue of who may receive the information in favor of designated agencies only. The choice here is between allowing any agency of the government to receive critical infrastructure information, or allowing only designated agencies or departments to receive it. We recommend that agency heads designate which components or bureaus, if any, may actually receive such information. This would provide for flexibility (agency heads could designate any appropriate office) and certainty (designated offices would know how to handle submitted information). This solution would also help prevent use of the Act as a sword–if an agency head did not want a component to receive protected information that might raise a question of immunity or improper use of voluntary submitted information, he or she could not designate that component.

Third, retain the provisions of the existing bills that require companies to voluntarily submit the information in order to obtain the protections of the bill. If the information is not so submitted–if it is instead produced in response to subpoena or a program requirement–the information is not covered. A voluntariness requirement is important because the goal of information sharing efforts is to encourage companies to share information that the government is not otherwise receiving.

We also suggest requiring that the submitter explicitly request the protection of the statute for two reasons. First, some information does not need protection, nor does industry want all information to be protected – yet all information would be automatically protected if no request is required. Second, a request will help the government identify the protected information, especially where such notification appears on the document itself.

Liability

As I mentioned earlier, FOIA is only the first of three issues raised by industry. The second issue relates to liability concerns. Some companies have expressed concern that, should they share information with the government, the government could then use that information in a civil or criminal suit against them. While perhaps legitimate concerns, let me be clear that the Justice Department would not support legislation that would prohibit the government from using voluntarily provided information in a criminal proceeding. Other mechanisms exist to give a company some consideration

and possible benefit for voluntarily providing information about criminal violations. Some of these are outlined in the Justice Department's 1991 Policy on Voluntary Disclosures.

If Congress chooses to include civil liability protections, the protections must be very carefully crafted so as not to hamper, or even eviscerate, law enforcement objectives. The bills already introduced include civil liability provisions. Some drafts of the liability provision have included so-called "indirect" use protections. We strongly believe that, at most, only "direct" use should be prohibited, since indirect or derivative use is extremely difficult to disprove. A similar issue frequently lurks in immunity proceedings in criminal cases, where the Federal government, in order to proceed with a criminal prosecution, may have to disprove derivative use of a defendant's statements in a so-called Kastigar hearing. In the civil context, for example, should the government receive information about a vulnerability under an information-sharing bill that included indirect civil protection and then seek to sue the submitter, we would be required to prove that the submitted information was not used in any way in the investigation, including developing leads. In essence, we have to prove that all of our evidence came from independent sources. Past experience clearly demonstrates that this is a very difficult burden to meet.

State Laws

As you know, infrastructure protection efforts are a cooperative effort among the Federal Government, industry, and State and local governments. Any information sharing bill needs to consider how and when information may be shared with State and local governments. All States have their own FOIA or sunshine laws, which vary widely. It would make little sense to protect the information federally but leave it subject to disclosure under State FOIA laws once shared with States.

Antitrust Issues

The third of the issues raised by industry are antitrust concerns. Historically, the Justice Department has viewed requests for antitrust exemptions from the private sector as unnecessary, since they are unlikely to violate the antitrust laws. However, an exemption with respect to critical infrastructure protection is being discussed within the Administration.

Conclusion

Mr. Chairman, I want to thank you again for this opportunity to testify about our efforts to protect critical infrastructure. Citizens are deeply concerned about their safety and security of our country. By addressing information sharing, Congress will enhance the ability of law enforcement to fight cybercrime, terrorism, and protect our infrastructure. The Department of Justice stands ready to work with the Members of this Committee to achieve these important goals.

Mr. Chairman, that concludes my prepared statement. I would be pleased to answer any questions that you may have at this time.