Order Code RL31547

Report for Congress

Critical Infrastructure Information Disclosure and Homeland Security

Updated January 29, 2003

John D. Moteff
Specialist in Science and Technology Policy
Resources, Science and Industry Division

Gina Marie Stevens
Legislative Attorney
American Law Division

Critical Infrastructure Information Disclosure and Homeland Security

Summary

Critical infrastructures have been defined as those systems and assets so vital to the United States that the incapacity of such systems and assets would have a debilitating impact on the United States. One of the findings of the President's Commission on Critical Infrastructure Protection, established by President Clinton in 1996, was the need for the federal government and owners and operators of the nation's critical infrastructures to share information on vulnerabilities and threats. However, the Commission noted that owners and operators are reluctant to share confidential business information, and the government is reluctant to share information that might compromise intelligence sources or investigations. Among the strategies to promote information sharing was a proposal to exempt critical infrastructure information from disclosure under the Freedom of Information Act.

The Freedom of Information Act (FOIA) was passed to ensure by citizen access to government information. Nine categories of information may be exempted from disclosure. Three of the nine exemptions provide possible protection against the release of critical infrastructure information: exemption 1 (national security information); exemption 3 (information exempted by statute); and exemption 4 (confidential business information). Congress has considered several proposals to exempt critical infrastructure information from FOIA. Generally, the legislation has created an exemption 3 statute, or adopted the exemption 4 D.C. Circuit standard.

Prior to passage of the Homeland Security Act (P.L. 107-296), the House (H.R. 5005) and Senate (S. 2452) bills differed significantly on language providing a FOIA exemption. Differences included the type of information covered and exempted from FOIA; the scope of the protections provided; the authorized uses or disclosures; the permissibility of disclosures of related information by other agencies; immunity from civil liability; preemption; and criminal penalties. The Homeland Security Act (P.L. 107-296, section 214) provisions regarding the exemption of critical infrastructure information from FOIA adopted the House language in its entirety.

Public interest groups question the necessity of a FOIA exemption suggesting that existing FOIA exemptions provide sufficient protections.. They also argued that the House language (which passed) was too broad and would allow a wider range of information to be protected (including information previously available under FOIA). They favored the more limited protections proposed in the S. 2452. Public interest groups also expressed concern that the provision which bars use of the protected information in civil actions would shield owners and operators from liability under antitrust, tort, tax, civil rights, environmental, labor, consumer protection, and health and safety laws. Owners and operators of critical infrastructures insisted that current law did not provide the certainty of protection needed. While they viewed the Senate language as a workable compromise, they favored the protections in H.R. 5005. Compelling arguments existed on both sides of the debate for and against exempting critical infrastructure information from the Freedom of Information Act. S. 6 introduced in the 108th Congress, resurrects S. 2452 (107th Congress). This report will be updated as warranted.

Contents

The authors wish to thank Morton Rosenberg and Linda-Jo Schierow of the Congressional Research Service for their contributions to this report.

Critical Infrastructure Information Disclosure and Homeland Security

Introduction and Background

Leading up to the passage of the Homeland Security Act of 2002 (P.L. 107-296), a debate ensued regarding the exemption of critical infrastructure information from the Freedom of Information Act, 5 U.S.C. § 552. Both the House and Senate versions of the Homeland Security Act (H.R. 5005 and S. 2452, respectively) contained language exempting such information, but the two versions were significantly different. Final passage of the Act included the House language (sections 211 - 215 of P.L. 107-296). This report discusses the differences in language and some of the arguments and concerns expressed by both supporters and critics of the exemption.

Certain socio-economic activities are vital to the day-to-day functioning and security of the country; for example, transportation of goods and people, communications, banking and finance, and the supply of electricity and water. These activities and services have been referred to as components of the nation's critical infrastructure. Domestic security and our ability to monitor, deter, and respond to outside hostile acts also depend on some of these activities as well as other more specialized activities like intelligence gathering, law enforcement, and military forces. Serious disruption in these activities and capabilities could have a major impact on the country's well-being.

In July 1996, President Clinton established the President's Commission on Critical Infrastructure Protection (PCCIP).[1] The Commission was tasked with assessing the vulnerabilities of the country's critical infrastructures and proposing a strategy for protecting them. In its final 1997 report,[2] the Commission stated that the "...two-way sharing [of] information is indispensable to infrastructure assurance," and that "increasing the sharing of strategic information within each infrastructure, across different sectors, and between sectors and the government will greatly assist efforts of owners and operators to identify their vulnerabilities and acquire tools needed for protection." According to the Commission, the exchange of information is also necessary to develop an analytic capability to examine information about incidents, vulnerabilities, and other intelligence information to determine whether events are related and can be used possibly to recognize or predict an attack.

---

[1] Executive Order 13010—Critical Infrastructure Protection. Federal Register, July 17, 1996. Vol. 61, No. 138. pp. 37347-37350.

[2] Critical Foundations: Protecting America's Infrastructures. The Report of the President's Commission on Critical Infrastructure Protection. Washington, D.C. October, 1997.

The Commission also noted that there is a reluctance on the part of the private sector and the government to share information related to vulnerabilities or incidents needed to plan for and effect adequate protections. The private sector is reluctant to submit information to the government related to vulnerabilities or incidents that might damage its reputation, weaken its competitive position, lead to costly investigations, be used inappropriately, or expose it to liability as a result of disclosure by the government of confidential business information. The government is reluctant to disclose threat information that might compromise intelligence activities or investigations.

The first objective of the Commission's recommended Strategy for Action was to promote a partnership between government and infrastructure owners and operators that would increase the sharing of information relating to infrastructure threats, vulnerabilities, and interdependencies. The Commission proposed developing an Information Sharing and Analysis Center (ISAC) that would consist of government and private sector representatives working together to receive information from all sources, analyze it, draw conclusions about vulnerabilities or incidents within the infrastructures, and inform government and private sector users. It also recognized that, in order to facilitate the exchange of information, the private sector would need assurances that its confidential information would be protected. The Commission noted that this might require that a legal vehicle be established within the critical infrastructure information sharing mechanism that would protect confidential information, and examined the ramifications of different approaches and strategies related to the federal government's protection of private sector information. It briefly discussed some pros and cons associated with the creation of a FOIA exemption 3 statute for critical infrastructure information. Under exemption 3 of the Freedom of Information Act (FOIA), 5 U.S.C. 552, information protected from disclosure under other statutes is also exempt from public disclosure under FOIA.[3]

In response to the Commission's report, President Clinton released Presidential Decision Directive No. 63 (PDD-63).[4] The Directive instructed the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism and other government officials to consult with private sector owners and operators of critical infrastructures, and encourage the creation of a private sector information analysis and sharing center as envisaged by the PCCIP. Although the Directive did not address FOIA explicitly, it did direct the National Coordinator to undertake studies to examine: liability issues arising from participation by private sector companies in the information sharing process; existing legislative impediments to information sharing with an eye toward removing those impediments; and the improved protection, including secure dissemination of industry trade secrets, of other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing

---

[3] Exemption 3 exempts from disclosure information specifically exempted by statute, as long as the statute leaves no discretion on disclosure and that the statute specifies particular criteria for withholding or refers to particular types of matters to be withheld. 5 U.S.C. § 552(b)(3). See the next section of this report for further discussion.

[4] The White House, Protecting America's Critical Infrastructures: Presidential Decision Directive 63 (May 1998). Available at [http://www.ciao.gov/resource/paper598.pdf].

vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, would be imprudent to disclose. The Clinton Administration, however, never adopted a formal position on the desirability of an exemption to FOIA or the necessity for any additional confidentiality protections.

In connection with the implementation of PDD-63, a number of industrial sectors which own and/or operate critical infrastructures formed ISACs, and entered into arrangements with the federal government to share information. However, the General Accounting Office reported in April 2001, that very little or no formalized flow of information has occurred from the private sector to the federal government.[5] According to the Director of the National Infrastructure Protection Center, the organization with which industry is to share information, one of the reasons for this is the uncertainty regarding FOIA exemptions.[6] Similarly, the Partnership for Critical Infrastructure Security, a cross-industry group formed to facilitate communication among industry sectors, has stated that it is not clear that any of the existing FOIA exemptions provide the certainty of protection that many companies require before disclosing threat and vulnerability information to the government.[7]

In the 106th Congress, both H.R. 4246 (Davis/Moran) and S. 3188 (Kyl) included an exemption from FOIA for cyber security information voluntarily provided to the federal government, and prohibited the information from being used, by either the federal government or a third party, in any civil action.[8] Neither bill was reported out of committee.

During the 107th Congress, two bills were introduced with many of the same provisions: H.R. 2435 (Davis) and S. 1456 (Bennett/Kyl) would have exempted information voluntarily submitted to the federal government in connection with critical infrastructure protection from FOIA,[9] and provided protection against civil action. Both bills remained in committee. In an effort to reconcile the two bills, S. 1456 was modified, taking some of the House language. The rewritten bill, however, was never introduced. The Bush Administration offered qualified support for both

---

[5] *Critical Infrastructure Protection. Significant Challenges in Developing National Capabilities.* United States General Accounting Office. GAO-01-323. April 2001. See Chapter 4.

[6] Id. Appendix 1, p.99. It should be noted that, according to the GAO, another reason the private sector has not shared information with the government is the lack of agreement on what type of information is needed.

[7] Partnership for Critical Infrastructure Protection. Working Group 3. Public Policy White Paper. p. 5. Available at [http://www.pcis.org/WG3/WG-3_Public_Policy_WP.pdf].

[8] See CRS Report RL30153, *Critical Infrastructures: Background and Early Implementation of PDD-63*.

[9] The Senate bill expanded the type of information to be protected to include information related to the physical security of critical infrastructures, referring to protected information as "critical infrastructure information," specified the agencies covered by the legislation, and prescribed how the information may be used.

bills.[10] In President Bush's initial proposal to establish a new Department of Homeland Security, part of which proposed establishing a critical infrastructure protection function, a FOIA exemption was included for information held by the Department. Subsequently, both the House and Senate bills establishing the new Department (H.R. 5005 and S. 2452, respectively) included more detailed language exempting critical infrastructure information from FOIA. The House language also offered more extensive protections: see Legislative Responses, below.

Freedom of Information Act

In 1966, during floor debate on passage of the Freedom of Information Act (FOIA),[11] Representative Rumsfeld quoted James Madison when he said,

> Knowledge will forever govern ignorance. And a people who mean to be their own governors, must arm themselves with the power knowledge gives. A popular government without popular information or the means of acquiring it, is but a prologue to a farce or a tragedy, or perhaps both.[12]

The sentiments expressed by Madison in 1822 are prescient today. The populace desires knowledge about the activities of its government in order to ensure accountability and oversight. The government desires information from owners and operators of critical infrastructures in order to protect persons and assets in the war on terrorism. The terrorist attacks of September 11 have prompted a reevaluation of how to balance public access to information with the need for safety and security.

The federal government, since its beginnings, has delegated to agency heads the basic authority to control the papers and documents of their departments. Through the Housekeeping Statute of 1789, federal agencies have kept control of the disclosure of their files.[13] The Administrative Procedure Act (APA) of 1946 had a slight impact upon departmental control of agency information.[14] Instances were documented, however, where both the Housekeeping Statute and the Administrative Procedure Act had been used as excuses for withholding information, and concern mounted that the APA had become a loophole for agency secrecy permitting agency heads to exercise broad, unrestrained powers of a discretionary nature. The Housekeeping Statute was amended to clarify that it does not authorize withholding

---

[10] White House Official Outlines Cyber Security Initiatives. Maureen Sirhal. National Journal's Technology Daily. January 25, 2002.

[11] 5 U.S.C. § 552 *et seq.*

[12] James Madison, 1822, quoted by Rep. Rumsfeld in House debate on passage of Freedom of Information Act, 114 Cong. Rec. 13, 654 (1966).

[13] "The head of an Executive department or military department may prescribe regulations for the government of his department, the conduct of its employees, the distribution and performance of its business, and the custody, use, and preservation of its records, papers, and property. This section does not authorize withholding information from the public or limiting the availability of records to the public." 5 U.S.C. § 301.

[14] 60 Stat. 238.

information from the public or limiting the availability of records to the public. The amendment of the Housekeeping Statute did not produce the results sought by advocates of greater public access to public information. The House Government Information Subcommittee proposed a freedom of information bill that created a right of any person to use the courts to enforce the right of access to federal information. Although the proposal was well received by the press, federal agencies were resistant. The Senate passed S. 1160 in 1965, the House in 1966, and the Freedom of Information Act (FOIA) was signed into law by President Johnson on July 4, 1966. The FOIA was subsequently amended in 1974, 1986, and 1996 for several reasons: ambiguity in the text and legislative history; agency and Department of Justice resistance to broader disclosure; increased oversight by Congress; court interpretations of the statute and its procedural requirements and exemptions; time delays by agencies in responding to requests for access to information and delaying tactics by agencies in litigation; to clarify the scope of the exemptions in response to Supreme Court decisions interpreting the Act's provisions; and to accommodate technological advances related to the methods prescribed for public access.

The purpose of the Freedom of Information Act (FOIA) was to ensure by statute citizen access to government information. The FOIA establishes for any person—corporate or individual, regardless of nationality—presumptive access to existing, unpublished agency records on any topic. The law specifies nine categories of information that may be exempted from the rule of disclosure. The exemptions permit, rather than require, the withholding of the requested information. Records which are not exempt under one or more of the Act's nine exemptions must be made available. If a record has some exempt material, the Act provides that any reasonably segregable portion of the record must be provided to any person requesting such record after deletion of the portions which are exempt. Disputes over the accessibility of requested records may be reviewed in federal court. Fees for search, review, or copying of materials may be imposed; also, for some types of requesters, fees may be reduced or waived. The FOIA was amended in 1996 to provide for public access to information in an electronic form or format. In 2001, agency annual reports indicated that they received approximately 1.9 million FOIA requests.

With respect to the Freedom of Information Act, three of the nine exemptions from public disclosure provide possible protections against the release of homeland security and critical infrastructure information: exemption 1 (national security information), exemption 3 (information exempted by statute), and exemption 4 (confidential business information).[15]

FOIA Exemption 1 – National Security Information

Exemption 1 of the FOIA protects from disclosure national security information concerning the national defense or foreign policy, provided that it has been properly classified in accordance with the substantive and procedural requirements of an executive order.[16] As of October 14, 1995, the executive order in effect is Executive

---

[15] See 5 U.S.C. § 552(b).

[16] 5 U.S.C. § 552(b)(1).

Order 12,958 issued by President Clinton (and amended in 1999 by Executive Order 13,142).[17] Section 1.5 of the order specifies the types of information that may be considered for classification: military plans, weapons systems, or operations; foreign government information; intelligence activities, sources or methods, or cryptology; foreign relations or foreign activities, including confidential sources; scientific, technological, or economic matters relating to national security; U.S. government programs for safeguarding nuclear materials and facilities; or vulnerabilities or capabilities of systems, installations, projects, or plans relating to national security. The categories of information that may be classified seemingly appear broad enough to include homeland security information concerning critical infrastructures. Under E.O. 12,958 information may not be classified unless "its disclosure reasonably could be expected to cause damage to the national security."[18]

On March 19, 2002, the White House Chief of Staff issued a directive to the heads of all federal agencies addressing the need to protect information concerning weapons of mass destruction and other sensitive homeland security-related information.[19] The implementing guidance for the directive concerns sensitive homeland security information that is currently classified, and previously unclassified or declassified information.[20] The guidance provides that with respect to such information currently classified, the classified status of such information should be maintained in accordance with Executive Order 12,958. This includes extending the duration of classification as well as exempting such information from automatic declassification as appropriate. With respect to previously unclassified or declassified information concerning weapons of mass destruction and other sensitive homeland security-related information, the implementing guidance provides that, to the extent it has never been publicly disclosed under proper authority, it may be classified or reclassified pursuant to Executive Order 12,958. If the information has been subject to a previous request for access, such as a FOIA request, classification or reclassification is subject to the special requirements of the executive order.

Section 792 of H.R. 5005, as passed by the House, directed the President to prescribe and implement procedures applicable to all federal agencies to share relevant, appropriate homeland security information among federal agencies, including the Department of Homeland Security, and with appropriate state and local personnel; to identify and safeguard sensitive, unclassified homeland security information; to determine whether, how, and to what extent to remove classified homeland security information, and to determine with whom such homeland security information should be shared after such classified information is removed. H.R.

---

[17] 3 C.F.R. 333 (1996), *reprinted in* 50 U.S.C. § 435 note.

[18] Exec. Order No. 12.958, § 1.2(a)(4).

[19] *See* White House Memorandum for Heads of Executive Departments and Agencies Concerning Safeguarding Information Regarding Weapons of Mass Destruction and Other Sensitive Documents Related to Homeland Security (Mar. 19, 2002); reprinted in *FOIA Post* (posted 3/21/02).

[20] *See* Memorandum from Acting Director of Information Security Oversight Office and Co-Directors of Office of Information and Privacy to Departments and Agencies (March 31, 2002); reprinted in *FOIA Post* (posted 3/21/02).

5005 specifically stated that the substantive requirements for classification are not changed. S. 2452, agreed to by the Senate Governmental Affairs Committee on July 25, 2002, did not have a parallel provision. The House language prevailed (in Section 982 of P.L. 107-296).

FOIA Exemption 3 – Information Exempt by Statute

Under exemption 3 of the FOIA, information protected from disclosure under other statutes is also exempt from public disclosure.[21] Exemption 3 provides that the FOIA does not apply to matters that are:

> specifically exempted from disclosure by statute . . . provided that such statute (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld.[22]

Exemption 3 allows the withholding of information prohibited from disclosure by another statute only if the other statute meets any one of the three criteria: (1) it requires that the records be withheld (*i.e.*, no agency discretion); (2) grants discretion on whether to withhold but provides specific criteria to guide the exercise of that discretion; or (3) describes with sufficient specificity the types of records to be withheld. To support an exemption 3 claim, the information requested must fit within a category of information that the statute authorizes to be withheld. As with all FOIA exemptions, the government bears the burden of proving that requested records are properly withheld. Numerous statutes have been held to qualify as exemption 3 statutes under the exemption's first subpart – statutes that require information to be withheld and leave the agency no discretion. Several statutes have failed to qualify under exemption 3 because too much discretion was vested in the agency, or because the statute lacked specificity regarding the records to be withheld.[23] Unlike other FOIA exemptions, if the information requested under FOIA meets the withholding criteria of exemption 3, the information must be withheld.

Congress has considered a number of proposals that address the disclosure under FOIA of cyber security information, of information maintained by the Department of Homeland Security, and of critical infrastructure information voluntarily submitted to the Department of Homeland Security. Generally, the legislation has specifically exempted the covered information from disclosure under FOIA, in effect creating an exemption 3 statute for purposes of FOIA.

---

[21] 5 U.S.C. § 552(b)(3).

[22] 5 U.S.C. § 552(b)(3).

[23] See CRS Congressional Distribution Memorandum, American Law Division, Freedom of Information Act: Statutes Invoked under Exemption 3 by Gina Stevens (July 11, 2002)

FOIA Exemption 4 – Confidential Business Information

Exemption 4 of FOIA exempts from disclosure "trade secrets and commercial or financial information obtained from a person and privileged or confidential."[24] The latter category of information (commercial information that is privileged or confidential) is relevant to the issue of the federal government's protection of private sector critical infrastructures information. To fall within this second category of exemption 4, the information must satisfy three criteria. It must be: a) commercial or financial; b) obtained from a person; and c) confidential or privileged. The D.C. Circuit has held that the terms "commercial or financial" should be given their ordinary meaning, and that records are commercial if the submitter has a "commercial interest" in them.[25] The second criteria, "obtained from a person," refers to a wide range of entities.[26] However, information generated by the federal government is not "obtained from a person," and as a result is excluded from exemption 4's coverage.[27]

Most exemption 4 cases have involved a dispute over whether the information was "confidential." In 1974, the D.C. Circuit in *National Parks and Conservation Association v. Morton*, held that the test for confidentiality was an objective one.[28] It held that neither the fact that a submitter would not customarily make the information public, nor an agency's promises of confidentiality were enough to justify confidentiality. *National Parks* enunciated a two-part test: commercial information is confidential "if disclosure of the information is likely to have either of the following effects: (1) to impair the government's ability to obtain necessary information in the future; or (2) to cause substantial harm to the competitive position of the person from whom the information was obtained."[29] These criteria are commonly referred to as Test 1 and Test 2.[30]

In 1992, in *Critical Mass Energy Project v. NRC*,[31] after examining arguments in favor of overturning *National Parks,* the D.C. Circuit reaffirmed application of the *National Parks* test based on the principle of *stare decisis* – which counsels against overruling established precedent. The plaintiff was seeking reports which a utility

---

[24] 5 U.S.C. § 552(b)(4).

[25] *Public Citizen Health Research Group v. FDA*, 704 F.2d 1280, 1290 (D.C. Cir. 1983).

[26] *See, Nadler v. FDIC*, 92 F.3d 93, 95 (2d Cir. 1996)(term "person" includes "individual, partnership, corporation, association, or public or private organization other than an agency" (quoting definition found in Administrative Procedure Act, 5 U.S.C. § 551(2)).

[27] *See, Allnet Communications Servs. v. FCC*, 800 F. Supp. 984, 988 (D.D.C. 1992).

[28] 498 F.2d 765 (D.C. Cir. 1974).

[29] *Id.* at 770.

[30] *See also, Niagara Power Corp. v. United States Department of Energy*, 169 F.3d 16 (D.C. Cir. 1999)(court held that material fact existed as to whether disclosure of fuel consumption and power generation figures provided pursuant to statute would impair agency's ability to collect information, and whether disclosure was likely to cause plants substantial harm).

[31] 975 F.2d 871, 879-80 (D.C. Cir. 1992)(*en banc*)("*Critical Mass II*"), *cert. denied*, 113 S. Ct. 1579 (1993).

industry group prepared and gave voluntarily to the NRC. The agency did, however, have the authority to compel submission. The full Circuit Court of Appeals clarified the scope and application of the *National Parks* test. The court limited its application "to the category of cases to which [they were] first applied; namely those in which a FOIA request is made for commercial or financial information a person was obliged to furnish to the Government."[32] The court established a new test for confidentiality when the information is submitted voluntarily;[33] the information is exempt from disclosure if the submitter can show that it does not customarily release the information to the public.[34] Under the *Critical Mass* decision, one standard (the traditional *National Parks* tests) applies to any information that a submitter "is required to supply," while a broader exemption 4 standard (a new "customary treatment" test) applies to any information that is submitted to an agency on a voluntary basis. The burden of establishing the submitter's custom remains with the agency seeking to withhold the records. Applying the customary treatment test to the information at issue (utility industry group reports voluntarily submitted), the D.C. Circuit agreed with the district court's conclusion that the reports were commercial; that they were provided to the agency on a voluntary basis; and that the submitter did not customarily release them to the public. Thus, the reports were found to be confidential and exempt from disclosure under exemption 4.

The key issue raised by *Critical Mass* is the distinction between "required" and "voluntary" information submissions. In its decision, the court did not expressly define the two terms. The Department of Justice has issued policy guidance on the distinction between information required and information voluntarily submitted under *Critical Mass*, and has taken the position that the submission of records in instances such as the bidding on government contracts is mandatory rather than voluntary.[35] The basic principles developed by the Justice Department are that a submitter's voluntary participation in an activity does not determine whether any information submission made in connection with that activity is "voluntary;" that *Critical Mass* determinations should be made according to the circumstances of information submission; that information submissions can be "required" by a range of legal authorities, including informal mandates that call for the submission of information as a condition of dealing with the government or of obtaining a government benefit; and that the existence of agency authority to require an information submission does not automatically mean that the submission is "required."[36] The decision in *Critical Mass* has generated a great deal of commentary.[37] In addition, there are many cases where courts have applied the

---

[32] *Id.* at 880.

[33] With respect to critical infrastructure information, the federal government seeks to ensure that it is able to obtain the information from the private sector on a voluntary basis.

[34] *Id.* at 879.

[35] *See FOIA Update*, Vol. XIV, No. 2, at 3-5 ("OIP Guidance: The Critical Mass Distinction Under Exemption 4").

[36] *Id.*

[37] *See, e.g.,* Rocco J. Maffei, *The Impact of FOIA after Critical Mass*, 22 Pub. Cont. L. J. (continued...)

Critical Mass distinction between voluntary and required submissions.[38] Nonetheless, the *Critical Mass* voluntary vs. required standard has not been widely adopted by the other circuits that have endorsed the *National Parks* test.

Executive Order 12,600 (*Predisclosure Notification Procedures for Confidential Commercial Information*), issued in 1987, requires each federal agency to establish procedures to notify submitters of confidential commercial information whenever an agency "determines that it may be required to disclose" such information under the FOIA.[39] The submitter is provided an opportunity to submit objections to the proposed disclosure.[40] If the agency decides to release the information over the objections of the submitter, the submitter may seek judicial review of the propriety of the release, and the courts will entertain a "reverse FOIA" suit to consider the confidentiality rights of the submitter.[41]

Another area of concern under exemption 4 jurisprudence is the so-called mosaic effect which recognizes that an individual piece of information, which in and of itself may not qualify as confidential business information, may be combined with other information to cause substantial competitive harm. Private information hawkers routinely engage in the business of assembling all of the pieces of information. Courts have applied the mosaic effect to prevent the disclosure of confidential business information.[42]

As previously noted with regard to critical infrastructure information, the federal government seeks to ensure that it is able to obtain information from the private sector on a voluntary basis. S. 2452, the Senate version of National Homeland Security and Combating Terrorism Act of 2002, would have essentially codified the

---

[37] (...continued)
757 (1993); G. Branch Taylor, *The Critical Mass Decision: A Dangerous Blow to Exemption 4 Litigation*, 2 CommLaw Conspectus 133 (1994).

[38] *See, e.g.., Lykes v. Bros. S.S. v. Pena*, No. 92-2780, slip op. at 8-11 (D.D.C. Sept. 2, 1993)("under *Critical Mass*, submissions that are required to realize the benefits of a voluntary program are to be considered mandatory"); *Lee v. FDIC*, 923 F. Supp. 451, 454 (S.D.N.Y. 1996)(when documents were "required to be submitted" in order to get government approval to merge two banks, court rejects agency's attempt to nonetheless characterize submission as "voluntary"); *AGS Computers, Inc. v. United States Dep't of Treasury*, No. 92-2714, slip op. at 10 (D.N.J. Sept. 16, 1993)(submitter's submission of documents to agency during a meeting was done voluntarily because there was no "controlling statute, regulation, or written order"); *Center for Auto Safety v. National Highway Traffic Safety Admin.*, 93 F. Supp.2d 1 (D.D.C. Feb. 28, 2000), *remanded by Center for Auto Safety v. National Highway Traffic Safety Admin.*, 244 F.3d 144 (D.C.Cir. Mar. 30, 2001)(information on airbag systems submitted in response to agency's request was a voluntary submission because agency lacked legal authority to enforce its request for information).

[39] 3 C.F.R. 235 (1988), *reprinted in* 5 U.S.C. § 552 note.

[40] Exec. Order No. 12,600, § 4.

[41] *Lee v. FDIC*, 923 F. Supp. 451, 455 (S.D.N.Y. 1996).

[42] See, e.g., *Tinken Co. v. U.S. Customs Serive*, 491 F. Supp. 557 (D.D.C. 1980).

voluntary/required rule from the D.C. Circuit's decision in *Critical Mass v. NRC*, and applies it to critical infrastructure information voluntarily submitted by the private sector, and not customarily available to the public, to the new Department of Homeland Security. Codification of the *Critical Mass* standard could eliminate differences in treatment in the federal courts of confidential business information related to critical infrastructure.

Legislative Responses

FOIA Exemption in the Administration's Initial Proposal for Homeland Security

The Bush Administration's initial legislative proposal establishing the new Department of Homeland Security proposed to exempt from disclosure under FOIA critical infrastructure information voluntarily submitted to the government by non-federal entities. Section 204 of the proposal stated:

> Information provided voluntarily by non-federal entities or individuals that relates to infrastructure vulnerabilities or other vulnerabilities to terrorism and is or has been in the possession of the Department [of Homeland Security] shall not be subject to section 552 of title 5, United States Code.

This proposed language did not provide additional specificity, and was criticized by the FOIA requester community as "cast[ing] a shroud of secrecy over one of the Department of Homeland Security's critical functions, critical infrastructure protection."[43]

FOIA Exemptions in Homeland Security Proposals

When the President's legislative proposal was reported out of the House Select Committee on Homeland Security as H.R. 5005 (Armey), the Administration's FOIA exemption was modified and included in a separate subtitle (Title VII, Subtitle C, sections 721 - 724).[44] The Senate Government Affairs Committee, too, voted to add a FOIA exemption to its bill S. 2452 (Lieberman, section 198) establishing a Department of Homeland Security. The House language prevailed as Title II, Subtitle B, Section 214, in P.L 107-296. A brief discussion of the FOIA exemptions in these two homeland security bills follows. A comparison of the language

---

[43] David, Sobel, Electronic Privacy Information Center, Testimony Before House Subcommittee on Oversight and Investigation on "Creating the Department of Homeland Security: Consideration of Administration's Proposal." (July 9, 2002).

[44] On the House floor, two amendments to this section of the bill were offered. Amendment No. 24 would have eliminated Subtitle C entirely. Amendment No. 25 would have amended the definition of "covered agency" to include not just the Department of Homeland Security, but any other agency designated by the Department of Homeland Security or with which the Department shares critical infrastructure information. Both amendments failed. 148 Cong. Rec. H5845 (July 26, 2002).

regarding FOIA exemptions is included in the CRS Report RL31513, *Homeland Security: Side-By-Side Comparison of H.R. 5005 and S. 2452, 107th Congress*.

P.L. 107-296, Title II, Subtitle B.

Section 214 of the Homeland Security Act of 2002 (P.L. 107-269) exempted from disclosure under FOIA "critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered agency for use by that agency regarding the security of critical infrastructure (as defined in the USA PATRIOT Act)...,[45] when accompanied by an express statement...." The Homeland Security Act defines critical infrastructure information to mean "information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

> (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the United States, or threatens public health and safety;
>
> (B) the ability of critical infrastructures or protected systems to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or,
>
> (C)any planned or past operational problem or solution regarding critical infrastructure...including repair, recovery, reconstruction, insurance, or continuity to the extent it relates to such interference, compromise, or incapacitation."[46]

A "covered agency" is defined as the Department of Homeland Security. The submission of critical infrastructure information is considered voluntary if done in the absence of the Department of Homeland Security exercising its legal authority to compel access to or submission of such information. Information submitted to the Securities and Exchange Commission pursuant to section 12 (i) of the Securities and Exchange Act of 1934 is explicitly not protected by this provision. Nor is information disclosed or written when accompanying the solicitation of an offer or a sale of securities, nor if the information is submitted or relied upon as the basis for licensing or permitting determinations, or during regulatory proceedings.

---

[45] "Systems or assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." P.L. 107-56, section 1016.

[46] P.L. 107-296, § 212(3).

Besides exempting from FOIA critical infrastructure information which has been submitted voluntarily with the appropriate express statement to the Department of Homeland Security, the Homeland Security Act also states that the information shall not be subject to any agency rules or judicial doctrine regarding *ex parte* communications with decision making officials. The Act also prohibits such information, without the written consent of the person or entity submitting such information in good faith, from being used directly by the Department of Homeland Security, any other federal, state, or local authority or any third party, in any civil action. Nor may the information, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for any purpose other than the purposes of the subtitle, except, in the furtherance of a criminal investigation or prosecution, or when disclosed to either House of Congress, or to the Comptroller General or other authorized General Accounting Office official, in the conduct of official business. Furthermore, any federal official or employee who knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any protected information, is subject to removal, imprisonment up to one year, and fines. If the information is disclosed to state or local officials, it may not be used for any purpose other than the protection of critical infrastructures, and it may not be disclosed under state disclosure laws. The protections afforded protected information do not result in waiver of any privileges or protections provided elsewhere in law. Finally, no communication of critical infrastructure information to the Department of Homeland Security shall be considered to be an action subject to the requirements of the Federal Advisory Committee Act.[47]

For information to be considered protected, it must be accompanied with a written marking to the effect that "this information is voluntarily submitted to the federal government in expectation of protection from disclosure as provided by the Critical Infrastructure Information Act of 2002 [the name given to Subtitle B]." The Secretary of the Department of Homeland Security is to establish procedures for handling the information once it is received. Only those agency components or bureaus, designated by the President or the Secretary of Homeland Security, as having a Critical Infrastructure Program may receive critical infrastructure information from the Department.

The above protections for information voluntarily submitted by a person or entity to the Department of Homeland Security do not limit or otherwise affect the ability of a state, local, or federal government entity, agency or authority, or any third party, under applicable law, to obtain critical infrastructure information (including any information lawfully and properly disclosed generally and broadly to the public) and to use that information in any manner permitted by law. Submittal to the government of information or records that are protected from disclosure is not to be construed as compliance with any requirement to submit such information to a

---

[47] The Federal Advisory Committee Act (FACA) requires that the meetings of all federal advisory committees serving executive branch entities be open to the public. The FACA specifies nine categories of information, similar to those in FOIA, that may be permissively relied upon to close advisory committee deliberations. 5 U.S.C. App. 2.

federal agency under any other provision of law. Finally, the Act does not expressly create a private right of action for enforcement of any provision of the Act.

S. 2452, Section 198 (107th Congress).

S. 2452, National Homeland Security and Combating Terrorism Act of 2002, as agreed to by the Senate Governmental Affairs Committee on July 25, 2002, exempted a "record" pertaining to the vulnerability of and threats to critical infrastructure (as defined in the USA PATRIOT Act) furnished voluntarily to the Department of Homeland Security from being made available under FOIA. A record was covered by the bill if the provider would not customarily make the record available to the public. It also required the provider to designate and certify, in a manner specified by the Department of Homeland Security, that the record is confidential and not customarily made available to the public.

Unlike the Homeland Security Act (P.L. 107-296), the Senate bill did not include a definition of "critical infrastructure information." However, the bill covered "records pertaining to the vulnerability of and threats to critical infrastructure (such as attacks, response, and recovery efforts)."

Under S. 2452 a record is submitted voluntarily if it was submitted to the Department of Homeland Security "in the absence of authority of the Department requiring that record to be submitted," and it is not submitted or used to satisfy any legal requirement or obligation or to obtain any grant, permit, benefit, or other approval from the federal government.[48]

Agencies with which the Department of Homeland Security shares protected records were to be bound by the FOIA exemption. FOIA requests for protected information were to be referred back to the Department of Homeland Security, and the Department was permitted to provide any portion of the record that is reasonably segregable from that part of the record which is exempt from disclosure, after deleting the protected information. The bill also allowed the provider of a record that is furnished voluntarily to the Department of Homeland Security to withdraw the confidential designation at any time in a manner specified by the Department.

S. 2542 allowed an agency which had received independently of the Department a record "similar or identical" to that received by the Department, to disclose the record under FOIA. The Senate bill did not preempt state or local disclosure laws if the state or local authority received the information independent of the Department of Homeland Security, nor did it contain any civil liability immunity, or criminal penalties.

The Secretary of the Department of Homeland Security was directed to prescribe procedures for: acknowledging the receipt of records furnished voluntarily; the

---

[48] Benefits include agency forbearance, loans, or reductions or modifications of agency penalties or rulings. Benefits do not include warnings, alerts, or other risk analysis offered by the Department.

certification of records furnished voluntarily as confidential and not customarily made available to the public; the care and storage of records furnished voluntarily; and the protection and maintenance of the confidentiality of records furnished voluntarily.

Finally, the Senate bill required the Comptroller General to report to Congress on the implementation and use of the above protections. The report was to include the number of persons in the private sector and the number of state and local agencies that furnished records voluntarily under these provisions, the number of requests for access granted or denied under these provisions, and any recommendations regarding improvements in the collection and analysis of sensitive information related to the vulnerabilities of and threats to critical infrastructures.

In sum, significant differences existed between H.R. 5005 (enacted into law as P.L. 107-296) and S. 2452. These differences included the scope of the information protection; the type of information covered and exempted from FOIA; the definition of a voluntary submission; the other purposes authorized for use or disclosure of the information; the disclosure of information with the consent of the submitter; the permissibility of disclosures of related information by other agencies; immunity from civil liability; preemption; and criminal penalties.

Issues and Concerns

The general concerns of the owners and operators of critical infrastructure are that the type and breadth of information they are being asked to submit on vulnerabilities, incidents, remedies, etc., if made available to competitors or to the general public, could harm their public relations, compromise their competitive position, expose them to liability, or disclose sensitive information to terrorists and others who might wish to disrupt the function of their infrastructure. It was their position that crafting a specific exemption to FOIA in statute (i.e., a (b)(3) exemption) would provide the greatest legal protections for the information they share. They believed that a narrowly tailored (b)(3) exemption would eliminate agency discretion to disclose protected information in response to a FOIA request. In addition, given the federal government's need to share sensitive business information for homeland security purposes with state and local officials, owners and operators also sought federal preemption of state and local disclosure laws. Owners and operators were concerned that some of this information could make them subject to liability in unforeseen ways.

A number of public interest groups have expressed (and continue to express) their opposition to the protections being applied, particularly those contained in the House version.[49] The primary concern is that the type of information exempted from FOIA was too broadly defined, and could allow any company claiming to be an

---

[49] Some of the groups that have expressed concern include the American Civil Liberties Union, the Electronic Privacy Information Center, Natural Resources Defense Fund, the Society of Professional Journalists, and the U.S. Public Interest Research Group. For a sample of the groups that have joined in opposition and their rationales, see [http://www.ombwatch.org/article/articleview/943/1/18/cleanwateraction.org].

owner or operator of a critical infrastructure to voluntarily submit almost any kind of information in order to protect the information from disclosure under the FOIA. Critics also believe the definition of critical infrastructure adopted from the USA PATRIOT Act is too broad.

The Act also covers information regarding an attack, or similar conduct, that violates law or harms interstate commerce. According to one critique, the language "or similar conduct" and "harms interstate commerce" is broad and could include non-criminal or inadvertent incidents that cause temporary interruption of normal business operations.[50] The criticism goes on to state that the purposes for which the information may be used (and therefore contributing to the definition of what kind of information may be protected) includes analysis, warning, interdependency study, recovery, reconstitution, or "other informational purposes." According to the critique, "other informational purposes" covers untold amounts of information, some of which may have been previously available to the public.

These groups also are concerned that information currently collected by various agencies and available to the public could now be protected from disclosure if submitted to the Department of Homeland Security initially as critical infrastructure information. This is particularly an issue in the area of environmental law relating to a community's right to know.[51] Both bills stated that the protections are granted "notwithstanding any other provisions of law." Under current law (the Emergency Planning and Community Right-to-Know Act, P.L. 99-499, 42 USC 11001-11050), facilities handling certain toxic substances in excess of a threshold amount annually must report to the Environmental Protection Agency and local officials the maximum and average daily amounts of such substances that they had on hand during the previous year; the location of such chemicals within the facility; and estimates of how much was released into the environment as part of normal handling and processing. In addition, in the event of an accidental release above a threshold amount, facilities immediately must report the amount released to local officials.

The 1990 amendments to the Clean Air Act (which were passed in P.L. 101-549, Section 301, amending 42 USC 7412) made it the duty of owners and operators of facilities producing, processing, handling, or storing certain extremely hazardous substances: to identify hazards that may result from releases; to design and maintain a safe facility; and to minimize the consequences of accidental releases which do occur. To prevent accidental releases, the Clean Air Act requires facilities handling such substances to develop "risk management plans." Among the items included in these plans are an accounting of any accidental releases of those substances over the previous five years; estimates of the quantities of chemicals that might be released in the event of an accident, including a worst-case accident; estimates of the potential exposures to affected downwind populations; a program for preventing releases; and an emergency response program to protect public health and the environment in the

---

[50] Problems with S. 1456, Critical Infrastructure Information Act. National Resources Defense Council. Although directed at the rewritten version of S. 1456 that was never introduced, the language at issue is the same as that proposed in H.R. 5005. The critique can be found at [http://www.ombwatch.org/info/cii/nrdcproblems.html].

[51] See CRS Report RL31530, *Chemical Plant Security* by Linda-Jo Schierow.

event of a release. Under the 1990 law, public disclosure of most of this information (which also could be released in response to FOIA requests) is required, but the details of the off-site consequence analyses (OCA) for hypothetical accidents are not required to be disclosed. In addition, companies may claim confidentiality for some submitted information, provided they can support that claim.

Security concerns arose about the potential utility to terrorists of risk management planning data, just as EPA was planning to make the plans widely available to the public via the Internet.[52] Convinced of the need for caution, EPA agreed not to post OCA data on its website. Nevertheless, the information could be obtained electronically using FOIA, and several public interest groups announced that they would do so and post the data. In 1999, Congress responded by again amending the Clean Air Act. The amended Act exempts OCA data from disclosure under FOIA, and directs EPA to limit public disclosure as necessary to reduce risks. EPA issued a final regulation on data access on August 4, 2000.[53] It allows the public to see paper copies of sensitive OCA information through federal reading rooms, approximately one per state, and provides Internet access to the OCA data elements that pose the least serious criminal risk. State and local agencies are encouraged to provide the public with read-only access to OCA information on local facilities. At the federal reading rooms, members of the public may read OCA information for up to 10 facilities per calendar month and for all facilities with potential effects in the jurisdiction of the local emergency planning committee. State and local officials and other members of the public may share OCA information as long as the data are not conveyed in the format of sensitive portions of the RMP or any electronic database developed by EPA from those sections.[54] A Clinton Administration proposal to implement the final rule (66 *Federal Register* 4021, Jan. 17, 2001) would have allowed people to view plans of facilities outside their local area and enhanced access for "qualified researchers." The draft plan was rescinded by the Bush Administration (66 *Federal Register* 15254, Mar. 16, 2001). No further regulatory action has been taken to date.

Critics of the FOIA exemption for critical infrastructure information submitted voluntarily with the appropriate express statement are concerned that the "notwithstanding any other provision of law" clause could possibly exempt from FOIA information about facilities handling potentially dangerous chemicals that is currently available under the Emergency Planning and Community Right-to-Know Act and the Clean Air Act.

Some public interest groups are concerned that the breadth of information that could be exempted from disclosure, combined with the prohibition on use of critical

---

[52] During the mid to late 1990s, federal agencies were facilitating electronic public access to governmental information in response to congressional directives, such as the Electronic Freedom of Information Act, P.L.104-231, and presidential initiatives, such as "President Clinton's Environmental Monitoring for Public Access and Community Tracking" program.

[53] 65 *Federal Register* 48107-48133.

[54] EPA Fact Sheet. "Chemical Safety Information, Site Security and Fuels Regulatory Relief Act: Public Distribution of Off-Site Consequence Analysis Information." EPA 550-F00-012, Aug. 2000.

infrastructure information in any civil suit, could give owners or operators of critical infrastructures an "unprecedented immunity" from complying with a variety of laws (i.e., antitrust, tort, tax, civil rights, environmental, labor, consumer protection, and health and safety laws). Another concern centers on a perceived lack of clarity on whether information obtained independently by subpoena, for example, could be used to bring civil suit (e.g., would a victim of chemical exposure be precluded from suing if information previously submitted to the Department of Homeland Security was obtained independently from the company by subpoena).

Another argument made by the public interest groups is that existing FOIA exemptions and case law offer sufficient protections to owner/operators. They cite exemption (b)(4), which allows agencies to withhold commercial information that is privileged or confidential, if by disclosing that information, the competitive position of the provider is harmed or the ability of the government to continue receiving that information is impaired. An exemption from FOIA for critical infrastructure information, they argue, would promote government secrecy and harm public access.

These groups are also concerned about a provision they say gives the private sector the power to determine what information is to be protected, simply by including an express statement of protection from disclosure on the submission to the federal government. The criminal penalties provided for the unauthorized disclosure of protected information are viewed by some groups as essentially an anti-whistleblower provision designed to stifle government accountability. Another issue raised by the groups is whether a submission of information to the government will be treated as voluntary in situations where an agency has not exercised its authority to compel submission. Finally, the groups take issue with the provision that preempts state and local freedom of information laws.

The public interest groups concerned with granting specific FOIA exemptions have expressed a guarded acceptance of the Senate version. They feel it basically puts into statute recent FOIA case law regarding the protections afforded confidential information submitted to government agencies under FOIA exemption 4.[55]

Representatives from industry responded to some of these concerns by stating that it was not their intent to evade current laws and regulations, but that the extra protections are needed before they are willing to voluntarily submit information that might be used against them later, either legally or competitively. Under the existing law, companies had no assurance that information they share with a government agency will be treated confidentially, and agencies are not required to commit to confidentiality at the time of disclosure. Agencies are not required to initiate the FOIA exemption process until a FOIA request is received. When it is received, the agency is asked to defend the information's confidentiality, and is not required to inform the originator if it believes it has enough information to proceed. Industry is generally in favor of legislation that accomplishes the goal of encouraging it to submit security-related information without fear of public disclosure.

---

[55] Industry Offers Support for Scaled-Back Senate FOIA Revisions, Inside EPA (July 26, 2002).

Representatives from owners and operators have also stated that they favor a narrow exemption so as to cover only infrastructure threat and vulnerability information.[56]

Conclusion

Compelling arguments existed on both sides of the debate for and against exempting critical infrastructure information from the Freedom of Information Act. However, the Senate bill, S. 2452, never made it to the Senate floor. After the November 2002 election, sentiment to pass a Homeland Security Act led to the adoption by the Senate of large portions of the House-passed bill. The provisions regarding the exemption of Critical Infrastructure Information from FOIA adopted the House language in total. Public interest groups continue to criticize the language. S. 6 introduced January 7, 2003, in the 108th Congress, and sent to the Senate Judiciary Committee, resurrects S. 2452 (107th Congress) language (Title VIII, Subtitle B).

[56] Kenneth C. Watson, President Partnership for Critical Infrastructure Security, Testimony Before House Subcommittee on Oversight and Investigation on "Creating the Department of Homeland Security: Consideration of Administration's Proposal." (July 9, 2002).