Order Code RL31762

Report for Congress
Received through the CRS Web

Homeland Security Act of 2002: Critical Infrastructure Information Act

February 28, 2003

Gina Marie Stevens
Legislative Attorney
American Law Division

Homeland Security Act of 2002: Critical Infrastructure Information Act

Summary

The Critical Infrastructure Information Act of 2002 ("CIIA"), to be codified at 6 U.S.C. §§131 - 134, was passed on November 25, 2002 as subtitle B of Title II of the Homeland Security Act (P.L. 107-296, 116 Stat. 2135, sections 211 - 215), and regulates the use and disclosure of information submitted to the Department of Homeland Security (DHS) about vulnerabilities and threats to critical infrastructure. This report examines the CIIA. For further information, see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John Moteff. This report will be updated as warranted.

Contents

Homeland Security Act of 2002: Critical Infrastructure Information Act

Background.

The President's National Strategy for Homeland Security, which proposed the creation of a new Department of Homeland Security (DHS), established as one of the Department's core missions the protection of America's infrastructure.[1] The proposal had the new Department responsible for comprehensively evaluating the vulnerabilities of America's critical infrastructure, including food and water systems, agriculture, health systems and emergency services, information and telecommunications, banking and finance, energy (electrical, nuclear, gas and oil, dams), transportation (air, road, rail, ports, waterways), the chemical and defense industries, postal and shipping entities, and national monuments and icons. Working closely with state and local officials, other federal agencies, and the private sector, the proposal had the Department helping to ensure that proper steps are taken to protect high-risk targets. Information sharing between public and private entities about threats and vulnerabilities to critical infrastructures was a central component of the President's proposal which was subsequently introduced by request as H.R. 5005 (Armey), the Homeland Security Act of 2002. Section 204 of H.R. 5005 exempted infrastructure vulnerabilities information from disclosure under the Freedom of Information Act (5 U.S.C. § 552), and stated that "Information provided voluntarily by non-federal entities or individuals that relates to infrastructure vulnerabilities or other vulnerabilities to terrorism and is or has been in the possession of the Department [of Homeland Security] shall not be subject to section 552 of title 5, United States Code."

A debate ensued regarding the exemption of critical infrastructure information from the Freedom of Information Act (FOIA). The debate essentially focused on the reconciliation of two public goods that come into conflict, on the one hand, the need to encourage voluntary information sharing, and on the other, the demands of open government. A new FOIA exemption for critical infrastructure information was opposed by civil libertarians and advocates of open government on several grounds. They testified that a new exemption would jeopardize the ability to obtain information about abusive government practices, would cast a shroud of secrecy over one of the Department of Homeland Security's critical functions, and was unnecessary because FOIA exemption 4 protects private companies against disclosures of trade secrets and confidential business information, and can be extended to critical infrastructure material that properly should be withheld from disclosure.

---

[1] A Legislative Proposal to Create a New Cabinet Department of Homeland Security, H. Doc. 107-227 (June 18, 2002).

Proponents of a new FOIA exemption for critical infrastructure information testified that private industry would be unwilling to voluntarily share critical infrastructure information with the federal government without assurances that its confidential business information would not be released by the government. Companies worried that if information sharing with the government becomes a reality, FOIA requests for information could prove embarrassing and costly. In addition, companies expressed concern that agency decisions about disclosure of business confidential data were fraught with ambiguity and discretion. There were also concerns expressed by private industry about antitrust and civil liability issues with respect to the willingness of some of those entities to provide information voluntarily to the federal government. Specifically, in congressional hearings industry representatives expressed concern about disclosure under the Freedom of Information Act; third-party liability (e.g., sharing suspected problems about a piece of equipment before its being thoroughly tested and verified); the lack of a defined antitrust exemption for appropriate information sharing concerning infrastructure vulnerabilities; possible disclosure of information under state open records laws; and disclosure of sensitive corporate information to competitors.

When H.R. 5005 was reported out of the House Select Committee on Homeland Security after hearings on the legislation, the Administration's FOIA exemption was modified, and new limitations on the use and disclosure of critical infrastructure information were included in a separate subtitle (Title VII, Subtitle C, sections 721 - 724). The Select Committee on Homeland Security significantly expanded upon the President's proposal for an exemption from FOIA for information on infrastructure vulnerabilities. Section 204 of H.R. 5005 was no longer limited to the exemption from disclosure under FOIA of information on "infrastructure vulnerabilities or other vulnerabilities to terrorism." Its protections now extended to a broad and newly defined category of information – *critical infrastructure information* voluntarily submitted to the DHS with an express statement of expectation of protection from disclosure. The reported bill included some of the protections sought by industry representatives: it provided exemption from disclosure under FOIA; it provided that covered information would not be used directly in civil actions; it provided that critical infrastructure information would not be used or disclosed by any Federal employee (except to further criminal investigation or prosecution or to disclose the information to Congress or the General Accounting Office); it established that critical infrastructure information provided to a State or local government by DHS may not be made available pursuant to any State or local law requiring disclosure of information or records; and it provided that communications of critical infrastructure information would not be subject to the requirements of the Federal Advisory Committee Act (FACA).

The Senate Governmental Affairs Committee, too, voted to add a FOIA exemption to its bill, S. 2452 (Lieberman, section 198) establishing a Department of Homeland Security. S. 2452, the National Homeland Security and Combating Terrorism Act of 2002, agreed to by the Senate Governmental Affairs Committee on July 25, 2002, exempted a "record" pertaining to the vulnerability of and threats to critical infrastructure (as defined in the USA PATRIOT Act), furnished voluntarily to the Department of Homeland Security, from being made available under FOIA. A record was protected from disclosure if the provider would not customarily make the record available to the public. It also required the provider to certify, in a manner

specified by the Department of Homeland Security, that the record is confidential and not customarily made available to the public. Under S. 2452 a record is submitted voluntarily if it was submitted to the Department of Homeland Security "in the absence of authority of the Department requiring that record to be submitted," and it is not submitted or used to satisfy any legal requirement or obligation or to obtain any grant, permit, benefit, or other approval from the federal government. Agencies with which the Department of Homeland Security shares protected records were to be bound by the FOIA exemption. FOIA requests for protected information were to be referred back to the Department of Homeland Security. S. 2452 allowed an agency which had received independently of the Department a record "similar or identical" to that received by the Department, to disclose the record under FOIA. The Senate bill did not preempt state or local disclosure laws if the state or local authority received the information independent of the Department of Homeland Security, nor did it contain civil liability immunity, or criminal penalties. Finally, the Senate bill required the Comptroller General to report to Congress on the implementation and use of its protections.

Critical Infrastructure Information Act of 2002.

On November 25, 2002, President Bush signed H.R. 5005, the Homeland Security Act of 2002, P.L. 107-296. The "Critical Infrastructure Information Act of 2002," ("CIIA"), to be codified at 6 U.S.C. § 131 *et seq.*, is found in Subtitle B of Title II of the Homeland Security Act (sections 211 - 215). CIIA consists of a group of provisions that address the circumstances under which the Department of Homeland Security may obtain, use, and disclose critical infrastructure information as part of a critical infrastructure protection program. CIIA establishes several limitations on the disclosure of critical infrastructure information voluntarily submitted to DHS. The CIIA was enacted, in part, to respond to the need for the federal government and owners and operators of the nation's critical infrastructures to share information on vulnerabilities and threats, and to promote information sharing between the private and public sectors in order to protect critical assets. The Homeland Security Act of 2002 adopted sections 721- 725 of H.R. 5005 on critical infrastructure information verbatim. Congress' enactment of the Critical Infrastructure Information Act of 2002 was and continues to be somewhat controversial. The narrower Senate version, S. 2452, was not considered by the full Senate, or the House of Representatives, when Congress enacted the Homeland Security Act on an accelerated schedule. The Homeland Security Act was approved by the House and the Senate expeditiously, with relatively little focus on its FOIA-related provisions. Following is a summary of the new law.

Definitions.

The CIIA includes 4 key definitions: covered federal agency; critical infrastructure information; voluntary; and express statement. Another key definition, critical infrastructure, is defined elsewhere in the Homeland Security Act.

The most important definition in CIIA is that of "critical infrastructure information" because the CIIA protections are triggered only for such information. Critical infrastructures are defined elsewhere in the Homeland Security Act. Section 2(4) of the Homeland Security Act states that *critical infrastructure* "has the

meaning given that term in section 1016(e) of Public Law 107-56 (42 U.S.C. 5195(e))."[2] Section 1016(e) of the USA PATRIOT 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 these matters."[3] This definition is viewed as a broad catch-all provision likely to cover a wide array of activities.

Critical infrastructure information is defined as "information not customarily in the public domain and related to the security of critical infrastructure or protected systems—

> (A) actual, potential, or threatened interference with, attack on, compromise of, or incapacitation of critical infrastructure or protected systems by either physical or computer-based attack or other similar conduct (including misuse of or unauthorized access to all types of communications and data transmission systems) that violates federal, state, or local law, harms interstate commerce of the United States, or threatens public health and safety;
> (B) the ability of critical infrastructure or protected systems to resist such interference, compromise, or incapacitation, including any planned or past assessment, projection or estimate of the vulnerability of critical infrastructure or a protected system, including security testing, risk evaluation thereto, risk management planning, or risk audit; or,
> (C) any planned or past operational problem or solution regarding critical infrastructure...including repair, recovery, reconstruction, insurance, or continuity to the extent it relates to such interference, compromise, or incapacitation."[4]

This definition covers a wide range of information, and is further expanded by reference to the statutory definition of critical infrastructure from the USA PATRIOT Act.[5]

Covered federal agency is defined by the CIIA as the Department of Homeland Security. On the House floor, an amendment to this definition was offered, and failed.[6] Amendment No. 25 would have amended the definition of "covered agency" to include not just the Department of Homeland Security, but any other agency

---

[2] P.L. 107-296, § 2(4), 116 Stat. 2140.

[3] P.L. 107-56, § 1016(e), 42 U.S.C. 5195(e).

[4] P.L. 107-296, § 212(3).

[5] See the "Issues and Concerns" section of CRS Report RL31547, *Critical Infrastructure Information Disclosure and Homeland Security*, by John Moteff and Gina Marie Stevens.

[6] P.L. 107-296, 116 Stat. 2135, § 212(2); *See also id.* at § 214(c) (adding that the provision does not apply to "independently obtained information").

designated by the Department of Homeland Security or with which the Department shares critical infrastructure information.[7]

Another important definition is of *voluntary*. Section 214 of the CIIA protects critical infrastructure information voluntarily submitted to the DHS when accompanied by an express statement of expectation of protection from disclosure. The term "voluntary" with respect to the 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 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"[8] The CIIA defines "Information Sharing and Analysis Organizations" as "any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of– (A) gathering and analyzing critical infrastructure information . . . (B) communicating or disclosing critical infrastructure information . . . and (C) voluntarily disseminating critical infrastructure information . . . ."[9] In addition, the definition of voluntary includes a critical exclusion. A voluntary submission to DHS does not include filings that were also made with the Securities and Exchange Commission or Federal banking regulators, statements made pursuant to the sale of securities, or information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings. Consequently, information falling within the exclusion would not be protected from disclosure.

The last critical definition is of an *express statement*.[10] In order to obtain the protections of the CIIA, the submission must be accompanied by an express statement. In the case of written information or records, this means a written marking on the information or records similar to "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."[11] In the case of oral information, CIIA requires the submission of a similar written statement within a reasonable time period following the oral communication.[12]

Protection of Voluntarily Shared Critical Infrastructure Information.

Section 214 of the CIIA is entitled "Protection of Voluntarily Shared Critical Infrastructure Information." The section establishes several protections for critical infrastructure information voluntarily submitted to the Department of Homeland Security for use regarding the security of critical infrastructures and protected systems and for other purposes when such information is accompanied by an express

---

[7] 148 Cong. Rec. H5845 (July 26, 2002).

[8] P.L. 107-296, § 212(7).

[9] P.L. 107-296, § 212(5).

[10] *See id.* at § 214(a)(2)(A)-(B)

[11] P.L. 107-296, § 214(a)(2).

[12] *Id.*

statement to the effect that the information is voluntarily submitted to the federal government in expectation of protection from disclosure. To encourage private and public sector entities and persons to voluntarily share their critical infrastructure information with the Department of Homeland Security, the CIIA includes several measures to ensure against disclosure of protected critical infrastructure information by DHS. Section 214(a)(1), entitled "In General", provides:

> 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 infrastructures and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement . . . .
>
> (A) "shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act)."[13]

According to the Department of Justice, the agency responsible for administering the FOIA, section 214(a)(1) will operate as a new "Exemption 3 statute"[14] under FOIA for "critical infrastructure" information that is obtained by the Department of Homeland Security.[15] This section eliminates the presumptive right of access by any person—corporate or individual, regardless of nationality— to existing, unpublished DHS records on critical infrastructure information. Unlike FOIA, which specifies nine categories of information that may be exempted from disclosure, and permits rather than requires the withholding of requested information section 214(a)(1)(A) leaves no discretion and requires that critical infrastructure information voluntarily submitted to the DHS not be disclosed under FOIA.

Prior to the enactment of this new FOIA exemption 3 statute, critical infrastructure information would have fallen under the scope of exemption 4 of FOIA which exempts from disclosure "trade secrets and commercial or financial information obtained from a person and privileged or confidential."[16] Most exemption 4 cases have involved a dispute over whether the information was "confidential." In 1992, in *Critical Mass Energy Project v. NRC*,[17] the full D.C.

---

[13] P.L. 107-296, 116 Stat. 2135, § 214(a)(1)(A) (to be codified at 6 U.S.C. § 133(a)(1)(A)).

[14] Under exemption 3 of the FOIA, information protected from disclosure under other statutes is also exempt from public disclosure 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. Unlike other FOIA exemptions, if the information requested under FOIA meets the withholding criteria of exemption 3, the information must be withheld. See 5 U.S.C. § 552(b)(3).

[15] Department of Justice, "Homeland Security Law Contains New Exemption 3 Statute," FOIA Post (2003).

[16] 5 U.S.C. § 552(b)(4).

[17] 975 F.2d 871, 879-80 (D.C. Cir. 1992)(*en banc*)(*"Critical Mass II"*), *cert. denied*, 113 S.

(continued...)

Circuit Court of Appeals established a new test to determine confidentiality for information submitted voluntarily to an agency. It ruled that voluntarily submitted information is exempt from disclosure under FOIA if the submitter can show that it does not customarily release the information to the public.[18] The court in *Critical Mass* did not expressly define the two terms "required" and "voluntary" information submissions. The Department of Justice issued policy guidance on the *Critical Mass* distinction under exemption 4.[19] Further guidance of the treatment of confidential business information is found in Executive Order 12,600 (*Predisclosure Notification Procedures for Confidential Commercial Information*).[20]

Similarly, the CIIA protects from disclosure critical infrastructure information "not customarily in the public domain" voluntarily submitted to DHS. The Report of the House Select Committee on Homeland Security accompanying H.R. 5005 states that "The Select Committee intends that subtitle C only protect private, security-related information that is *voluntarily shared* with the government in order to assist in increasing homeland security. This subtitle does not protect information required under any health, safety, or environmental law" (emphasis added).[21] It should be noted that section 214(d) provides that "the voluntary submittal to the Government of information or records that are protected from disclosure by the Act shall not be construed as compliance with any legal requirement to submit such information to a federal agency."

Section 214(a)(1)(B) of the CIIA provides that covered information will not be subject to agency rules or judicial doctrine regarding ex-parte communications. The Administrative Procedure Act (APA) establishes the rules for agencies to adhere to with respect to ex parte communications in agency proceedings.[22] The APA defines an "ex parte communication" as an "oral or written communication not on the public record with respect to which reasonable prior notice to all parties is not given . . ."[23] Section 556(e) of the Administrative Procedure Act incorporates the principle that formal agency adjudications are to be decided solely on the basis of record evidence. It provides that "[t]he transcript of testimony and exhibits, together with all papers and requests filed in the proceeding, constitutes the exclusive record for decision."[24] The reason for this "exclusiveness of record" principle is to provide fairness to the parties in order to ensure meaningfully participation. Challenges to the "exclusiveness of record" occur when there are ex parte contacts – communications

---

[17] (...continued)
Ct. 1579 (1993).

[18] *Id.* at 879.

[19] Department of Justice, "OIP Guidance: The Critical Mass Distinction Under Exemption 4," FOIA Update, Vol. XIV, No. 2, at 3-5.

[20] Exec. Order No. 12,600, 3 C.F.R. 235, *reprinted in* 5 U.S.C. § 552 note.

[21] H. Rep. No. 107-609, Homeland Security Act of 2002, p. 116.

[22] 5 U.S.C. § 551 *et seq.*

[23] 5 U.S.C. § 551(14).

[24] *Id.* at § 556(e).

from an interested party to a decision making official that take place outside the hearing and off the record. Ex parte contact issues arise more frequently in agency adjudications than in judicial proceedings because the latter are almost always made on the record, after an adversary proceeding; however, on the record proceedings are a very small part of the docket in most agency proceedings.

Section 557(d)(1) of the APA prohibits any "interested person outside the agency" from making, or knowingly causing, "any ex parte communication relevant to the merits of the proceeding" to any decision making official. Similar restraints are imposed on the agency decision makers, who are defined to include any "member of the body comprising the agency, administrative law judge, or other employee who is or may reasonably be expected to be involved in the decisional process."[25] When an improper ex parte contact occurs, the APA requires that it be placed on the public record; if it was an oral communication, a memorandum summarizing the contact must be filed.[26] Upon receipt of an ex parte communication knowingly made or knowingly caused to be made by a party in violation of the APA, the agency, administrative law judge, or other employee presiding at the hearing may require the party to show cause why his claim or interest in the proceeding should not be dismissed, denied, disregarded, or otherwise adversely affected on account of such violation.[27] Section 214(a)(1)(B) of the CIIA exempts protected critical infrastructure information from APA prohibitions on ex parte communications.[28]

Section 214(a)(1)(C) of the CIIA creates an evidentiary exclusion for protected information. Section 214(a)(1)(C) prohibits the direct use, without the written consent of the information submitter, of protected critical infrastructure information by such agency (DHS), any other Federal, State, or local authority, or third party in any civil action arising under federal or state law if submitted in good faith. This protection is limited to critical infrastructure information that is voluntarily submitted to a covered federal agency [DHS] for use by that agency regarding the security of critical infrastructure and protected systems . . . or other informational purpose, when accompanied by an express statement. This evidentiary limitation does not apply to regulatory or enforcement actions by Federal, State, or local governmental entities, nor to civil actions when the information is obtained independently of the DHS. The courts may also limit application of the evidentiary exclusion in cases of bad faith. Public interest groups are concerned that this provision is very broad, and would shield owners and operators from liability under antitrust, tort, tax, civil rights, environmental, labor, consumer protection, and health and safety laws. However, a Federal entity may separately obtain the critical infrastructure information submitted to the DHS for its critical infrastructure protection program through the use of independent legal authorities, and use such information in any action.[29] The CIIA

---

[25] 5 U.S.C. § 557(d)(1)(E).

[26] *Id.* at § 557(d)(1)(C).

[27] *Id.* at § 557(D).

[28] For an example of a statute which modifies the APA rules with respect to ex parte communications, see 49 U.S. C. 11324.

[29] Subsection § 214(c) provides: "(c) INDEPENDENTLY OBTAINED INFORMATION-
(continued...)

does not limit the ability of governments, entities, or third parties to independently obtain critical infrastructure information or to use critical infrastructure information for limited purposes.

Section 214(a)(1)(D) of the CIIA prohibits use or disclosure of critical infrastructure information by U.S. officers or employees, without consent, for unauthorized purposes; and authorizes the use or disclosure of such information by such officers and employees in furtherance of the investigation or the prosecution of a criminal act; or for disclosure to Congress or the General Accounting Office. The President's signing statement accompanying the Homeland Security Act of 2002 expressly addressed this provision. It states that "The executive branch does not construe this provision to impose any independent or affirmative requirement to share such information with the Congress or the Comptroller General and shall construe it in any manner consistent with the constitutional authorities of the President to supervise the unitary executive branch and to withhold information the disclosure of which could impair foreign relations, the national security, the deliberative processes of the Executive, or the performance of the Executive's constitutional duties."[30]

This subsection adopts word-for-word the language from provisions of the Privacy Act of 1974 which permit disclosure of personal information maintained by executive branch agencies in systems of records to Congress, and to the General Accounting Office.[31] Similarly, FOIA provides that it is not authority for withholding information from Congress.[32] Several existing federal statutes authorize the disclosure of certain categories of information for the investigation or prosecution of a criminal act. Federal laws protecting government, credit, communications, education, bank, cable, video, motor vehicle, health, telecommunications, children's, and financial information generally carve out exceptions for the disclosure of personally identifiable information to law enforcement officials, and authorize access to personal information through use of search warrants, subpoenas, and court orders.[33]

---

[29] (...continued)
Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.

[30] The White House, Statement by the President on H.R. 5005, the Homeland Secuirty Act of 2002 (Nov. 25, 2002).

[31] *See* 5 U.S.C. § 552a(b)(9 -10)("(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee; (10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office;").

[32] 5 U.S.C. § 552(d).

[33] See CRS Report RL31730, *Privacy: Total Information Awareness Programs and Related* (continued...)

Section § 214(a)(1)(E) of the CIIA specifically mandates that the critical infrastructure information now exempt under the FOIA "shall not, if provided to a State or local government . . . be made available pursuant to any State or local law requiring disclosure of information or records." This statute thus explicitly provides for the "preemption" of state freedom of information laws by federal law.[34] It also prohibits State or local governments from disclosing protected critical infrastructure information provided to them by DHS without written consent of the entity submitting the information; prohibits its use for other than critical infrastructure protection, or the furtherance of a criminal investigation or prosecution.

Section 214(a)(1)(F) of the Act guards against "waiver of any applicable privilege or protection provided under law, such as trade secret protection." Legal protections for trade secrets vary from state to state. According to the Restatement of Torts, § 757, comment b, as adopted by most state laws, "a trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it." Other relevant evidentiary privileges may include the attorney-client privilege.[35]

Section 214(b) of the Act provides that no communication of critical infrastructure information to the Department of Homeland Security pursuant to the CIIA shall be considered an action subject to the requirements of the Federal Advisory Committee Act which requires that the meetings of federal advisory committees serving executive branch entities be open to the public. FACA defines an "advisory committee" as "any committee, board, commission, council, conference, panel, task force, or other similar group, or any subcommittee or other subgroup thereof (hereafter in this paragraph referred to as "committee"), which is - (A) established by statute or reorganization plan, or (B) established or utilized by the President, or (C) established or utilized by one or more agencies, in the interest of obtaining advice or recommendations for the President or one or more agencies or officers of the Federal Government, except that such term excludes (i) any committee that is composed wholly of full-time, or permanent part-time, officers or employees of the Federal Government, and (ii) any committee that is created by the National Academy of Sciences or the National Academy of Public Administration."[36] The FACA also specifies nine categories of information, similar to those in FOIA, that may be permissively relied upon to close advisory committee deliberations.[37]

Prior to passage of the critical infrastructure information provisions, meetings of "Information Sharing and Analysis Organizations" (ISAO) could potentially be subject to FACA's requirements. However, the CIIA expressly authorizes ISAOs to

---

[33] (...continued)
Information Access, Collection, and Protection Laws, by Gina Marie Stevens.

[34] *See also Freedom of Information Act Guide & Privacy Act Overview* (May 2002), at 563-64 (discussing operation of "preemption doctrine" in FOIA context).

[35] See Fed. Evid. Rule 501.

[36] 5 U.S.C. App. 2, § 3(2).

[37] 5 U.S.C. App. 2.

voluntarily submit information to the DHS on behalf of itself or its members with the result being that such information will be protected in material respects under the Act from uses and disclosures unrelated to critical infrastructure protection.[38] The CIIA defines "Information Sharing and Analysis Organizations" as "any formal or informal entity or collaboration created or employed by public or private sector organizations, for purposes of– (A) gathering and analyzing critical infrastructure information . . . (B) communicating or disclosing critical infrastructure information . . . and (C) voluntarily disseminating critical infrastructure information . . . ."[39] For a discussion of information sharing and analysis centers formed by several sectors (e.g., banking and finance, telecommunications, electricity, water, etc.), see CRS Report RL30153, *Critical Infrastructures: Background, Policy, and Implementation*, by John Moteff.

Section 214(e) requires the Secretary of DHS to establish procedures for the receipt, care, and storage of critical infrastructure information not later than 90 days after enactment. The Homeland Security Act took effect 60 days after passage; the legislation was enacted on November 25, 2003. In other words, Secretary Ridge is to establish those procedures no later that February 23, 2003. The Secretary of Homeland Security is to consult with the National Security Council and the Office of Science and Technology Policy to establish uniform procedures. In addition, it appears that these DHS procedures will not be subject to agency notice and comment rulemaking requirements for agency regulations under the APA because the CIIA requires the promulgation of agency procedures, not regulations. Moreover, in other sections of the Homeland Security Act, Congress clearly directed that regulations be promulgated. Presumably it would have done the same here if that is what it sought.

Judicial review of agencies' interpretations of statutes entails a significant element of deference, as the Supreme Court emphasized in *Chevron U.S.A., Inc. v NRDC*.[40] In *Chevron*, the Court prescribed two inquiries that a reviewing court should conduct when reviewing an agency's construction of a statute. The first was whether "Congress has directly addressed the precise question at issue." If so, the court would have to "give effect to the unambiguously expressed intent of Congress." However, if the statute were to prove "silent or ambiguous with respect to the specific issue," the remaining question was whether the agency's answer was "permissible" – or, as the Court phrased it, a "reasonable interpretation." *Chevron*, in effect, creates a presumption applicable to regulatory schemes in which Congress has delegated power to an agency: to whatever extent the statute remains ambiguous, the reviewing court should presume that Congress has delegated to the agency the task of filling in the gap in some reasonable way.

Criminal Penalties.

Section 214(f) contains a provision that makes it a criminal offense for any federal employee to "knowingly . . . disclose[] . . . any critical infrastructure

---

[38] *Id.* at § 212(7)

[39] P.L. 107-296, § 212(5).

[40] 467 U.S. 837 (1984).

information [that is] protected from disclosure" under it, without proper legal authorization.

> "(f) PENALTIES- Whoever, being an officer or employee of the United States or of any department or agency thereof, knowingly publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law, any critical infrastructure information protected from disclosure by this subtitle coming to him in the course of this employment or official duties or by reason of any examination or investigation made by, or return, report, or record made to or filed with, such department or agency or officer or employee thereof, shall be fined under title 18 of the United States Code, imprisoned not more than 1 year, or both, and shall be removed from office or employment."

This provision is similar to the criminal penalties imposed in the Privacy Act,[41] and the Trade Secrets Act.[42]

Whistleblower Protection Act.

A possible concern with the criminal penalty provisions imposed under CIIA is their potential conflict with certain protections provided under the Whistleblower Protection Act (WPA),[43] which protects covered employees from prohibited personnel actions taken because of a protected disclosure.[44] WPA expressly provides that current employees, former employees, or applicants for employment to positions in the executive branch of government in both the competitive and the excepted

---

[41] 5 U.S.C. § 552a (i)(1)(" Criminal Penalties. Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.")

[42] 18 U.S.C. § 1905 (Whoever, being an officer or employee of the United States or of any department or agency thereof, any person acting on behalf of the Office of Federal Housing Enterprise Oversight, or agent of the Department of Justice as defined in the Antitrust Civil Process Act (15 U.S.C. 1311-1314), publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined under this title, or imprisoned not more than one year, or both; and shall be removed from office or employment.").

[43] Codified, as amended, at 5 U.S.C. § 1201 et seq.

[44] 5 U.S.C. § 2302. See CRS Report 97-787, *Whistleblower Protections for Federal Employees*, (May 18, 1998) by L. Paige Whitaker; and CRS Video Tape MM70034, Proposed Department of Homeland Security: Freedom of Information Act Exemptions, Whistleblower Protection Act, and Information Sharing by Gina Stevens, Paige Whitaker, and Elizabeth Bazan. Online Video. (September 25, 2002).

service, as well as positions in the Senior Executive Service, are considered covered employees.[45] WPA protects "any disclosure of information" that the employee "reasonably believes" evidences "a violation of any law, rule, or regulation" or evidences "gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety," if the disclosure is *not* prohibited by law or required to be kept secret by Executive Order.[46] WPA also protects "*any* disclosure" made to the Special Counsel or to the Inspector General of an agency or another employee designated by the head of the agency to receive such disclosures, which the employee "reasonably believes"evidences "a violation of any law, rule, or regulation," or evidences "gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[47] WPA further protects "cooperating with or disclosing information to the Inspector General of an agency, or the Special Counsel, in accordance with applicable provisions of law."[48] WPA provides that the whistleblowing provisions are "not to be construed to authorize the withholding of information from the Congress or the taking of any personnel action against an employee who discloses information to the Congress."[49]

Hypothetically, if a "covered" federal employee discloses protected critical infrastructure information without legal authorization, she would be in violation of CIIA (and, for example, could be fined, imprisoned, and removed from office or employment). That is, since CIIA generally prohibits the disclosure of protected critical infrastructure information, except for the purpose of criminal investigation or prosecution or to disclose protected information to Congress or the General Accounting Office, such a disclosure would subject the "covered" federal employee to criminal sanctions under the CIIA. Moreover, the protections of the CIIA apply "Notwithstanding any other provision of law."[50] Under the WPA, if a "covered" federal employee disclosed protected critical infrastructure information without legal authorization, she would not be protected by WPA if the disclosure was prohibited by law. However, the "covered" federal employee would appear to be protected by WPA, on the condition that such employee made "any disclosure to the Special Counsel, or to the Inspector General of an agency ... which the employee or applicant reasonably believes evidences a violation of any law, rule or regulation," or evidences "gross mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety."[51] Furthermore, she

---

[45] 5 U.S.C. § 2302(a)(2)(B). Legislative branch employees would not fall within this definition.

[46] 5 U.S.C. § 2302(b)(8)(A).

[47] 5 U.S.C. § 2302(b)(8)(B)(*emphasis added*).

[48] 5 U.S.C. § 2302(b)(9)(C).

[49] 5 U.S.C. § 2302(b).

[50] P.L. 107-296, § 214(a)(1).

[51] 5 U.S.C. § 2302(b)(8)(B).

would appear to be protected "from the taking of any personnel action against an employee who discloses information to Congress."[52]

In addition, it should be noted that Section 883 of the Homeland Security Act (P.L. 107-296), to be codified at 6 U.S.C. § 463, expressly provides that "Nothing in this Act shall be construed as exempting the Department [of Homeland Security] from requirements applicable with respect to executive agencies ... (2) to provide whistleblower protections for employees of the Department (including pursuant to the provisions in section 2302(b)(8) and (9) of such title."[53]

Congressional Disclosure.

Another issue that has been raised with respect to the criminal penalties provision in section 214(f) of the CIIA which applies to "an officer or employee of the United States" is whether Members of Congress and their staff could be criminally liable for the release of protected critical infrastructure information. The CIIA does not include a definition of "officer or employee of the United States." Section 214(C) of CIIA prohibits without written consent the use or disclosure of protected information by any officer or employee of the United States for unauthorized purposes except when disclosure would be for criminal prosecution or investigation, to Congress, or to GAO presumably for purposes of oversight. The Report of the Select Committee on Homeland Security on H.R. 5005, the Homeland Security Act, states that "unauthorized disclosures of critical infrastructure information by *any* U.S. employee may be punished by fines, imprisonment up to one year, and removal from employment."[54]

In light of the fact that the underlying purpose of the CIIA is to promote voluntary information sharing on threats and vulnerabilities to critical infrastructure through the establishment of a statutory scheme designed to protect against unauthorized disclosures of confidential business information, it is arguable that the criminal penalties for unauthorized disclosure of protected information were intended to apply to Congress. However, if Congress had thought it was including itself, then disclosure from "an officer or employee of the United States" to Congress might arguably not be a "disclosure" at all, just information shared between one officer of the United States and another officer of the United States, and one could argue that the exception permitting disclosure to Congress wouldn't have been necessary.

Another consideration that supports the conclusion that Congress is not subject to the criminal penalty provision is the fact that one of the penalties is "removal from employment." This argues against the provision applying to Congress, since a

---

[52] 5 U.S.C. § 2302(b).

[53] P.L. 107-296, § 883. For information on the DHS Inspector General's reporting requirements to Congress, *see* CRS Report RS21251, *Analysis of President's Proposal Concerning the Office of Inspector General for the Proposed Department of Homeland Security*. *See also* Homeland Security Act of 2002 Amendments, Sec. 104 (Inspector General of the Department of Homeland Security) in the H. Conference Rep. on H.J.Res. 2, Consolidated Appropriations Resolution, 2003, 149 Cong. Rec. H846 (Feb. 12, 2003).

[54] H.Rept. 107-609, Part 1 at 116.

Member of Congress cannot be removed by statutory fiat, but only by the Constitutional process set out in Article I, Section 5 of the Constitution, that is, expulsion. Even though the plain meaning of "an officer or employee of the United States" could reasonably be interpreted to include Members of Congress, the Supreme Court had interpreted 18 U.S.C. 1001, prohibiting false statements in any matter before any agency or department of the United States, as not applying to Congress or the courts after more than 40 years of applying it to statements before some congressional entities.[55] Congress had to amend it to expressly include Congress.[56] In light of the *Hubbard* precedent it would appear unlikely that the term "officer or employee of the United States" would be construed by a court as applying to Congress without more definitions or legislative history.

Moreover, the Speech or Debate clause of the U.S. Constitution prevents criminal prosecution of a Member of Congress for what she says on the floor, or during committee proceedings. Members of Congress have immunity for their legislative acts under Article I, § 6, cl. 1, of the Constitution, which provides in part that "for any speech or debate in either House, [Senators and Representatives] shall not be questioned in any other place." Even if the actions of a Senator or Representative are within the scope of the speech or debate clause or some other legal immunity, he remains accountable to the House of Congress in which he serves and to the electorate. The clause protects a Member when speaking on the House or Senate floor, introducing and voting on bills and resolutions, preparing and submitting committee reports, acting at committee meetings and hearings, and conducting investigations and issuing subpoenas.[57] In a frequently quoted description of the scope of the privilege, the Court in *Gravel v. United States*,[58] explained that, in addition to actual speech or debate in either House, the clause applies only to acts which are "an integral part of the deliberative and communicative processes by which Members participate in committee and House proceedings with respect to the consideration and passage or rejection of proposed legislation or with respect to other matters which the Constitution places within the jurisdiction of either House."[59] In addition, the "Speech or Debate Clause applies not only to a Member but also to his aides insofar as the conduct of the latter would be a protected legislative act if performed by the Member himself."[60]

---

[55] *Hubbard v. U.S.*, 514 U.S. 695 (1995).

[56] See CRS Congressional Distribution Memo CD953350, "Impact of United States v. Hubbard, 115 S.Ct. 1754 (1995), on the Prosecution of False Statements Made in Matters of Concern to the Judiciary and the Congress" (July 13, 1995).

[57] See CRS Report RL30843, *Speech or Debate Clause Constitutional Immunity: An Overview*, by Jay Shampansky.

[58] 408 U.S. 606 (1972).

[59] *Id.* at 625.

[60] *Id.* at 618.

Other Provisions.

Section 214(g) of the CIIA authorizes the federal government to provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential threats to critical infrastructure. In issuing a warning, the federal government must protect from disclosure the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning, or information that is proprietary, business sensitive, or otherwise not appropriately in the public domain.

Section 215 of CIIA expressly provides that a private right of action for enforcement of the Act is not created. Many federal statutes contain a private right of action, usually express but occasionally implied, which authorizes suits against the United States.