

---

# Balancing Homeland Security and Freedom of Information

---

Stephen Gidiere and Jason Forrester

*A popular Government, without popular information, or the means of acquiring it, is but a prologue to a farce or a tragedy.*

James Madison  
August 4, 1822

The hallmarks of America are our freedoms: freedom of speech, freedom of association, freedom of movement, freedom of the press and, the subject of this article, freedom of information. The terrorist attacks of September 11 have prompted a reevaluation of how each of these freedoms balances against the need for safety and security, and our approach to public access to information in the hands of the government is no different.

Specifically, attention is focusing on the need for the protection of information relevant to the new war on terrorism—a war in which domestic assets are both targets and weapons. Information and electronic access to it have become weapons in this new war. In the environment, energy, and resources arena, information about power plants, pipelines, transmission systems, emergency preparedness, and hazardous and toxic materials storage and transportation is directly relevant to homeland security. In a stark example, the Federal Bureau of Investigation (FBI) issued an alert to the oil and gas industry on November 26, 2001, that terrorists may be planning an attack on natural gas infrastructure in the event that Osama bin Laden is captured or killed.

But, despite the fact that “everything has changed” in our post-September 11 world, policy decisions about our societal freedoms must be made with some historical perspective. When Congress enacted the Freedom of Information Act (FOIA) in 1966, 5 U.S.C. § 552, it formalized a principle which Americans have understood since the beginning of our republic—that “an informed citizenry is vital to the functioning of a democratic society,” in words attributed to Thomas Jefferson. FOIA’s drafters recognized that government accountability to the public was critical to a properly functioning government and, more importantly, to a free society.

---

*Mr. Gidiere practices environmental and natural resources law with Balch & Bingham LLP in its Birmingham, Alabama office. He may be reached at [sgidiere@balch.com](mailto:sgidiere@balch.com). Mr. Forrester is research director of the Nuclear Threat Reduction Campaign. He may be reached at [jason@vi.org](mailto:jason@vi.org).*

In this spirit, FOIA requires a federal agency to release information in its control to “any person” following a request reasonably describing the documents sought. But, Congress did not simply hand the public the keys to the government’s filing cabinets. The statute balances public disclosure against other important considerations, including national security, through nine exemptions. Of these exemptions, four stand out as possible protections against the release of information critical to homeland security: Exemptions 1 (classified information), 2 (internal agency procedures), 3 (exempted by statute), and 4 (confidential business information). See 5 U.S.C. § 552(b).

At first blush the thought of a would-be terrorist availing himself of the traditional FOIA process seems absurd—imagine a man crouched in the mouth of a cave in the wind-swept hills outside of Kandahar scribbling in broken English a written FOIA request to the Environmental Protection Agency (EPA) seeking information about U.S. facilities that store toxic and hazardous materials. He is careful, of course, to request a fee waiver and insists (as does any seasoned practitioner) that the agency provide all reasonably segregable portions of any withheld records. (One could only hope that he is beset by the same incessant delays that plague all of us who file written FOIA requests.) Sounds ridiculous, right?

Unfortunately, recent events have demonstrated all too vividly that worlds we once thought were distant are now colliding. The terrorists of September 11 availed themselves of the everyday freedoms that Americans take for granted. Booking an airline ticket over the Internet, reserving a rental car, arranging for pilot training, and, in our environmental world, obtaining a hazardous substance transportation license are everyday activities in the U.S. which are now potential instruments of war.

Moreover, information may fall into the wrong hands without a direct request by a potential terrorist. Once information is released into the public domain, it becomes easily accessible. Commercial services that compile and organize public information into private databases for resale are commonplace. In fact, the bluntness of one recent e-mail solicitation from such a service is startling. The solicitation boasted access to “thousands of databases from around the world” and offered “to conduct in-depth background searches on in-

dividuals, companies, institutions and organizations in over 120 countries." The service claimed to use "intelligence-based software products to ferret out useful and relevant information on the targets of your inquiries" and even guaranteed that its "electronic searches are non-traceable to our clients, undetectable by the target and leave 'no footprints in the sand.'" (November 1, 2001 e-mail on file with the authors).

In addition to this avenue, immediate, direct, *and free* electronic access to information in the government's possession has become the norm. The Electronic FOIA Amendments of 1996 (E-FOIA), Pub. L. No. 104-231, 110 Stat. 3048, for example, require federal agencies to establish so-called electronic reading rooms. Basically, E-FOIA requires that records created by an agency after November 1, 1996, be made available on the agency's website following a FOIA request, if "the agency determines [the records] have become or are likely to become the subject of subsequent requests for substantially the same records." 5 U.S.C. § 552(a)(2)(D).

Importantly, electronic posting is not required for information *obtained* by a federal agency from a private business or other entity. Rather, posting of such obtained information is within the discretion of the agency, subject to certain restrictions like copyright laws. *See* 5 U.S.C. § 552(a)(2); U.S. Department of Justice, *FOIA Update*, Vol. XVIII, No. 1 (Winter 1997) (the complete text of all issues of DOJ's *FOIA Update* cited in this article can be accessed at [www.usdoj.gov/oip/foi-upd.htm](http://www.usdoj.gov/oip/foi-upd.htm)). Because a large amount of homeland security information, such as critical infrastructure information, is obtained from private parties, agencies can use their discretion not to post that information. However, once an agency incorporates or summarizes such information into a newly created record (as agencies are wont to do), the record becomes subject to the mandatory posting requirement.

Prior to September 11, agencies flooded their websites with information, not only to comply with E-FOIA, but also to regulate through disclosure and to ease their own administrative burden of responding to written requests. But since September 11, agencies have done an about-face and have rushed to remove information from their websites that they deem may be useful to would-be terrorists.

For example, the Nuclear Regulatory Commission (NRC) initially took its entire website offline and has subsequently begun "deploying its newly redesigned public Web site in a phased approach following a thorough review of all information at the site." *See* [www.nrc.gov](http://www.nrc.gov), visited Nov. 9, 2001. The State of New Jer-

sey, a leader in regulation through disclosure of information collected under its Community Right-to-Know Survey, has pulled the plug on Internet access to its facilities database, which includes information about hazardous materials storage. *See* [www.state.nj.us/NASApp/pCRTK/jsp/ecrtkview.jsp](http://www.state.nj.us/NASApp/pCRTK/jsp/ecrtkview.jsp), visited Nov. 28, 2001 ("The Public Access System is temporarily unavailable."). The Federal Energy Regulatory Commission (FERC) announced that in light of September 11 it was removing information from its website containing specifications of certain energy facilities it licenses. *See* 66 Fed. Reg. 52,917 (2001). To obtain such materials, interested persons must submit a written FOIA request.

There are numerous other examples: the Department of Energy removed its National Transportation of Materials site; the U.S. Geological Survey removed a number of water resource reports from its site and requested that its CD-ROM publication on large public surface water supplies be removed from circulation and destroyed; and the Department of Transportation's Office of Pipeline Safety removed pipeline mapping data from its site.

It is not yet clear whether this quick response by federal and state agencies will result in the permanent withholding of the types of records that were once readily available or whether it is simply a temporary reaction. No doubt the reevaluation now taking place at many agencies involves an analysis of the various FOIA exemptions that could be used to protect homeland security information either from traditional written disclosure or electronic posting. This article first discusses FOIA's Exemptions 1 (classified information), 2 (internal agency procedures), and 4 (confidential business information), in an attempt to determine their efficacy in preventing the release of

information relevant to homeland security and the need for legislative or administrative changes. This article also discusses legislation pending in Congress that would prohibit the release of critical infrastructure information via FOIA's Exemption 3.

In addition to the language of the exemptions and the relevant case law, these exemptions must now be read in light of Attorney General Ashcroft's October 12, 2001 memorandum to all federal agencies on FOIA implementation (Ashcroft Memo). It has become the tradition since the Carter administration for Attorneys General to issue memos to the agencies describing the Department of Justice's (DOJ) policy for defending agencies in their decisions to withhold documents. *See, e.g.,* Attorney General Reno's FOIA Memorandum to Heads of Departments and Agencies (Oct. 1993) (Reno

---

*FOIA's drafters recognized  
that government  
accountability to the public  
was critical to a properly  
functioning government.*

---

Memo). The Ashcroft Memo states that DOJ will defend agency withholdings “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.”

This “sound legal basis” standard is much more slanted toward withholding than the standard announced in 1993 by Attorney General Reno. The Reno Memo instructed agencies to use their discretion to release records—even where they qualified for an exemption—unless release would cause “foreseeable harm” to the purposes for which the exemption was established. The Ashcroft Memo does not explicitly state that it was promulgated in response to September 11, but its more liberal withholding policy will certainly affect agencies’ implementation of the exemptions discussed below.

### *Exemption 1: Classified Information*

Perhaps the most obvious place to begin a discussion of whether FOIA is effective in protecting homeland security information is Exemption 1. Exemption 1 protects information classified pursuant to an applicable executive order. The operative executive order today is Executive Order No. 12,958 issued by President Clinton in 1995 (and amended in 1999 by Executive Order No. 13,142). See Exec. Order No. 12,958, 60 Fed. Reg. 19,825 (1995) (Clinton Executive Order). It is the fifth in a series of such executive orders, the first of which was issued by President Truman in 1951.

The categories of information that may be classified under the Clinton Executive Order are broad enough to include homeland security information. Information may be classified if it concerns scientific, technological, or economic matters relating to the national security; a U.S. government program for safeguarding nuclear materials or facilities; or vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security. See Clinton Executive Order § 1.5. Not surprisingly, military, intelligence, and foreign relations information is also eligible for classification. See *id.* Information falling within any of these categories may be classified if its release “reasonably could be expected to result in damage to the national security” and that damage is identified or described by the classifying agency. *Id.* § 1.2(a)(4).

The Clinton Executive Order is significant as a reaction to the perceived *excessive secrecy* of the government during the Cold War period. The Clinton Executive Order was an attempt to loosen control and to speed the declassification of information within the government’s control.

In this vein, the executive order preamble states:

Our democratic principles require that the American people be informed of the activities of their Government. . . . Nevertheless, throughout our history, the na-

tional interest has required that certain information be maintained in confidence in order to protect our citizens, our democratic institutions, and our participation within the community of nations. . . . *In recent years, however, dramatic changes have altered, although not eliminated, the national security threats that we confront. These changes provide a greater opportunity to emphasize our commitment to open Government.*

(Emphasis added).

More than six years later, the question today is whether the reality of terrorism warrants a reevaluation of this premise and the trend toward openness reflected in the Clinton Executive Order. A look at some of the details of the Clinton Executive Order can help answer that question.

The Clinton Executive Order differs most significantly from its predecessor (Exec. Order No. 12,356 issued by President Reagan) with respect to the new procedures and presumptions put in place. These new procedures encourage the classification of less information and the faster declassification of more information. For example, among other things, the Clinton Executive Order: (1) places a general ten-year limit on classifications (the Reagan Executive Order had no limit); (2) establishes an automatic declassification mechanism (the Reagan Executive Order had no such mechanism); (3) removes certain presumptions of classified status (the Reagan Executive Order contained three presumptions of classified status); and (4) creates a mechanism for agency personnel to challenge classification decisions to an Interagency Security Classification Appeals Panel (the Reagan Executive Order had only a limited internal appeals process for certain donated records).

One question that must be addressed today is whether these new procedures should be reversed in favor of reestablishing greater secrecy. The most obvious argument against reversal is that the September 11 terrorists apparently did not utilize previously classified information. Moreover, the Clinton Executive Order was only one response to widespread criticism of the classification process following the end of the Cold War. The government was, and still is to some, keeping too much information classified.

For example, the classification process was the focus of the bipartisan Senate Commission on Protecting and Reducing Government Secrecy, chaired by Senator Daniel Patrick Moynihan (D-NY) and including Republican foreign relations heavyweight Senator Jesse Helms (R-NC). The commission issued a unanimous report in 1997. Among its key findings were: (1) that secrecy is itself a type of government regulation, and (2) that excessive secrecy has significant consequences when policymakers are not fully informed, the government is not held accountable for its actions, and the public cannot engage fully in informed debate. See S. Doc. No. 105-2 (1997). In the words of the Commission, “[t]he classification system . . . is used too often to deny the public an understanding of the policymaking

process, rather than for the necessary protection of intelligence activities and other highly sensitive matters.”

Thus, the struggle to bring more accountability to the classification process has been long and hard fought, and reversing that trend could have wider policy implications than necessary to address current concerns. Greatly limiting public access prevents the widest array of minds and institutions from working to reduce our vulnerabilities. Additionally, agencies already have the upper hand over the public in the classification process—they receive considerable deference on judicial review of their classification decisions.

Prior to September 11, the Bush administration initiated an interagency review of Exec. Order No. 12,958 as part of a general review of policies of the prior administration. The intervening events of September 11 are sure to influence that review. A complete discussion of all the potential issues involved in such a review is well beyond the scope of this article. Suffice it to say, however, an overhaul of the current executive order may not necessarily be the most effective way to protect homeland assets against terrorist threats—particularly given the availability of other FOIA exemptions as discussed below.

There are ways to work within the confines of the current executive order to address current events, and President Bush has already shown an inclination to do so. On December 10, 2001, President Bush acted pursuant to the Clinton Executive Order to grant the Secretary of Health and Human Services (whose agency is on the front line of the bioterrorism war) the authority to classify information as secret. *See* 66 Fed. Reg. 64,345 (2001). Perhaps another simple way to guarantee that homeland security interests are appropriately considered under Exemption 1 is for the President to include the new Director of the Office of Homeland Security Thomas Ridge on the Interagency Security Classification Appeals Panel. The President could also review the membership of the Information Security Policy Advisory Council, a federal advisory committee that advises the President on the classification process, to ensure that it includes sufficient representation of industries relevant to homeland security.

### *Exemption 2: Risk of Circumvention*

On its face, Exemption 2 does not seem to support the withholding of homeland security information. The exemption applies to information “related solely to the internal personnel rules and practices of an agency.” 5 U.S.C. § 552(b)(2). Courts have recognized, however,

that Exemption 2 applies not just to trivial internal matters like sick leave and parking policies (called “Low 2” information), but also to more substantial information, the disclosure of which would assist lawbreakers (called “High 2” information). Typically, High 2 information includes things like law enforcement manuals, guidelines for conducting investigations or conducting litigation, and information that would reveal the identity of confidential informants or undercover agents.

The seminal case recognizing the High 2 category, *Crooker v. ATF*, 670 F.2d 1051 (D.C. Cir. 1981), set out the two-part test still used today: (1) the requested document must be “predominantly internal” and (2) its disclosure must significantly risk the circumvention of agency regulations or statutes or impede the effectiveness of law enforcement activities.

In the wake of September 11, the DOJ’s Office of Information and Privacy (OIP) is encouraging agencies to use Exemption 2 to protect certain information about

critical domestic assets. In an epilogue to the Ashcroft Memo, OIP directed that “[a]gencies should be sure to avail themselves of the full measure of Exemption 2’s protection for their critical infrastructure information as they continue to gather more of it, and assess its heightened sensitivity, in the wake of the September 11 terrorist attacks.” *See* OIP, *New Attorney General FOIA Memorandum Issued*, posted Oct. 15, 2001, available at [www.usdoj.gov/oip/foiapost/2001foiapost19.htm](http://www.usdoj.gov/oip/foiapost/2001foiapost19.htm). OIP specifically instructed federal agencies that vulnerability assessments of “critical systems, facilities, stockpiles, and other assets” should be protected from disclosure under

the High 2-prong of Exemption 2.

An oft-cited example of such a vulnerability assessment is the computer security plans that the Computer Security Act of 1987, Pub. L. No. 100-235, 101 Stat. 1724, requires federal agencies to prepare. These plans describe the vulnerability of federal computer systems and the security measures taken to protect them from unauthorized access or tampering. Since as early as 1989, DOJ has been encouraging the withholding of these plans. *See FOIA Update*, Vol. X, No. 3 (Summer 1989).

But information about the vulnerability of *private* assets, unlike an agency’s assessment of its own assets, is not as clearly protected by Exemption 2. Exemption 2 applies only to an agency’s “predominantly internal” records, which seems to exclude records submitted by an outside private party. It could be argued, however, that this distinction is too simplistic. Courts often address the “predominantly internal” requirement when the document in question essentially establishes a legal

---

*On its face,  
Exemption 2 does not  
seem to support the  
withholding of homeland  
security information.*

---

norm. In other words, if the agency documents concern standards for regulating the public (often termed “secret law”), then Exemption 2 will not protect them. See *Cox v. DOJ*, 601 F.2d 1 (D.C. Cir. 1979). So, perhaps focusing the “predominantly internal” inquiry on the use to which an agency puts a particular piece of information, and not on its original source, would allow an agency to withhold information about the vulnerability of private assets.

Even DOJ’s OIP—which discharges DOJ’s administrative and policy responsibilities under FOIA and promotes governmentwide compliance with the Act—has not clearly stated whether Exemption 2 could be used to protect vulnerability and infrastructure information submitted to an agency by a private entity regarding nonagency assets. OIP’s 1989 guidance on vulnerability assessments mentions only one example of the successful withholding of such information (regarding threat levels at nuclear facilities) but that information was protected under Exemption 1. DOJ’s annual *FOIA Guide*, going a bit further, states that vulnerability assessments that properly fall within Exemption 2 “generally assess an agency’s vulnerability (or that of another institution) to some form of outside interference or harm by identifying those programs or systems deemed the most sensitive and describing specific security measures that can be used to counteract such vulnerabilities.” U.S. Department of Justice, *Freedom of Information Act Guide & Privacy Act Overview* (May 2000), at 125 (emphasis added) (*FOIA Guide*). Perhaps sensing the uncertainty on the issue, OIP’s epilogue to the Ashcroft Memo does not directly address the issue of nongovernmental assets, perhaps anticipating a legal challenge down the road. The clear implication of OIP’s epilogue is that such information is protected by Exemption 2.

Given this uncertainty, agencies may be searching for additional support for their decisions to withhold vulnerability and infrastructure information submitted by private entities. Agencies may find this additional support in Exemption 4, below.

#### *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.” 5 U.S.C. § 552(b)(4). Most information protected by Exemption 4 falls within the second part of this language as “confidential business information” or “CBI.”

The parameters of what qualifies as CBI have been fleshed out over the years, beginning with the seminal case of *National Parks & Conservation Association v. Morton*, 498 F.2d 765 (D.C. Cir. 1974). *National Parks* recognizes that information is protected as CBI if its release would either: (1) impair the government’s ability to obtain necessary information in the future, or (2)

cause substantial harm to the competitive position of the person from whom the information was obtained. See *id.* at 770.

The *National Parks* test was subsequently refined by *Critical Mass Energy Project v. NRC*, 975 F.2d 871 (D.C. Cir. 1992). Under *Critical Mass*, the first determination to be made is whether the information was submitted to the government “voluntarily” or whether it was required to be submitted. If the information was given over to the government voluntarily, then the only question is whether it is the type of information that “for whatever reason, would customarily not be released to the public by the person from whom it was obtained.” *Id.* at 878. If the business was compelled to provide the information, then essentially the two prongs of the *National Parks* test apply. The *Critical Mass* test for CBI is the most modern interpretation of Exemption 4—the D.C. Circuit generates more FOIA law than any other circuit and is generally thought to be on the cutting edge of those issues. Despite this, not all federal circuits have adopted the *Critical Mass* approach to CBI.

Exemption 4, then, seems to protect just the type of homeland security information only questionably protected by Exemption 2—vulnerability and infrastructure information submitted to agencies by private entities about private assets. First, if the information is “voluntarily” submitted, it would seem that such critical information is not the type of information that would be “customarily released” by the business. Moreover, even if the information is required to be submitted (or in a jurisdiction that has not adopted *Critical Mass*), vulnerability and infrastructure information is competitive in nature. Destruction of a business’s facility or equipment would undoubtedly cause it “substantial competitive harm”—just ask the airlines, who would be out of business after September 11 without a federal bailout.

In addition, Exemption 4 (unlike Exemptions 1 and 2) provides an existing procedural mechanism for the submitting business to explain to the agency why the information is critical and, therefore, protected from disclosure. With homeland security information—which often involves private, not public, assets—this is particularly important, as recognized by Director Ridge. In recent remarks about the security of critical information infrastructure systems, Director Ridge described the protection of such systems as “a political challenge, because the government must act in partnership with the private sector, since most of the assets that are involved in this effort are owned by the private sector, which owns and operates the vast majority of America’s critical infrastructure.” Remarks of Director Ridge, October 9, 2001, available at [www.whitehouse.gov/news/releases/2001/10](http://www.whitehouse.gov/news/releases/2001/10).

Exemption 4 provides just such an opportunity for partnership. EPA’s regulations, for example, require the agency, upon receipt of a FOIA request, to make a preliminary determination of CBI status and then, prior to making a final determination, provide the submitting

business with an opportunity to provide “substantiation comments” in support of the business’s CBI claim. *See generally* 40 C.F.R. Part 2, Subpart B. This opportunity to share information about the nature of submitted information is not unique to EPA’s procedures. Executive Order No. 12,600 requires all agencies to provide submitters advance notice and opportunity to comment prior to release of information claimed as CBI.

Equally important to protecting the information itself from release is the need to protect these substantiation comments. Such comments are themselves essentially a vulnerability assessment of the infrastructure or asset described in the originally submitted information. In recognition of the importance of receiving full and open comments from the private sector, EPA’s regulations provide that substantiation comments submitted by a business to EPA are themselves given *automatic* confidential treatment. *See* 40 C.F.R. § 2.205(c). In a pre-September 11 proposal that is still pending, EPA has proposed to eliminate this automatic confidential treatment for substantiation comments, and instead to subject the comments to the process of preliminary determination, comment, and final determination. *See* 64 Fed. Reg. 57,421 (1999). In light of September 11, EPA should consider withdrawing this proposal.

Another area for administrative action under Exemption 4 is formal acknowledgment and application of the so-called mosaic effect. The mosaic effect recognizes that an individual piece of information, which alone may not qualify as CBI, may be combined with other pieces of information to cause substantial competitive harm. This common-sense approach prevents the piecemeal accumulation of critical security information. With the ubiquitous existence of private information hawkers, finding all of the other pieces is not difficult. Courts have applied the mosaic effect to prevent the disclosure of CBI, *see, e.g., Tinken Co. v. U.S. Customs Service*, 491 F.Supp. 557 (D.D.C. 1980), and Exec. Order No. 12,958 uses the mosaic effect for classified information protected under Exemption 1. OIP should encourage the agencies to consistently apply it under Exemption 4 as well.

One high-profile situation in the environmental arena where Exemption 4 may come into play is EPA’s recent decision to pull from its website portions of Risk Management Plans (RMPs) once thought innocuous. *See* [www.epa.gov/ceppo/review.htm](http://www.epa.gov/ceppo/review.htm), visited Dec. 10, 2001 (“RMP files that do not contain [off-site consequences analysis] information have been temporarily removed by EPA from its website in light of the Sep-

tember 11 [attacks]. EPA is reviewing the information we make available over the Internet and assessing how best to make the information publicly available. We hope to complete that effort as soon as possible.”).

Under Clean Air Act § 112(r), certain private facilities must submit RMPs to EPA. RMPs provide information about regulated substances used at a facility, including a hazard assessment, a release prevention plan, and an emergency response plan—types of information that seem obviously relevant to homeland security. A particularly sensitive piece of an RMP is the off-site consequences analysis (OCA) that describes worst-case accident scenarios.

Clean Air Act § 112(r) requires that RMPs be made available to the public pursuant to Section 114(c) of the Act. EPA initially proposed to carry out this disclosure provision by posting RMPs, including OCAs, on its website. EPA’s electronic access proposal prompted a firestorm of protest, including from law enforcement and intelligence agencies that argued that OCA information would assist would-be terrorists in targeting U.S. facilities.

Ultimately, Congress stepped in and added a new subsection (H) to Section 112(r) that specifically addressed the public availability of OCAs. *See* Chemical Safety Information, Site Security and Fuels Regulatory Relief Act, Pub. L. No. 106-40, 113 Stat. 207 (1999). EPA issued its implementing regulations on August 4, 2000. *See* 65 Fed. Reg. 48,107 (2000).

Detailed discussions of the new subsection (H) and EPA’s implementation of it are beyond the scope of this article. In general, the new rules provide for various levels of access to certain OCA information. Under the rules, the most sensitive information is available for review in paper

form in a limited number of physical reading rooms, while less sensitive information is posted on EPA’s web site along with “non-OCA” RMP information. But, in the wake of September 11, EPA pulled *all* RMP information from its website, even non-OCA information not subject to subsection (H). Many are complaining about this move, characterizing it as a backdoor way to protect industry from embarrassing and indicting information. EPA is now faced with the unenviable job of having to strike the difficult balance between the need for citizens to know about the facilities in their back yards and the need to protect those facilities from a terrorist threat.

Exemption 4 may play into the analysis regarding non-OCA RMP information not subject to the new subsection (H) or EPA’s regulations implementing it. As mentioned above, RMPs are to be released to the public “under section 7414(c)” of the Act. That section explicitly requires the withholding of certain competitively

---

*The CIISA has been severely criticized as creating a major new loophole to FOIA’s right of public access.*

---

valuable information, namely “methods or processes entitled to protection as trade secrets.” One could argue that this “trade secret” exception is not as broad as CBI under Exemption 4, but EPA has not historically interpreted Section 114(c) that narrowly.

EPA struggled with the meaning of this phrase when developing its initial regulations implementing Section 114(c). Ultimately, EPA concluded that Section 114(c) protects a broader class of business information than the narrow phrase “methods or processes entitled to protection as trade secrets” may at first suggest. The regulations, now found at 40 C.F.R. Part 2, Subpart B, were based on an understanding that Section 114(c) protects “data which in many cases businesses regard as confidential, such as operating costs, profits and losses, details of transactions with others, plans for capital investment, marketing information, proposed new products, input and output rates, and similar information.” 40 Fed. Reg. 21,987, 21,990 (1975) (proposed rule); 41 Fed. Reg. 36,902 (1976) (final rule).

This broad interpretation of Section 114(c) seems to be consistent with the language of Section 114(c) and the legislative history of the Clean Air Act Amendments of 1970. Section 114(c) specifically references the Trade Secrets Act (TSA), a statute with a sweeping disclosure prohibition. Moreover, the legislative history of the Clean Air Act Amendments of 1970 indicates that Congress intended Section 114(c) to protect from disclosure the same information that falls within the scope of the TSA. *See* S. REP. NO. 91-1196, at 19 (1970).

How EPA will resolve the issue of RMPs, and whether Exemption 4 will play a role, is still uncertain.

### *Exemption 3: The Critical Infrastructure Information Security Act of 2001*

An additional basis being considered for use in protecting homeland security information is Exemption 3. Exemption 3 protects information “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.” 5 U.S.C. § 552(b)(3). The Critical Infrastructure Information Security Act of 2001 (CIISA), S.1456, was introduced in the Senate on September 24, 2001, by Senators Robert Bennett (R-UT) and Jon Kyl (R-AZ) in an attempt to use Exemption 3 to protect certain homeland security information.

The stated purpose of the CIISA is to “facilitate the security of the critical infrastructure of the United States, to encourage the secure disclosure and protected exchange of critical infrastructure information, to enhance the analysis, prevention, and detection of attacks on critical infrastructure, to enhance the recovery from such attacks, and for other purposes.”

To effectuate this “protected exchange,” the CIISA exempts from disclosure under FOIA “critical infrastructure information that is voluntarily submitted” to one of thirteen covered federal agencies (including EPA). The CIISA has been severely criticized as creating a major new loophole to FOIA’s right of public access. But whether the CIISA’s disclosure exemption is either “new” or “major” is subject to debate. In fact, much, if not all, of the information that falls within the ambit of the CIISA may be protected already by Exemption 4.

Significantly, the CIISA protects only “voluntarily” submitted critical infrastructure information. This sounds very similar to “voluntarily” submitted commercial or financial information protected by the *Critical Mass* interpretation of Exemption 4. Given that information is generally considered “commercial or financial” under Exemption 4 if it simply relates to a business or trade, *see FOIA Guide* at 165, the CIISA seems to address a subset of Exemption 4 business information. The only difference is that, under *Critical Mass*, “voluntarily” submitted information is considered “confidential” only if it is not the type of information that the business would normally provide to the public. But this public availability limitation may be built into the CIISA, which notes that critical infrastructure information is in fact “not normally in the public domain.”

Thus, the CIISA’s definition of “voluntary” is a critical facet of the bill. Under the proposed legislation, voluntary means the “submittal of the information or records in the absence of an agency’s exercise of legal submission.” DOJ’s OIP reads the term “voluntary” to mean essentially the same thing in the Exemption 4 and *Critical Mass* context. OIP says that an information submission is voluntary unless the collecting agency actually exercises its valid authority to collect the information. *See FOIA Guide* at 174.

So why the debate? Why does the CIISA itself find that “Federal law provides no clear assurance that critical infrastructure information voluntarily submitted to the Federal Government will be protected from disclosure or misuse”? One reason may be that the *Critical Mass* test for voluntarily submitted business information has not been adopted by all federal circuits and has not been incorporated into all federal agencies’ CBI regulations. Perhaps it should be—or perhaps in essence it will be for infrastructure information if the CIISA is enacted.

As America learned on September 11, terrorism is real and in our backyard. No less real is the current war against terrorism. On the information front of that war, government agencies are struggling to balance the important functions served by the public’s access to information with the well-recognized need for domestic security. In the end, the tug of war between disclosure and protection—whether taking place in a court, before Congress, or in an executive agency—may be as important to our democracy as the result itself. 