NARROW LANES AHEAD?: AN EXAMINATION OF PUBLIC ACCESS TO INFORMATION REGARDING THE TRANSPORTATION OF HAZARDOUS MATERIALS IN A POST-9/11 WORLD

*Amy Kristin Sanders, J.D.**

TABLE OF CONTENTS

INTRODUCTION 126
I. THE EXECUTIVE BRANCH, FOIA, AND ACCESS TO FEDERAL GOVERNMENT INFORMATION 129
A. The Department of Transportation and FOIA 131
II. PRE-9/11 INFORMATION ACCESS 133
A. Exemption One and National Security Information 134
B. Exemption Four and Confidential Business Information 136
C. Exemption Three and Statutory Protections 137
D. Administrative Policy 137
III. POST-9/11 INFORMATION ACCESS 138
A. Exemption Three and the Critical Infrastructure Information Act 140
B. The Scope of Protection Under the Critical Infrastructure Information Act 144
C. Limits on Critical Infrastructure Protection 145
D. DHS Procedures for Handling Critical Infrastructure Information 146
CONCLUSION 147

INTRODUCTION

More than 800,000 hazardous material ("HazMat") shipments traverse the United States each day via trucks, trains, and airplanes, making their way on our roads, through our neighborhoods and over our homes.[1] These shipments range from low-level hazards such as fireworks and other explosives to highly sensitive cargoes including Anthrax and other pathogens.[2] Regardless of their method of transport, these hazardous material shipments must comply with federal transportation laws and regulations.[3] Promulgated by Congress and the Department of Transportation (DOT) under the advisement of the DOT's Research and Special Programs Administration, these laws and regulations cover when, how, and where hazardous materials may be handled and transported.[4] In addition, these provisions establish licensing procedures and record-keeping practices for HazMat producers and carriers.[5]

Like other federal agency information, the documents and records kept by the DOT have historically been subject to the federal Freedom of Information Act (FOIA).[6] However, since the September 11, 2001 terrorist attacks[7], the

---

* Amy Kristin Sanders, J.D., is a Ph.D. student in the College of Communication and Journalism at the University of Florida.

[1] Jim Mitchell, *Transportation Secretary Mineta Proposes Stronger Hazardous Materials Legislation To Improve Security and Safety*, (October 10, 2001), *available at* http://www.dot.gov/affairs/rspa2701.htm.

[2] 49 C.F.R. § 172.101 app. A, tbl. 1 (2004).

[3] 49 U.S.C. § 5103(b) (2004).

> The Secretary shall prescribe regulations for the safe transportation, including security, of hazardous material in intrastate, interstate, and foreign commerce. The regulations: 1) apply to a person i) transporting hazardous material in commerce; ii) causing hazardous material to be transported in commerce; or iii) manufacturing, fabricating, marking, maintaining, reconditioning, repairing, or testing a packaging or a container that is represented, marked, certified, or sold by that person as qualified for use in transporting hazardous material in commerce; and 2) shall govern safety aspects, including security, of the transportation of hazardous material the Secretary considers appropriate.

Id.

[4] 49 U.S.C. § 5103(a) (2004).

[5] 49 U.S.C. § 5103(a) (2004) (discussing procedure required for states to issue licenses as well as reporting requirements that states must follow when issuing those licenses to hazardous materials' carriers).

[6] 5 U.S.C. § 551 (2004). The Federal Freedom of Information Act mandates that certain federal records shall be open to inspection by the public unless they fall within the specific exceptions to the statute. *Id.* For the purpose of this subchapter, "agency" means each authority of the Government of the United States, whether or not it is within or subject to review by another agency. *Id.*

[7] *See generally* www.september11news.com (last visited November 21, 2005).
On September 11, 2001, terrorists hijacked four commercial airplanes, crashing two into New York City's World Trade Center and one in the Pentagon in Washington, D.C. The fourth plane crashed

George W. Bush Administration has hesitated to release information that might assist those looking to harm the United States, including these records.[8] Much of the data maintained by the DOT is gathered through licensing and inspection procedures whereby HazMat carriers submit information to obtain permission to transport hazardous goods.[9] Government officials fear terrorists may request this type of information to better plan future attacks on the nation's critical infrastructure.[10] In light of this concern, Congress acted shortly after the 2001 attacks to pass the USA PATRIOT Act, which was the first piece in the government's information-gathering plan.[11] Subsequently, Congress enacted the Homeland Security Act of 2002,[12] which contains provisions that exempt voluntarily shared critical infrastructure information submitted by the private sector to the federal government from the Freedom of Information Act.[13] This exemption has the potential to threaten the public's ability to access information regarding the transportation of hazardous materials.[14]

---

into a Pennsylvania field. *Id.*

[8] President George W. Bush, Address at the signing of the USA Patriot Act (Oct. 26, 2001). "As of today, we're changing the laws governing information-sharing. And as importantly, we're changing the culture of our various agencies that fight terrorism. Countering and investigating terrorist activity is the number one priority for both law enforcement and intelligence agencies." *Id.*

[9] 49 U.S.C. § 5103(a) (2004).

[10] President George W. Bush, Address at the signing of the USA Patriot Act (Oct. 26, 2001).

> Surveillance of communications is another essential tool to pursue and stop terrorists. The existing law was written in the era of rotary telephones. This new law that I sign today will allow surveillance of all communications used by terrorists, including e-mails, the Internet, and cell phones. ... Current statutes deal more severely with drug-traffickers than with terrorists. That changes today. We are enacting new and harsh penalties for possession of biological weapons. We're making it easier to seize the assets of groups and individuals involved in terrorism. The government will have wider latitude in deporting known terrorists and their supporters. The statute of limitations on terrorist acts will be lengthened, as will prison sentences for terrorists."

Id.

[11] U.S.A. Patriot Act, Pub. L. No. 107-296 (2001).

[12] Homeland Security Act of 2002, Pub. L. No. 107-296 (2002) (codified as amended at 6 U.S.C. §§ 131 et. seq. (2002)). The Homeland Security Act of 2002 established the Department of Homeland Security, whose major functions relate to preventing and investigating terrorist attacks on the United States. *Id.*

[13] *Id.*

[14] *See* Kristen Elizabeth Uhl, *The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection and Homeland Security*, 53 AM. U. L. REV. 261 (2003) (arguing that War on Terrorism does not justify the climate of non-disclosure that has developed in United States since September 11 terrorist attacks).

This paper explores the public's ability to access information about the transportation of hazardous materials in light of changes in law and policy since the 2001 terrorist attacks. Central to this discussion is the implementation of the Critical Infrastructure Information Act of 2002 and its potential effect on the public's ability to request information regarding HazMat transportation under federal Freedom of Information (FOI) provisions. Part I includes an examination of the Department of Homeland Security's 2004 rule-making pertaining to critical infrastructure information. Part II provides an overview of the federal FOIA, including the purpose of its enactment, its interpretations by the Executive Branch, and its application to HazMat regulation. Part I also discusses Section 214 of the Homeland Security Act of 2002,[15] commonly referred to as the Critical Infrastructure Information Act (CIIA). This discussion will place Section 214 in the larger context of the Bush Administration's attempt to protect critical infrastructure information[16] while executing a monumental information-gathering project aimed at increasing homeland security. The Administration hopes to accomplish this while controlling the release of government information to the public. Part II examines the Department of Transportation's Freedom of Information policy prior to the September 11 terrorist attacks. This section delineates the type of information made available to the public under FOIA and includes a discussion of the practical uses and applications of HazMat transportation information requested under FOIA. Part III analyzes the impact of the post-9/11 measures on the Department of Transportation's Freedom of Information policy by evaluating the amount of information available under FOIA after the enactment of these measures. In

---

[15] Homeland Security Act of 2002, Pub. L. No. 107-206 (2002) (codified as amended at 6 U.S.C. §§ 131 et. seq. (2002).

[16] 6 U.S.C. § 131 (2002). The Critical Infrastructure Information Act defines critical infrastructure information as:

> [I]nformation not customarily in the public domain and related to the security of critical infrastructure or protected systems: 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 the 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 or safety; the ability of any critical infrastructure or protected system 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 any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation.

Id.

addition, Part III contains an analysis of the type of information that may be exempted from disclosure in the future. This paper concludes with an evaluation of the public's ability to access HazMat transportation information in a post-9/11 environment. The evaluation consists of a discussion of the public policy implications of voluntary disclosure of critical infrastructure information as well as an analysis of the newly expanded FOIA exemption.

I. THE EXECUTIVE BRANCH, FOIA, AND ACCESS TO FEDERAL GOVERNMENT INFORMATION

The legal development of open government[17] in the United States has occurred through a series of legislative amendments and court decisions.[18] During the 1950s and 1960s, Congress took small steps toward providing the public with the right to access government information and records.[19] This included an amendment to the federal Housekeeping Act,[20] under which many government officials sought to keep information secret, and a 1959 attempt to narrow the scope of the Administrative Procedures Act, ("APA").[21] This attempt to narrow the APA required that agencies publish their regulations, their public information policies, and other information.[22] Shortly after these amendments, Congress passed a more comprehensive Freedom of Information Act, which President Lyndon B. Johnson signed into law on July 4, 1966. The new provision included a presumption in favor of disclosure of information, requiring that the government bear the burden of proving why information should remain confidential.[23] In 1973, Congress attempted to pass an amendment strengthening FOIA, but President Gerald Ford vetoed the

---

[17] John Adams, *A Dissertation on the Canon and Feudal Law* (1765), reprinted in 1 *Papers of John Adams* 120 (M.J. Kine ed., 1977) (explaining belief that government should operate transparently and under the supervision of public scrutiny can be traced back to writings of some of our nation's founders); Letter from James Madison to W. T. Barry (August 4, 1882), reprinted in 9 *James Madison's Writings* 103 (Gaillard Hunt ed., 1910).

[18] *See generally* HERBERT N. FOERSTEL, FREEDOM OF INFORMATION AND THE RIGHT TO KNOW: THE ORIGINS AND APPLICATIONS OF THE FREEDOM OF INFORMATION ACT 10-14 (1999) (noting that FOI movement began to take hold in early Twentieth Century when several U.S. Supreme Court justices addressed the need for an informed citizenry).

[19] *See generally* Freedom-of-Information Bill (H.R. 2767), which amended the Housekeeping Act (5 U.S.C. § 22) to include the language: "This section does not authorize withholding information from the public or limiting the availability of records to the public." *Id.* After the enactment of Pub. L. No. 89-554 in September 1966, Congress has amended FOIA numerous times. Major revisions occurred in the 1970s, including amendments in 1974, 1976 and 1978. *See* Pub. L. No. 94-409 §5(b); Pub. L. No. 95-454, tit. IX, § 906(a)(10); Pub. L. No. 98-620, tit. IV, § 402(2).

[20] The Federal Housekeeping Act was the predecessor to the Freedom of Information Act. It was codified in Chapter 5 of the United States Code.

[21] 5 U.S.C. § 1002.

[22] *See* Pub. L. No. 89-554, Sept. 6, 1966, 80 Stat. 378.

[23] 5 U.S.C. § 552(a) (2003).

legislation.[24] Congress eventually overrode the veto and the amendments took effect in February 1975.[25] This amendment added several essential elements of FOIA which continue to be valid law today.[26]

Another major revision to FOIA occurred in 1976 when Congress responded to the U.S. Supreme Court's broad interpretation of FOIA Exemption 3, which exempts information protected from disclosure by other statutes.[27] Exemption 3 allows the government to protect information from disclosure by relying on specific statutes outside the scope of the Freedom of Information Act as the source for the exemption. In *F.A.A. Administrator v. Robertson,*[28] the Federal Aviation Administration ("FFA") relied on Exemption 3 to bar disclosure of information sought by researchers studying airline safety. The reports requested were the Systems Worthiness Analysis Program ("SWAP") Reports, which include the FAA's analyses of the operation and maintenance performance of the commercial airlines.[29] The Court ruled that Exemption 3 did not contain a built-in standard for use in determining which information the government must disclose.[30] In light of the lack of a standard, the Court held that Exemption 3 did not repeal the nearly 100 statutes restricting access to government information.[31] Shortly after the decision, Congress responded by

---

[24] *See* Pub. L. No. 93-502 (1975).

[25] *Id.*

[26] *Id.* The law allowed agencies to provide documents to requesters without charge or at a reduced cost, courts to conduct in camera review of contested materials to determine whether they were properly withheld, and judges to award attorney fees and litigation costs when a complainant had "substantially prevailed" in seeking records. *Id.* Courts could take notice of 'arbitrary and capricious' withholding of documents and require an investigation to determine whether disciplinary action against agency officials was warranted; any records containing segregable portions of exempted material had to be released after necessary deletions; exemptions pertaining to classified information and law enforcement materials were narrowed. *Id.* The definition of agencies covered by the FOIA was expanded and clarified and specific response times were established for agency action on initial requests, appeals, and lawsuits. *Id.*

[27] *See* 5 U.S.C. § 552(b)(3) (2003). "This section does not apply to matters that are specifically exempted from disclosure by statute (other than section 552b of this title), provided that such statute requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or establishes particular criteria for withholding or refers to particular types of matters to be withheld." *Id.* For example, the U.S. District Court for the District of Columbia has held that the Federal Technology Transfer Act, 15 U.S.C. § 3710(a) (2003), is a qualifying Exemption 3 statute. *Public Citizen Health Research Group v. National Institutes of Health*, 209 F.Supp.2d 37 (D. D.C. 2002). The court relied on language in the statute that authorized the denial of requests for financial or confidential information pertaining to health research that had been conducted. *Id.* at 43.

[28] Administrator v. Robertson, 422 U.S. 255 (1975). In *Robertson*, the Supreme Court held that Exemption 3 was ambiguous enough to believe Congress intended federal agencies to have broad discretion in determining which statutes allowed the withholding of information under FOIA. *Id.*

[29] *Robertson*, 422 U.S. at 255.

[30] *Robertson*, 422 U.S. at 264.

[31] *Robertson*, 422 U.S. at 265.

changing the language of the exemption.[32] The new standard required that a statute specifically establish a policy for disclosure, and that the statutory exemption relied upon allow no discretion regarding disclosure.[33] Thus, the Supreme Court's decision to broadly interpret Exemption 3 led Congress to legislatively revise the statute to provide a narrower exemption.

A. The Department of Transportation and FOIA

During Fiscal Year 2003, the Department of Transportation ("DOT") received more than 10,600 FOIA requests seeking information and records that the department had maintained.[34] The DOT had compiled many of these records as part of the complex management of the national transportation system.[35] Like most of the DOT's protocols, the United State Code and the Code of Federal Regulations codified the DOT's regulations of HazMat transportation.[36] This regulatory process involves numerous federal agencies, including the Department of Transportation,[37] the Federal Aviation Administration,[38] the Environmental Protection Agency,[39] and the Occupational Safety and Health Administration.[40]

> To require this interpretation would be to ask of Congress a virtually impossible task. Such a construction would also imply that Congress had undertaken to reassess every delegation of authority to withhold information which it had made before the passage of this legislation – a task which the legislative history shows it clearly did not undertake."

Id.

[32] *See* Pub. L. No. 94-409 § 5 (1976). The new exemption reads:

> (3) [D]isclose matters specifically exempted from disclosure by statute (other than 5 U.S.C. 552), 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.

Id.

[33] *See* 5 U.S.C. § 552(b)(3) (2003).

[34] *See* 2003 DOT ANN. REP. pt. V, Sec. A, *available at* http://www.dot.gov/foia/reports/2003annualreport.html.

[35] *See, e.g.*, 49 U.S.C. §§ 5101 et. seq. (2004).

[36] *See, e.g.*, 40 C.F.R. §§172.101 et. seq. (2004).

[37] *See, e.g., id.* §§ 171.1 et. seq. (2004).

[38] *See, e.g.*, 49 U.S.C. §§ 1301 et. seq. (2004).

[39] *See, e.g.*, 40 C.F.R. §§ 263.10 et. seq. (2004).

[40] 49 C.F.R. § 171.8. One of the primary roles the Department of Transportation plays in the regulation of HazMat transportation is the establishment of a classification system for hazardous materials. *Id.*

Title 49 of the Code of Federal Regulations defines materials that the government regulates as hazardous under the auspices of the DOT.[41] These materials are then classified into taxonomies based on their relative danger.[42] To transport certain classes of hazardous materials, carriers must comply with a series of regulations. These regulations specify a range of requirements, from a maximum amount of material that may be transported to specific containers in which a material must be carried.[43] In addition, HazMat carriers must submit to inspections, licensing, and other disclosure requirements to ensure they comply with federal HazMat law.[44]

Once submitted to an agency, the government may protect this type of regulatory information from public disclosure in a number of ways. Agencies may attempt to protect it either under a FOIA exemption[45] or other established

---

[41] *Id.* The section defines hazardous materials as "[a] substance or material, including a hazardous substance, which has been determined by the Secretary of Transportation to be capable of posing an unreasonable risk to health, safety, and property when transported in commerce, and which has been so designated." *Id.*

[42] 49 U.S.C. § 5103(a) (2002).

> The Secretary of Transportation shall designate material (including an explosive, radioactive material, etiologic agent, flammable or combustible liquid or solid, poison, oxidizing or corrosive material, and compressed gas) or a group or class of material as hazardous when the Secretary decides that transporting the material in commerce in a particular amount and form may pose an unreasonable risk to health and safety or property.

Id.

[43] 49 U.S.C. § 5104 et. seq. (2002).

[44] *See* 49 U.S.C. § 5103(a) (2002) (mandating background checks for HazMat carriers and requiring states to disclose when aliens apply for HazMat carriage licenses).

[45] *See* 5 U.S.C. § 552(b) (2004). Nine FOIA exemptions are delineated in the statute. Under these exemptions, FOIA does not apply to:

> (A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order; (2) related solely to the internal personnel rules and practices of an agency; (3) specifically exempted from disclosure by statute (other than section 552b of this title) 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; (4) trade secrets and commercial or financial information obtained from a person and privileged or confidential; (5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency; (6) personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy; (7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information (A) could reasonably be expected to interfere with enforcement proceedings, (B) would deprive a person of a right to a fair trial or an impartial adjudication, (C) could reasonably be expected to constitute an unwarranted

disclosure policies and procedures. For example, the Executive Branch's policy on information disclosure, usually contained in an Executive Order and explained in subsequent memoranda, plays a role in how federal agencies comply with FOIA.[46] The Executive Branch's policy, in addition to other intra-governmental documents, provides guidance for interpreting statutes such as the FOIA. Federal court decisions interpreting FOIA also impact disclosure of information to the public.[47] Relevant judicial precedent will be analyzed throughout the article.

II. PRE-9/11 INFORMATION ACCESS

The September 11, 2001 attacks prompted Congress to enact the Homeland Security Act, which included the Critical Infrastructure Information Act. Prior to these enactments, the Department of Transportation was obligated to rely on one of the existing nine FOIA exemptions to protect any critical infrastructure information. The exemptions the DOT most frequently cited to protect critical infrastructure-type information were Exemption 1, to protect classified national security information,[48] and Exemption 4, to protect confidential business information, including trade secrets and financial information.[49] The statutory exceptions to FOIA, covered under Exemption 3, at times also applied to prevent information disclosure. The various exemptions addressing HazMat information will be discussed below.

> invasion of personal privacy, (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local, or foreign agency or authority or any private institution which furnished information on a confidential basis, and, in the case of a record or information compiled by criminal law enforcement authority in the course of a criminal investigation or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source, (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or (F) could reasonably be expected to endanger the life or physical safety of any individual; (8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or (9) geological and geophysical information and data, including maps, concerning wells."

Id.

[46] *See infra* Part III.

[47] *Id.*

[48] 5 U.S.C. § 552(b)(1) (2004). FOIA does not apply to information that is "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order." *Id.*

[49] 5 U.S.C. § 552(b)(4) (2004). FOIA does not apply to "trade secrets and commercial or financial information obtained from a person and privileged or confidential." *Id.*

A. Exemption One and National Security Information

Exemption 1 protects national security information that has been classified under Executive Order 12958 from disclosure.[50] Known as the "oldest and most well-established ground for withholding government information," Exemption 1 provides agencies with broad discretion to protect information.[51] In evaluating an agency's reliance on Exemption 1, the courts give great deference to the agency's affidavit of classification, which is used to defend the agency's basis for classification.[52]

In March 2003, President Bush amended Executive Order 12958. This amendment prevents some information from being declassified.[53] Under the Bush Administration's amendments, information classified in the past 25 years should remain classified,[54] and thus retain its protection from disclosure. In addition, classified information more than 25 years old may remain classified if this information relates to weapons of mass destruction.[55] The Executive Order also allows for the classification of previously unclassified information or re-classification of information that has been declassified.[56] The Bush

---

[50] Exec. Order No. 13,292, 68 Fed. Reg. 15,315.

[51] Scott A. Faust, *National Security Information Disclosure Under the FOIA: The Need for Effective Judicial Enforcement*, 25 B.C. L. REV. 611, 617 (1984), *quoting* 1 J. O'REILLY, FEDERAL INFORMATION DISCLOSURE 4-11 (1983).

[52] *Id.*

[53] *See* Exec. Order No. 13,292 § 1.5.

[54] *See id.* (explaining that although most information must be declassified within 10 years, Executive Order notes that classification periods can and should extend up to 25 years, particularly if it relates to weapons of mass destruction).

[55] *See* Exec. Order No. 12,958 § 3.2(b).

> It is presumed that information that continues to meet the classification requirements under this order requires continued protection. In some exceptional cases, however, the need to protect such information may be outweighed by the public interest in disclosure of the information, and in these cases the information should be declassified. When such questions arise, they shall be referred to the agency head or the senior agency official. That official will determine, as an exercise of discretion, whether the public interest in disclosure outweighs the damage to national security that might reasonably be expected from disclosure.

Id.

[56] *See* Exec. Order No. 12,958, § 1.6.

> Duration of Classification. (a) At the time of original classification, the original classification authority shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The date or event shall not exceed the time frame in paragraph (b), below. (b) If the original classification authority cannot determine an earlier specific date or event for declassification, information shall be marked for declassification 10 years from the date of the original decision, except as provided in paragraph (d), below. (c) An original classification authority may

Administration also increased the number of agencies with classification powers to include the Secretary of Health and Human Services, the Secretary of Agriculture, and the administrator of the Environmental Protection Agency ("EPA"). Finally, the Bush Administration has encouraged protection from disclosure for sensitive but non-classified information relating to national security.[57] Thus, information classified as sensitive for security purposes may also be exempted from release. The combination of these changes to the federal government's disclosure policy has the ability to drastically affect an agency's use of FOIA exemptions.

The Department of Transportation has relied on Exemption 1 to deny FOIA requests in the past. In 2000, the agency denied 28 requests based on Exemption 1.[58] Since then, utilization of Exemption 1 has decreased drastically – only five uses in the past three years.[59] This may be due in part to the fact that the EPA

> extend the duration of classification or reclassify specific information for successive periods not to exceed 10 years at a time if such action is consistent with the standards and procedures established under this order. This provision does not apply to information contained in records that are more than 25 years old and have been determined to have permanent historical value under title 44, United States Code. (d) At the time of original classification, the original classification authority may exempt from declassification within 10 years specific information, the unauthorized disclosure of which could reasonably be expected to cause damage to the national security for a period greater than that provided in paragraph (b), above, and the release of which could reasonably be expected to: (1) reveal an intelligence source, method, or activity, or a cryptologic system or activity; (2) reveal information that would assist in the development or use of weapons of mass destruction; (3) reveal information that would impair the development or use of technology within a United States weapons system; (4) reveal United States military plans, or national security emergency preparedness plans; (5) reveal foreign government information; (6) damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than that provided in paragraph (b), above; (7) impair the ability of responsible United States Government officials to protect the President, the Vice President, and other individuals for whom protection services, in the interest of national security, are authorized; or (8) violate a statute, treaty, or international agreement. (e) Information marked for an indefinite duration of classification under predecessor orders, for example, "Originating Agency's Determination Required," or information classified under predecessor orders that contains no declassification instructions shall be declassified in accordance with part 3 of this order."

Id.

[57] *See, e.g.*, Memorandum from Andrew H. Card Jr., Assistant to the President and Chief of Staff, to the Heads of the Executive Departments and Agencies (March 19, 2002), *available at* http://www.fas.org/sgp/bush/wh031902.html; Memorandum from Laura L.S. Kimberly, Acting Director of Information Security Oversight Office, to Departments and Agencies (March 19, 2002), *available at* http://www.fas.org/sgp/bush/wh031902.html.

[58] 2000 DOT ANN. REP., *available at* http://www.dot.gov/foia/2000annual_foia_report.html.

[59] *See* 2001 DOT ANN. REP., *available at* http://www.dot.gov/foia/reports/2001annualreport.html; 2002 DOT ANN. REP., *available at*

now has the power to classify documents, and the EPA handles some HazMat information requests that DOT previously handled. Because the EPA now participates in the regulation of hazardous materials, these changes could have a significant effect on the classification of hazardous material information in the future.

B. Exemption Four and Confidential Business Information

As the DOT has lessened its reliance on Exemption 1, the DOT's use of Exemption 4 has remained consistent.[60] Exemption 4, commonly referred to as the "business records exemption," provides for the withholding of confidential business information, trade secrets, and financial data.[61] A 1992 case, *Critical Mass Energy Project v. Nuclear Regulatory Commission,*[62] established the prevailing test for Exemption 4 confidential business information. In this case, the D.C. Circuit Court of Appeals noted that Congress designed Exemption 4 to foster information-sharing between the government and private industry.[63] For this reason, this court held that information protected under FOIA Exemption 4 must be of a commercial nature, voluntarily secured in confidentiality, and not regularly available to the public.[64]

The *Critical Mass Energy* test also encompasses a two-part test for confidentiality that was previously established by the same court in *National Parks and Conservation Association v. Morton.*[65] For information to qualify as confidential under the *National Parks* standard, the agency's disclosure of that information must have the likely effect of hampering the government's ability to gather subsequent data or cause competitive harm to the person submitting the

---

http://www.dot.gov/foia/reports/2002annualreport.html; 2003 DOT ANN. REP., *available at* http://www.dot.gov/foia/reports/2003annualreport.html.

[60] The number of requests denied under Exemption 4 has numbered between 230 and 285 during the past four years. *See* 2000 DOT ANN. REP., *available at* http://www.dot.gov/foia/2000annual_foia_report.html; 01 DOT ANN. REP., *available at* http://www.dot.gov/foia/reports/2001annualreport.html; 2002 DOT ANN. REP., *available at* http://www.dot.gov/foia/reports/2002annualreport.html; 2003 DOT ANN. REP., *available at* http://www.dot.gov/foia/reports/2003annualreport.html.

[61] 5 U.S.C. § 552(b)(4) (2004). The exemption protects "trade secrets and commercial or financial information obtained from a person and privileged or confidential." *Id.*

[62] Critical Mass Energy Project v. Nuclear Regulatory Commission, 975 F.2d 871 (D.C. Cir. 1992).

[63] *Id.* at 879.

[64] *Id.* at 879.

[65] *See* Nat'l Parks & Conservation Ass'n v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974) (holding that for information to fall under FOIA Exemption 4, disclosure must impair government's ability to obtain necessary information or to cause substantial harm to competitive position of person from whom information is obtained).

information.[66] Exemption 4 includes many elements similar to the provisions of the Critical Infrastructure Information Act.[67] Both Exemption 4 and the Critical Infrastructure Information Act both require that the information be voluntarily disclosed to the government by an individual.[68] These statutes also mandate that information normally released to the public does not qualify for protection from disclosure because it would not be considered confidential.[69]

C. Exemption Three and Statutory Protections

Prior to the enactment of the Homeland Security Act, federal agencies could rely on any statutory exemption that comported with the requirements of Exemption 3 if they desired to protect information.[70] In order for an agency to rely on Exemption 3, the relied-upon statute must mandate that the information be protected from disclosure.[71] If the statute provides for discretionary release of information, Exemption 3 does not apply.[72] Thus, an agency cannot rely on Exemption 3 to withhold information if the statute provides the agency with discretion to allow its release. The statute relied upon also must provide a policy for the withholding of information.[73] This requires the establishment of procedures for withholding information as well as a description of information that can be withheld. [74]

D. Administrative Policy

The tone set by a presidential administration often influences the Department of Justice's (DOJ) interpretation of FOIA. The DOJ acts as legal representation for the federal government and government agencies in all FOIA litigation. In addition, the DOJ maintains a large amount of policy, procedure, and case information about FOIA litigation. Because the DOJ acts as the primary overseer of federal compliance with FOIA, the precedent it establishes ultimately affects the public's ability to access information.[75] Shortly after beginning his first term, President Bill Clinton issued a memorandum advocating an increase in information disclosure.[76] The memorandum

---

[66] *Id.* at 770.

[67] *Compare* 6 U.S.C. § 133(a)(1), *with National Parks*, 498 F.2d at 770.

[68] *Compare* 6 U.S.C. § 133(a)(1), *with National Parks*, 498 F.2d at 770.

[69] *Compare* 6 U.S.C. § 133(a)(1), *with National Parks*, 498 F.2d at 770.

[70] 5 U.S.C. § 552(b)(3) (2003).

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] Department of Justice Web Page, www.usdoj.gov/foia.html.

[76] William J. Clinton, Memorandum for Heads of Departments and Agencies: The Freedom of

emphasized the need for open government and for the free flow of information.[77] In addition, former Attorney General Janet Reno issued a memorandum furthering this policy and directing all personnel to withhold information under a FOIA exemption only where "the agency reasonably foresees that disclosure would be harmful to an interest protected by that exemption."[78] Essentially, the Reno memorandum established a presumption in favor of disclosure. These memoranda changed the DOJ's legal standard for disclosure, implementing Reno's "foreseeable harm" standard in place of the standard established by President Ronald Reagan's administration, which was less favorable to disclosure.[79] Under the Reno policy, the Department of Justice would only support a federal agency's decision to withhold information if the agency met the foreseeable harm standard.

III. POST-9/11 INFORMATION ACCESS

The Clinton Administration's policy on information disclosure lasted for less than one year following the election of President George W. Bush. Shortly after the September 11, 2001 terrorist attacks, the Bush Administration reinstated the "substantial legal basis" standard that drove the Reagan Administration's interpretation of FOIA. In October 2001, Attorney General John Ashcroft issued a memorandum discussing the desire of the Bush Administration to revise the FOIA policy. This document recognized that the federal government must comply with FOIA: "As you know, the Department of Justice and this Administration are committed to full compliance with the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2000)."[80] However, the

---

Information Act (Oct. 1993), *available at* http://www.usdoj.gov/04foia/93_clntmem.htm.

> I therefore call upon all Federal departments and agencies to renew their commitment to the Freedom of Information Act, to its underlying principles of government openness, and to its sound administration. This is an appropriate time for all agencies to take a fresh look at their administration of the Act, to reduce backlogs of Freedom of Information Act requests, and to conform agency practice to the new litigation guidance issued by the Attorney General, which is attached."

Id.

[77] *Id.*

[78] Janet Reno, Memorandum for Heads of Departments and Agencies: The Freedom of Information Act (Oct. 1993), *available at* http://www.fas.org/sgp/clinton/reno.html.

[79] *Id.* For a discussion of the previous standard, known as the "sound legal basis" standard, *see infra* Part IV discussing the Ashcroft Memorandum.

[80] John Ashcroft, Memorandum for Heads of All Federal Departments and Agencies: The Freedom of Information Act (Oct. 2001), *available at* http://www.fas.org/sgp/foia/ashcroft.html. "It is only through a well-informed citizenry that the leaders of our nation remain accountable to the governed and the American people can be assured that neither fraud nor government waste is concealed." *Id.*

memorandum also contained language that encouraged agency heads to protect information whenever it might be possible to do so under a FOIA exemption: "I encourage your agency to carefully consider the protection of all such values and interests when making disclosure determinations under the FOIA."[81] Finally, the memorandum assured agency heads that the Department of Justice would support decisions to withhold information based on the FOIA exemptions.[82] Unlike the presumption of disclosure established by the Reno memorandum's "foreseeable harm" standard, the Ashcroft memorandum's "substantial legal basis" standard instead created a presumption that agencies withhold information. In addition, the "sound legal basis" standard encourages agencies to find ways to prevent the disclosure of information by supporting decisions to withhold information if there is any justification.[83]

Many scholars have suggested that the Ashcroft memorandum would have a significant impact on the willingness of federal agencies to release information under FOIA.[84] However, a study of federal agencies, including the Department of Transportation, by the U.S. General Accounting Office, suggests that this may not be the case.[85] The Freedom of Information officers surveyed disagreed as to whether disclosure has decreased in light of the Ashcroft memorandum.[86] Of the 52 percent who believed agency disclosure practice had changed since the memorandum's issuance, only one-third of them reported a decrease in FOIA releases.[87] Interestingly, of those who did report a decrease, more than 75 percent cited the Ashcroft memorandum as the reason behind the change.[88] The arguably minimal decrease suggests that despite the Ashcroft memorandum's

---

[81] John Ashcroft, Memorandum for Heads of All Federal Departments and Agencies: The Freedom of Information Act (October 2001), *available at* http://www.fas.org/sgp/foia/ashcroft.html. (stating that any discretionary decision by an agency to disclose information protected under FOIA should be made only after full and deliberate consideration of institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information).

[82] *Id.* (stating that when carefully considering FOIA requests and decide to withhold records, in whole or in part, one can be assured that Department of Justice will defend decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records).

[83] *Id.*

[84] *See* Keith Anderson, *Is There Still A 'Sound Legal Basis?: The Freedom of Information Act in a Post-9/11 World*, 64 OHIO ST. L.J. 1605 (2003); Patrice McDermott, *Withhold and Control: Information in the Bush Administration*, 12-Spr. KAN. J.L. & PUB. POL'Y 671 (2003); Uhl, *supra* note 14, at 265 (arguing that War on Terrorism does not justify climate of non-disclosure that has developed in United States since the September 11th terrorist attacks).

[85] U.S. GEN. ACCT. OFFICE, FREEDOM OF INFORMATION ACT: AGENCY VIEWS ON CHANGES RESULTING FROM NEW ADMINISTRATION POLICY (Sept. 2003).

[86] *Id.* Of those surveyed, 48 percent reported no change in the amount of information they were disclosing. *Id.*

[87] *Id.*

[88] *Id.*

insistence that FOIA officers thoroughly consider all exemptions and consider the ability of agencies to rely on the broad language of the Critical Infrastructure Information Act, agencies may not have drastically changed their disclosure practices. The recent nature of the Critical Infrastructure Information Act, combined with its sweeping language, makes it difficult to determine patterns of specific change in any agency's actual practice.

The Homeland Security Act of 2002 has implications for the public's ability to access information because it creates a new statutory exemption from FOIA.[89] The legislation, enacted by Congress in November 2002, established the Department of Homeland Security, giving the new department responsibility for information analysis and infrastructure protection.[90] The legislature sought to accomplish this mission through an increase of involuntary sharing of information between the federal government and the private sector.[91] "Information that people can act upon is an invaluable weapon in any war."[92] Title II of the Homeland Security Act provides for this information-sharing program through a provision known as the Critical Infrastructure Information Act.[93] Designed to encourage the private sector to provide information to the Department of Homeland Security, the Critical Infrastructure Information Act creates a statutory exemption to the Freedom of Information Act that will prohibit the public from accessing protected critical infrastructure information submitted under the new statute.[94]

A. Exemption Three and the Critical Infrastructure Information Act

Under Exemption 3 to FOIA, Congress has the authority to enact statutory provisions that prohibit information from being disclosed.[95] In order for a statutory provision to qualify under Exemption 3, the statute must unequivocally require that such information be prohibited from disclosure.[96] The statute must also establish a withholding procedure to determine which information qualifies for the exemption.[97] The Critical Infrastructure Information Act operates as this

---

[89] Homeland Security Act of 2002, Pub. L. No. 107-296, §§ 200 et. seq..

[90] *Id.*

[91] Homeland Security Secretary Tom Ridge, Address to the American Enterprise Institute (Sept. 2, 2003), *available at* http://www.whitehouse.gov/news/releases/2003/09/20030902-7.html. "[T]he new Department's Information Analysis and Infrastructure Protection Unit focuses exclusively on threats to the homeland and how we can reduce our vulnerability to attack, strengthen our critical infrastructure, both cyber and physical." *Id.*

[92] *Id.*

[93] Homeland Security Act of 2002, Pub. L. No. 107-296, § 214.

[94] *Id.*

[95] 5 U.S.C. § 552(b)(3) (2004).

[96] *Id.*

[97] *Id.*

type of statutory exemption,[98] providing the private sector with numerous protections for submitted critical infrastructure information.[99] Section 214 of the Critical Infrastructure Information Act protects private-sector critical infrastructure information submitted under the law from disclosure.[100] The Department of Homeland Security's Procedures for Handling Critical Infrastructure Information, however, provide guidance on disclosure of this information.[101] Congress designed these broad protections to encourage members of the private sector to share information about their business infrastructures, communication systems, emergency action plans, and potential vulnerabilities with the Department of Homeland Security.[102] Conscious that this information-sharing might subject them to lawsuits, prosecution, and other unforeseen consequences, industry leaders testified that they were hesitant to provide such information if it had to be made available to the public.[103] The CIIA protected this information from public disclosure, thus protecting an industry that provided the information.

Congress crafted the language of the Critical Infrastructure Information Act to cover information that might be disclosed by the private sector but would not gain protection under other FOIA exemptions.[104] "Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose . . . shall be exempt from

---

[98] 6 U.S.C. § 133(a)(1)(A) (2004).

> Notwithstanding any other provision of law, critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2) shall be exempt from disclosure under § 552 (commonly referred to as the Freedom of Information Act).

Id.

[99] 6 U.S.C. § 133 (2004). Under this section, critical infrastructure information is not subject to FOIA, agency rules regarding ex parte communications, use by federal agencies to which it was not disclosed or use in criminal investigations or prosecutions. *Id.*

[100] 6 U.S.C. § 133(a)(1) (2004).

[101] Department of Homeland Security Procedures for Handling Critical Infrastructure Information, 6 C.F.R. § 29 (2004).

[102] Gina Marie Stevens, Cong. Res. Serv., Homeland Security Act of 2002: Critical Infrastructure Information Act 5 (Feb. 2003).

[103] *Id.*

[104] *Id.*

disclosure under [FOIA]."[105]

For information to qualify as critical infrastructure information and gain the statutory exemption from FOIA, it must meet four requirements outlined in the statute. First, it must be voluntarily submitted by a member of the private sector.[106] If a federal agency has compelled a private entity to provide the information, it will not qualify for protection under the statutory exemption.[107] In addition, a company's required filings with the Securities Exchange Commission fall outside the protection of the FOIA exemption.[108] Information that a private party submits in order to comply with federal licensing requirements is also considered involuntarily submitted.[109] Information obtained during regulatory hearings is exempt from the Critical Infrastructure Information Act's protection as well because it does not meet the requirement of voluntary submission.[110]

Once the Department of Homeland Security determines the information was voluntarily submitted, the second step requires analysis of whether the information relates to the submitting entity's critical infrastructure. Embedded within the Critical Infrastructure Information Act's definition of critical infrastructure information is the requirement that the information relates to a company's critical infrastructure.[111] While the Critical Infrastructure Information Act does not define critical infrastructure, section II of the Homeland Security Act does provide a definition.[112] Essentially, critical infrastructure is an entity's assets, both physical and virtual, that would have a significant effect on the nation's security, economic stability, or public health if these assets were compromised.[113] The definition of critical infrastructure

---

[105] 6 U.S.C. § 133(a)(1)(A) (2004).

[106] 6 U.S.C. § 131(7)(A) (2004) states:

> The term 'voluntary,' in the case of any submittal of critical infrastructure information to a covered Federal agency, means the submittal thereof in the absence of such agency's exercise of legal authority to compel access to or submission of such information and may be accomplished by a single entity or an Information Sharing and Analysis Organization on behalf of itself or its members.

Id.

[107] 6 U.S.C. § 131(7)(A) (2004).

[108] 6 U.S.C. § 131(7)(B)(i)(I) (2004).

[109] 6 U.S.C. § 131(7)(B)(ii) (2004).

[110] *Id.*

[111] 6 U.S.C. § 133 (2004).

[112] Homeland Security Act of 2002, Pub. L. No. 107-296, § 2.

[113] *Id.* The Act defines critical infrastructure as "systems and 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." *Id.*

information also is complex.[114] In order to qualify for protection, the information submitted must somehow relate to the protection of a part of the industry that is essential to our nation's ability to function or that would be potentially harmful if attacked.[115] An industry's documents relating to risk identification, management, and prevention also are covered under the definition of critical infrastructure information.[116] Information that normally falls within public knowledge, however, does not qualify for protection.[117] The information must relate to the security or protection of critical infrastructure, which is also defined in the statute.[118]

The third step to gain protection from disclosure under the Critical Infrastructure Information Act requires that the Department of Homeland Security analyze the purpose under which the private entity submitted the information. To gain protection, the information must be submitted in good faith by a member of the private sector with the belief that the information qualifies under one of the purposes enumerated in the statute.[119] The language provides for seven broad purposes, ranging in specificity from "interdependency

---

[114] *See* 6 U.S.C. § 131(3) (2004). The term "critical infrastructure information" means:

> [I]nformation not customarily in the public domain and related to the security of critical infrastructure or protected systems 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 the 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 or safety; the ability of any critical infrastructure or protected system 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 any planned or past operational problem or solution regarding critical infrastructure or protected systems, including repair, recovery, reconstruction, insurance, or continuity, to the extent it is related to such interference, compromise, or incapacitation."

Id.

[115] 6 U.S.C. § 131(3) (2004).

[116] *Id.*

[117] *Id.*

[118] *Id.*

> The term 'protected system' means any service, physical or computer-based system, process, or procedure that directly or indirectly affects the viability of a facility of critical infrastructure; and includes any physical or computer-based system, including a computer, computer system, computer or communications network, or any component hardware or element thereof, software program, processing instructions, or information or data in transmission or storage therein, irrespective of the medium of transmission or storage.

Id.

[119] *Id.*

study" to "other informational purpose."[120]

Finally, the statute requires an explicit statement by the submitting entity that the entity intends the information to fall within the FOIA exemption provided by the Critical Infrastructure Information Act.[121] If the entity supplies the records in written form, this statement must be clearly marked on the document.[122] To gain protection for oral information, the Critical Infrastructure Information Act mandates that submitters must provide a written statement of intent to submit the oral information as protected critical infrastructure information within a short time after the initial communication is made.[123] Subsequent documents require a written statement of intent to protect oral communications within 15 calendar days of its oral transmission.[124]

B. The Scope of Protection Under the Critical Infrastructure Information Act

The DOT and the Department of Homeland Security have implemented several joint initiatives that seek to evaluate transportation safety and gather information in response to those security assessments.[125] Much of this information would likely be unavailable to members of the public. For example, members of the private-sector transportation industry, including rail transportation companies such as Amtrak and other industrial carriers, have begun to create risk-assessment documents, vulnerability evaluations, and emergency preparedness plans in response to these government initiatives.[126] The program, designed to help carriers assess weaknesses in passenger and cargo security, also encourages private-sector transportation providers to

---

[120] *Id.* The full range of purposes includes "the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose." *Id.*

[121] 6 U.S.C. § 133(a)(2) (2004).

> For purposes of paragraph (1), the term "express statement", with respect to information or records, means in the case of written information or records, a written marking on the information or records substantially similar to the following: "This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002"; or in the case of oral information, a similar written statement submitted within a reasonable period following the oral communication.

Id.

[122] *Id.*

[123] *Id.*

[124] Department of Homeland Security, Procedures for Handling Critical Infrastructure Information, 6 C.F.R. § 29 (2004).

[125] Department of Homeland Security, Rail Transit Fact Sheet (March 22, 2004), *available at* http://www.dhs.gov/dhspublic/display?content=3377.

[126] *Id.*

document these shortcomings. Under such a plan, disclosure of this written information could pose a legal liability to the companies that compile it. However, were a private-sector transportation provider to turn over this information to the federal government, it would likely come under the protection of the Critical Infrastructure Information Act. As long as the transporter voluntarily submitted the information, it would fall within the protections of the Critical Infrastructure Information Act, making it non-disclosable under Exemption 3 of the FOIA. In addition, the submitting entity could ensure that the information not be used as the basis for any civil or criminal action brought by the United States.

In addition to providing protection from legal or regulatory action, the Critical Infrastructure Information Act contains other provisions that may harm the public's ability to access information. The Act itself makes no reference to how the DOT will determine whether submissions qualify for protection. Instead, the Act outlines a list of criteria for the submission of information. The Department of Homeland Security, in its subsequent guidance document, determined that all information submitted in compliance with the statute's mandates, including voluntary submission and proper marking as critical infrastructure information, will be presumed to be protected from the time it is received.[127] The only way protection will be removed is if the Protected Critical Infrastructure Information Program Manager determines that the information is not to be protected.[128] Thus, the presumption of protection provides the public with no direct way to challenge the submission of information or its classification as protected. Essentially, only one person, the Program Manager, has the authority to determine if submitted information can be withheld from the public.

C. Limits on Critical Infrastructure Protection

Attempts by the Department of Transportation to improve the safety of HazMat transportation in the wake of the September 11th terrorist attacks may actually provide the public with a better chance to obtain information regarding private HazMat carriers. Since 2001, the DOT has enacted regulations that require HazMat carriers to submit more information regarding their activities than previously required.[129] The regulations seek to obtain information that the carriers might have provided voluntarily under the Critical Infrastructure

---

[127] Department of Homeland Security, Procedures for Handling Critical Infrastructure Information, 6 C.F.R. § 29.6(b) (2004).

[128] *Id.*

[129] *See, e.g.*, Hazardous Materials: Enhancing Hazardous Materials Transportation Safety, 49 C.F.R. §§ 107.105, 107.109, 171.12A, 176.7, 177.804 (2004); Hazardous Materials: Security Requirement for Transporters and Offerors of Hazardous Materials, 49 C.F.R. § 172 (2003).

Information Act.[130] This information includes personal data about employees who handle hazardous materials, including their citizenship and criminal history. Because the carriers submit the information under the legal authority of the Department of Transportation, the submission should not fall within the definition of voluntary. Thus, exemption under the Critical Infrastructure Information Act, as well as Exemption 4, should be barred.

The DOT has also recently expanded its regulation of the hazardous materials transportation process to include both the packaging and the pre-transportation functions, as well as loading, transportation, and unloading.[131] More private-sector companies will now come under the purview of the DOT's licensing and information-gathering mandates. Much of the information mandated from these companies includes delivery practices, packaging methods, and other handling instructions. The obligatory submission of information will preclude these private-sector industries from submitting the information for protection under the Critical Infrastructure Information Act, which would have been permissible had they not fallen within the DOT's regulatory jurisdiction.

D. DHS Procedures for Handling Critical Infrastructure Information

Some provisions in the Department of Homeland Security ("DHS") guidance documents may help agencies implement the Critical Infrastructure Information Act in a manner that is more favorable to access.[132] These documents delineate the differences between protected critical infrastructure information and information that is not exempt from disclosure under FOIA.[133] For example, the regulation specifically addresses information submitted to fulfill any federal statutory or regulatory request for information by ruling it cannot be protected under the exemption. In addition, submitting information for Critical Infrastructure Information Act protection cannot be used to fulfill any other federal information submission requirements.[134]

The guideline document also limits critical infrastructure information only to information submitted to the Department of Homeland Security. This eliminates the concern that indirect submissions would be protected under the statutory exemption.[135] Under the new guidance document, the entity must

---

[130] *Id.*

[131] Department of Transportation Research and Special Programs Administration, Applicability of Hazardous Materials Regulations to Loading, Unloading, and Storage, 49 C.F.R. §§ 171, 173, 174, 175, 176, 177, 178 (2003).

[132] *See* Dept. of Homeland Security, Procedures for Handling Critical Infrastructure Information, 6 C.F.R. § 29 (2004).

[133] *Id.*

[134] *Id.*

[135] *Id.*

submit the information directly to DHS in order to qualify as protected information.[136] Critical infrastructure information that the entity does not submit to the Protected Critical Infrastructure Information Manager will not receive an exemption from FOIA.[137] The guidance document establishes a policy for information mistakenly submitted to the wrong entity. The policy mandates that any federal official receiving critical infrastructure information must maintain the information in accordance with the DHS guidelines until the information can be forwarded to the Protected Critical Infrastructure Information Manager.

The DHS guidelines also establish a procedure for evaluating information to ensure that it should qualify as protected critical infrastructure information. If the Manager determines the information is not protected, the Manager must notify the submitting party, who is then given the opportunity to further justify why the information merits protection. The notification also allows the submitting party the opportunity to withdraw the information. If, after subsequent review, the Manager makes a final determination that the submitted information does not merit protection, the submitting party may submit the information without exemption from FOIA or the Manager may dispose of the information in accordance with federal law. However, one of the greatest weaknesses of the new rule is its failure to establish a time frame in which these decisions must be made, which allows agencies to delay denying information protection in order to prevent its release for a longer period of time.[138]

Finally, the guideline document addresses the relationship between the Critical Infrastructure Information Act and other FOIA exemptions. This section should provide agencies with a greater understanding of the disclosure policies. The guidelines note that protected critical infrastructure information is exempt from FOIA. Additionally, no state or local FOI laws can be used to force disclosure by state or local governments in possession of critical infrastructure information. The guidelines do make clear, however, that the Critical Infrastructure Information Act does not protect from disclosure any information that may be legally requested under federal, state, or local laws, even if it would qualify as protected critical infrastructure information.

CONCLUSION

Depending on its interpretation, the Critical Infrastructure Information Act has the potential to severely limit the amount of information that the public can access regarding the transportation of hazardous materials. Given its broad language, the statutory exemption could be read to include voluntarily submitted

---

136 *Id.*

137 *Id.*

138 *Id.*

information such as risk-management plans, transportation-route safety evaluations, and other information that would be beneficial to public knowledge. Recent efforts by the Department of Transportation to make submission of this information less likely to be considered voluntary may provide the public with a chance to argue for access.

The limits placed upon the Critical Infrastructure Information Act by the Department of Homeland Security's Procedures for Handling Critical Infrastructure Information will help ensure that the exemption created by the statute will not swallow up the disclosure rule. Narrowing the scope of protected critical infrastructure information was essential to ensuring the public's access to information regarding the transportation of hazardous materials. In addition, the recognition that not all critical infrastructure information is protected will substantially shift the burden onto the private sector to prove that the information should be protected. In doing so, the burden regarding disclosure again shifts to the government and away from the public by requiring agencies to determine if submitted information actually meets the four criteria demanded by the Critical Infrastructure Information Act in order for it to be withheld.

Many of the provisions of the Critical Infrastructure Information Act's statutory exemption merely codify already existing case law regarding other FOIA exemptions. Its resemblance to the rulings in *Critical Mass Energy* and *National Parks* seem to imply that the Act may actually be a way to solidify this area of access law. However, some of the broad provisions of the Critical Infrastructure Information Act, such as its all-encompassing definition of critical infrastructure information, only add haze to a possible attempt to clarify the ambiguities of Exemptions 1 and 4. Again, interpretation of such terms will be essential to ensuring that public access to information remains viable.

Because the Department of Justice is charged with overseeing the administration of FOIA, the Attorney General also has the ability to influence its interpretation. The recent appointment of Alberto Gonzales as the 80th U.S. Attorney General may limit the impact of post-9/11 legislation on public access to information. Since his February 2005 confirmation, Gonzales has expressed a willingness to re-visit the information-squelching perspective outlined in the Ashcroft memorandum. In his Installation Address, Gonzales commented that his foremost priority as the Attorney General must be upholding the U.S. Constitution.[139] Therefore, a decision by Gonzales to return to pre-Ashcroft levels of disclosure could prevent the critical infrastructure exemption from burgeoning into an all-encompassing limitation on access to information.

---

[139] Alberto Gonzales, Installation Address (Feb. 14, 2005), *at* http://www.usdoj.gov/ag/speeches/2005/02142005_aggonzales.htm (last visited March 1, 2006).