

Critical Infrastructure Information: The Statutory Regime Protecting Voluntary Disclosure

According to the U.S. government, over 80% of the nation's critical infrastructure assets are owned by private interests. In order to formulate a plan to protect these assets, the Department of Homeland Security IAIP Directorate will require unparalleled cooperation and disclosure from these private entities. At the outset, IAIP will look for all private owners of critical infrastructure assets to voluntarily share information and analysis relating to the potential vulnerabilities of these assets.

Prior to the passage of the HSA, a serious obstacle impeded this cooperation. Under the Freedom of Information Act (5 U.S.C. § 552 as amended by Pub.L. No. 104-231, 110 Stat. 3048) ("FOIA"), the federal government is required to eventually make available to the public most information it gathers. The potential application of FOIA to critical infrastructure information concerned all parties involved. Security professionals in the government were concerned that making such information public could aid terrorists plotting attacks against critical infrastructure assets. At the same time, the owners of these assets worried that making all of the data they supplied to the federal government publicly available could put them at a competitive disadvantage.

The HSA addressed these concerns by creating a specific statutory FOIA exemption for voluntarily submitted critical infrastructure information. This law is known as the Critical Infrastructure Information Act ("CIIA") of 2002.¹ It meets the two-part test for a FOIA Section (b)(3) exemption since the CIIA (1) specifically identifies the type of information covered, and (2) leaves DHS no discretion on whether to withhold covered information. At its heart, the CIIA provides that "Critical Infrastructure Information" voluntarily submitted to a "covered Federal agency" shall be exempt from disclosure under FOIA. 6 U.S.C. § 133. As the law is currently written, the exemption is broad and permissive and should easily cover the vast bulk of information submitted to IAIP. Indeed, in the Supplementary Information to the Department's proposed rules for handling critical infrastructure information, IAIP states that they will rely "upon the discretion of the submitter as to whether the volunteered information meets the definition of critical infrastructure information." Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 18,524 (proposed Apr. 15, 2003) (to be codified at 6 C.F.R. pt. 29). Further, while DHS appears to be the only "covered Federal agency" at this time, the proposed rules clearly state that information submitted to another federal agency with the direction that it be subsequently submitted to DHS as critical infrastructure information will be protected by the CIIA. *See id.* at 18,527.

The CIIA's coverage does not stop there. The law also directs that such voluntarily submitted information shall not be subject to any agency rules or judicial doctrine on *ex parte* communication with a decision-making official. 6 U.S.C. § 133(a)(1)(B). So long as the information is submitted in good faith (*i.e.*, not submitted merely to hide it within this privilege), the information may not be used by any federal, state or local authority or any third party in any civil action, unless the submitting party gives its

If you have any questions or would like any assistance regarding the matters discussed in this memorandum, please contact the following attorneys or your call your regular Skadden contact.

Leonard Rawicz
Washington, D.C.
202.371.7001

Joseph Beach
Washington, D.C.
202.371.7879

* * *

This memorandum is provided by Skadden, Arps, Slate, Meagher & Flom LLP and its affiliates for educational and informational purposes only and is not intended and should not be construed as legal advice. This memorandum may be considered advertising under applicable state laws.

written consent. *Id.* at § 133(a)(1)(C). To further protect this information while in government hands, it may not be used or disclosed by any officer or employee of the federal government, including contractors, for purposes other than homeland security² without the submitter's consent, except in the case of criminal investigations or disclosure to Congress or the comptroller general. *Id.* at § 133(a)(1)(D). Further, while DHS has authority to share this information with state and local governments, those governments are forbidden to disclose such shared information or use for any non-homeland security purpose except for criminal investigations. *Id.* at § 133(a)(1)(E). While the protection of the CIIA clearly flows down with information submitted to the federal government and later shared with state and local governments, *see* Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 18,524, 18,528 (proposed Apr. 15, 2003) (to be codified at 6 C.F.R. pt. 29), there is no indication that the reverse is true. While later rules may alter the landscape, the current proposed rules do not cover Critical Infrastructure Information submitted to state and local governments and shared by those governments with DHS. A more interesting but cloudy issue is whether information first disclosed to state and local governments, and later voluntarily disclosed to DHS by the private entity, will retroactively qualify for the protections of the CIIA. A strict reading of the statute would appear to argue against such protection, but there may be enough ambiguity in the statute for DHS to mandate a different outcome in its rules. Finally, voluntary disclosure of critical infrastructure information to DHS shall not constitute waiver of any applicable privilege or protection, including trade secret protection. 6 U.S.C. § 133(a)(1)(F).

In order to gain the broad protections provided by the CIIA, the disclosing party must ensure it meets all of the pertinent conditions. First, the CIIA only covers disclosure to a "covered Federal agency." At this time, the only such agency is the Department of Homeland Security. 6 U.S.C. § 131(2), but, as mentioned above, DHS's rules allow for information submitted to other federal agencies to be protected so long as the submitter directs that the information be transferred to DHS. Full protection, however, cannot be guaranteed until the information has been received and marked by DHS. Second, the CIIA only protects information that is voluntarily disclosed. While some courts have developed a body of law surrounding the idea of "voluntary submission" under the FOIA trade secrets/business confidential information exemption (FOIA Section (b)(4)), *see, e.g.,* Critical Mass Energy Project v. Nuclear Regulatory Commission, 975 F.2d 871 (D.C. Cir. 1992), this concept is novel in the context of FOIA Section (b)(3). The act defines a "voluntary submission" as a submission without DHS exercising any legal authority to compel access or submission, and a submission that can be accomplished by a single entity acting alone or by a collaborative Information Sharing and Analysis Organization ("ISAO") acting for the single entity. *See* 6 U.S.C. § 131(7). Thus, submissions that require cooperation between asset owners will not be covered unless those owners first band together to create an ISAO. The term "voluntarily" specifically excludes information concurrently submitted for licensing or regulatory proceedings and also excludes information filed with the Securities and Exchange Commission. The CIIA and proposed rules are silent, however, as to the treatment of information submitted in connection with a government procurement.

2 Judging from the proposed rules, these purposes are "securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstruction, or for another informational purposes related to homeland security." Procedures for Handling Critical Infrastructure Information, 68 Fed. Reg. 18,524, 18,528 (proposed Apr. 15, 2003) (to be codified at 6 C.F.R. pt. 29).

Finally, the law requires that information submitted under the CIIA be accompanied by the following "express statement" claiming these protections: "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." 6 U.S.C. § 133(a)(2)(A).

In the event that the disclosure in question was made orally, the protections of the CIIA will apply so long as the initial disclosure is followed within 15 calendar days by this written express statement. Even though this requirement may appear to be pro forma, there is every reason to believe that it will be enforced to the letter. In a recent case, the Federal Circuit Court of Appeals ruled that a contractor who failed to stamp every page of its unsolicited proposal as required by applicable regulation with the required restrictive legend thereby forfeited all protection against disclosure. *See Xerxe Group, Inc. v. United States*, 278 F.3d 1357 (Fed. Cir. 2002). In light of this decision, submitters must precisely follow the instruction in the law, as well as any forthcoming regulations, concerning the use of the required "express statement."

On the other hand, it is important to note that the exemption mandated by this act invokes only one of many FOIA exemptions. If critical infrastructure information were submitted and not granted the protection of this act, it is still possible for the IAIP Directorate to argue that it should be withheld from disclosure under another of the FOIA exemptions. For example, the Federal Energy Regulatory Commission ("FERC") has promulgated formal rules regarding the treatment of information that it determines to be "Critical Energy Infrastructure Information." According to FERC's analysis, this information will be exempt from disclosure by the operation of FOIA Section (b)(2) (exemption for agency personnel rules and practices), Section (b)(4) (trade secrets and commercial information), and/or Section (b)(7) (law enforcement information). Which exemption will apply will be determined on a case-by-case basis. *See Order No. 630, Critical Energy Infrastructure Information*, 68 Fed. Reg. 9,857-901 (Mar. 3, 2003). This approach is less preferable for the owners of critical infrastructure assets, however, as the exemption is the government's to claim. The submitter of this information may utilize a reverse FOIA suits to attempt to force the government to apply the exemption. The situation is more certain under the CIIA, however, since disclosure of qualifying information is clearly forbidden. Once qualifying Critical Infrastructure Information has been submitted, the law provides for strict care and custody by DHS. The Department proposed rules envision procedures to cover acknowledgement of receipt, labeling the information as "voluntarily submitted," care and storage, and protection of its confidentiality. *See Procedures for Handling Critical Infrastructure Information*, 68 Fed. Reg. 18,524 (proposed Apr. 15, 2003) (to be codified at 6 C.F.R. pt. 29). These procedures will include the creation of a Critical Information Program administration under the direction of the Critical Infrastructure Information program manager, who will report directly to the undersecretary of Information Analysis and Infrastructure Protection. *See id.* at 18526. This group will determine that submitted information qualifies for protection, mark it accordingly, and oversee the use, dissemination and storage of all protected information. *See id.* at 18,526-29. While there are strict criminal penalties for officers and employees of the federal government who inappropriately disclose submitted information, the CIIA specifically states that there are no new private rights of action to enforce any provision of the act. 6 U.S.C. § 134.