

Public Citizen and Freedom of Information Clearinghouse.txt
Subject: Comments on Proposed Regulations
Date: Mon, 16 Jun 2003 09:46:46 -0400
From: "Michael Tankersley" <tankers@citizen.org>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Attached are the comments of Public Citizen and the Freedom of Information Clearinghouse in the proposed procedures for managing CII

Michael Tankersley
Public Citizen Litigation Group
1600 20th Street, NW
Washington, DC 20009
tankers@citizen.org

dhs_ciirule_pccomments.PDF Name: dhs_ciirule_pccomments.PDF
 Type: Acrobat (application/pdf)
 Encoding: base64
 Description: dhs_ciirule_pccomments.PDF

COMMENTS OF PUBLIC CITIZEN, INC. AND THE FREEDOM OF INFORMATION CLEARINGHOUSE ON THE DEPARTMENT OF HOMELAND SECURITY'S PROPOSED REGULATIONS IMPLEMENTING THE CRITICAL INFRASTRUCTURE INFORMATION ACT OF 2002

Public Citizen and the Freedom of Information Clearinghouse submit these comments regarding the Department of Homeland Security's proposed rules for implementing a subtitle of the Homeland Security Act that is known as the Critical Infrastructure Information Act of 2002. *See* Pub. L. 107-296, § 211-215, 116 Stat. 2150 (2002) (codified at 6 U.S.C. § 131-34) and 68 Federal Register 18525 (April 15, 2003).

Interests of Public Citizen and the Clearinghouse

Public Citizen and the Freedom of Information Clearinghouse have a longstanding commitment to enhanced public access to government-held information. We submit these comments to ensure that the agency's regulations do not create barriers to the use and disclosure of critical infrastructure information that are not authorized by law. Public Citizen, founded by Ralph Nader in 1971, is a non-profit consumer advocacy organization with over 120,000 active supporters nationwide. From its founding, Public Citizen has regularly used the FOIA to request records related to its advocacy efforts and has represented FOIA requesters in approximately 300 lawsuits challenging government secrecy.

The Freedom of Information Clearinghouse is a project of Ralph Nader's Center for Study of Responsive Law, directed by a Public Citizen lawyer. The Clearinghouse has provided technical and legal assistance since 1972 to individuals, public interest groups, and the media who seek access to information held by government agencies.

Comments on Proposed Regulations

Private parties have information about the vulnerabilities of critical infrastructure systems, such as computer networks, water supplies, public health systems, and power grids. The government already obtains such “critical infrastructure information” through a variety of means, but in the interest of encouraging voluntary submission of additional information to the Department of Homeland Security (“DHS”), the Critical Infrastructure Information Act of 2002 imposes three significant restrictions on the use and disclosure of information that qualifies for protection under the Act: (i) the information is exempt from the Federal Freedom of Information Act and similar legal standards that would otherwise require governmental entities to disclose what they have been told; (ii) neither Federal, State or local government authorities, nor third parties may directly use the information in any civil action; and (iii) Federal officers or employees who knowingly divulge the information in a manner not authorized by law are subject to criminal penalties. 6 U.S.C. § 133(a)(1), (b), (f).

These restrictions are likely to prevent the public and governmental authorities from being able to obtain and make use of important information about avoidable risks, violations of legal requirements, hazards to public safety that should be regulated, and other matters. Consequently, the procedures implementing the statute should ensure that restrictions are only imposed on information that is covered by the statute. Extending the restrictions to information that is *not* covered by the Act, or creating ambiguity about whether information is covered by the Act, would undermine all laws that depend on the availability of such information, including the Homeland Security Act itself.

Significant changes should be made to the proposed regulations that DHS promulgated on April 15, 2003 because the regulations depart from the limitations imposed by the statute and would discourage the lawful use of critical infrastructure information. The substantive standards defining when information is protected under the Critical Infrastructure Information Act of 2002 (“CII Act”), and the consequences of that protection, are defined by the statute. Although the Act provides that the Secretary shall establish procedures concerning “the receipt, care and storage” of critical infrastructure information (“CII”) that is voluntarily submitted to DHS, 6 U.S.C. § 133(e)(1), this authority does not give the Secretary the power to expand the types of information that are protected by the CII Act or to alter limitations set forth in the statute. As described below, in several key provisions, the proposed regulations misstate the scope of the statute by suggesting that the law restricts the use of information that, in fact, is not protected by the statutory provisions.

In addition, the proposed regulations need to be revised because they are internally inconsistent on several critical issues. The regulations also fail to require that submitters substantiate claims that information meets the requirements for protection under the statute, and do not provide a mechanism to promptly remove Protected CII labels whenever it is revealed that the information does not qualify for protection.

These comments identify nine specific areas in which the proposed regulations are inconsistent with the statute or need to be amended because crucial provisions are missing:

1. The Proposed Regulations Erroneously State That the CII Act Restricts Information That Is Obtained by Authorities Independent of Submissions Under the Act. 4

2.	The Proposed Regulations Improperly State That Information Submitted ‘Indirectly’ to DHS Is Eligible for Protection.	7
3.	The Proposed Regulations Fail to Distinguish and Properly Manage Protected CII and Unprotected Information When Both Appear in the Same Record.	9
4.	The Proposed Regulations Improperly Suggest That the CII Act Protects Information If DHS Has Not Determined That the Information Meets the Requirements of the Statute.	11
5.	The Proposed Regulations Should Clearly State the Authority of Government Officials to Use Protected CII.	14
6.	The Proposed Regulations Overstate the Extent to Which the Database Tracking CII Submissions Is Protected.	17
7.	The Proposed Regulations Should Be Amended to Allow Any Interested Party to Request Review of Whether Information Marked Protected Qualifies under the Act.	18
8.	The Proposed Regulations Should Be Amended to Require Submitters to Verify That Submissions Satisfy the Requirements for Protection under the CII Act.	19
9.	The Proposed Regulation Concerning Destruction of Submissions That Do Not Qualify as CII Misstates the Law.	22

The last section of these comments identifies some miscellaneous inconsistencies in the proposed regulations (p. 24).

1. The Proposed Regulations Erroneously State That the CII Act Restricts Information That Is Obtained by Authorities Independent of Submissions Under the Act.

The Critical Infrastructure Information Act of 2002 indicates that Congress only intended to restrict the use of CII that was voluntarily submitted to the Department of Homeland Security for certain specified purposes. Subsection 214(a)(1) describes the types of submissions to DHS that will receive protection, 6 U.S.C. § 133(a)(1), and other provisions emphasize that the

restrictions set forth in the Act do *not* apply to information obtained when the Department exercises its legal authority to obtain information, or when other governmental entities or private parties obtain information through *any* means other than a voluntary submission of CII to the Department.

Section 214(c) of the statute underscores this limitation:

INDEPENDENTLY OBTAINED INFORMATION- 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.

6 U.S.C. § 133(c). Significantly, this statutory language does not distinguish between information that another governmental authority obtains by exercising its legal authority to compel disclosure and information that it obtains without exercising such authority, such as information that is voluntarily disclosed or that an agency discovers through its own investigation. Information that governmental authorities obtain in *any* manner that is independent of the voluntary submissions to DHS described in 6 U.S.C. § 133(a)(1) is not restricted by the CII Act.

The proposed regulations are not faithful to this statutory language. For example, proposed § 29.3(d) is entitled “Independently obtained information,” but the proposed language differs from the statutory provision quoted above because it provides that the procedures “shall not be construed to limit or in any way affect the ability of a Federal, State, or local Government entity, agency, or authority, or any third party, under applicable law, *to obtain information by means of a different law, regulation, rule, or other authority.*” (italics added) The italicized

language suggests that DHS would require Federal, State and local authorities to restrict access to information that they obtain without invoking a law, regulation rule or other authority. To restrict the use of information that these authorities obtain through voluntary submission or their own investigation could thwart their ability to carry out their governmental responsibilities and interfere with public access. Most importantly, extending the restrictions of the CII Act to such information is contrary to the Act.

Other provisions of the regulations contain similar errors. For example, proposed § 29.3 states:

(a) Freedom of Information Act access and mandatory submissions of information.

The CII Act of 2002 and these procedures do not apply to or affect any requirement pertaining to information *that must be submitted* to a Federal agency or pertaining to the obligation of any Federal agency to disclose *such information* under the Freedom of Information Act. Similarly, the CII Act of 2002 and these procedures do not apply to any information *that is submitted to a Federal agency pursuant to any legal requirement*.

(italics added). Because this proposed regulation identifies the information that is not subject to the restrictions of the CII Act as information that “must be submitted” or is submitted pursuant to a “legal requirement,” DHS is erroneously implying that information that agencies obtain through other means would be exempt from the FOIA and that the agency’s own ability to use such information is circumscribed by the CII Act. The CII Act does not impose such restrictions, and DHS is not authorized to create such restrictions by regulation.

The language of proposed § 29.3(d) should be amended to conform to 6 U.S.C. § 133(c), and proposed § 29.3(a) should be completely rewritten to make clear that the restrictions imposed by the CII Act, including the exemption from the FOIA, apply only to information that satisfies all of the requirements of 6 U.S.C. § 133(a)(1).

2. The Proposed Regulations Improperly State That Information Submitted “Indirectly” to DHS Is Eligible for Protection.

The CII Act contemplates that the ability to receive voluntary submissions seeking the special protections of the Act will be limited to certain specially-designated subdivisions of DHS. In particular, the statute defines “critical infrastructure protection program” as any component or bureau of the DHS “that has been designated by the President or any agency head to receive critical infrastructure information.”⁶ U.S.C. §§ 131(4), 132.

The proposed regulations authorize a significantly different procedure in which private submitters could seek CII Act protection for information that was not submitted to a designated component of DHS, but submitted *indirectly* to DHS through other Federal agencies. *See* Proposed § 29.2(i). The failure of the proposed regulations to conform to the statute on this issue is evident from the fact that the proposed regulations contain a definition of “Critical Infrastructure Information Program” that is entirely different from the statutory definition quoted above, and the proposed regulations do not provide for limiting receipt of CII to designated DHS components.¹

Instead of following the CII Act, the proposed regulations would create a burdensome process in which other Federal agencies that will receive submissions seeking protection under the CII Act, will forward the submissions to DHS, and will retain a copy of the submission -- but will be barred from distributing or disseminating the information pending a determination of its status by the CII Program Manager. Proposed § 29.6(d)(2).

¹ The proposed regulations define Critical Infrastructure Information Program as “the maintenance, management, and review of these procedures and of the information provided to DHS in expectation of the protections provided by the CII Act of 2002.” It is not clear what, if any, role this definition serves in the proposed regulations.

These provisions purport to impose an obligation on other Federal agencies to restrict disclosure of indirect submissions that are awaiting review by DHS that is greater than agencies' obligations with respect to Protected CII received from DHS. Under the proposed regulations, an agency cannot even disseminate proposed-CII information for the purposes authorized by the CII Act until there has been a determination that it qualifies as Protected CII. *See* 6 U.S.C. § 133(a)(1)(D) (authorizing agencies to use Protected CII for purposes of homeland security, for investigation or prosecution of a criminal act, and for disclosures to Congress). For example, if a Federal agency receives information that would assist in a criminal investigation and the information is accompanied by a request that it be forwarded to DHS as Protected CII, under the proposed regulations the agency would be prohibited from making *any* use of the information until the CII Program Manager "has acknowledged and validated the information." Proposed § 29.5(d)(2). There is no limitation on how long the Program Manager may take to complete the acknowledgment and validation process, and the process may be protracted and time consuming if it requires further communications with a submitter who is making a questionable claim that the information that it has submitted is entitled to protection. *See* Proposed § 29.6 (providing, among other things, for a thirty day period for submitter to respond to Program Managers' notice questioning whether information meets the requirements for Protected CII).

The CII Act does not authorize the DHS to create such impediments to Federal agencies' use or disclosure of information that they receive from sources other than DHS. The Act provides only for protection of information "that is voluntarily *submitted to a covered Federal agency for use by that agency*" for certain purposes listed in the statute. 6 U.S.C. § 133(a)(1). DHS is the only "covered Federal agency" and, as discussed above, the statute contemplates that

only designated components of DHS would be authorized to receive CII. The statute does not authorize indirect submissions through other Federal agencies, and information tendered for the use of an agency other than DHS would not qualify for protection under the Act. Moreover, the proposed regulations do not identify any reason why other Federal agencies should be used as a conduit for forwarding information to DHS, instead of requiring that all submissions seeking the protection of the CII Act be submitted directly to DHS. Indeed, the very fact that information is submitted to an agency other than DHS suggests that the submitter has a reason for that agency to have the information *independent* of the voluntary submission of CII to DHS. The CII Act is not intended to place restrictions on information that would independently be submitted to other federal agencies.

Consequently, DHS should delete the portion of the proposed regulations that defines “Submission to DHS” to include information provided “indirectly via another Federal agency,” Proposed § 29.2(i), and the provisions in proposed § 29.5 that discuss forwarding information and indirect submissions. These provisions are not authorized and would create a burdensome and unnecessary procedure that will only promote confusion concerning what information is protected.

3. The Proposed Regulations Fail to Distinguish and Properly Manage Protected CII and Unprotected Information When Both Appear in the Same Record.

In the context of the FOIA and other laws in which restrictions are placed on the disclosure of certain types of information, there is an important distinction between “information” and “records.” If certain information in a record is protected, it does not follow that the entire record receives the same protection. Instead, the record should be released after

deleting the portions that contain the protected information. *See, e.g., Environmental Protection Agency v. Mink*, 410 U.S. 73, 90 (1973); *Rugiero v. United States Department of Justice*, 257 F.3d 534 (6th Cir. 2001); *Mead Data Central, Inc. v. United States Dept. of Air Force*, 566 F.2d 242, 259 (D.C. Cir.1977); 6 C.F.R. § 5.11(b)(7) (review under FOIA includes redacting records for disclosure); 32 C.F.R. § 286.23(d) (describing obligation to segregate information).

The CII Act provides for the protection of certain “information,” not the protection of entire records that have some protected information within them. 6 U.S.C. § 133(a)(1). The proposed regulations, however, are not consistent with the statute. Instead, DHS’s proposed regulations state that “CII consists of records or information” concerning various topics. *See* Proposed § 29.2(b). The reference to “records” should be removed from the proposed regulations.

More importantly, the proposed regulations should provide procedures for segregating information so that the use and dissemination of unprotected information is not restricted. The information that a submitter claims qualifies as Protected CII should be identified and segregated at the time of the initial submission, and further segregation should occur if it is later determined that only part of the information labeled as Protected CII actually satisfies the statutory requirements for protection. The serious penalties imposed for disclosure of Protected CII magnify the importance of ensuring that government officials know which information may be used in carrying out their official duties, and which information may only be used for limited purposes because of the CII Act.²

² The proposed regulation on “validation” states that the Program Manager’s initial determination may result in a decision “that some or all” of the information does not meet the requirements for protection, but this clause is the only provision that recognizes that the presence

Accordingly, DHS should add to the regulations provisions on segregating information that are analogous to those found in the regulations of Federal agencies that require a submitter to separate protected and unprotected information when the submitter asserts that information is entitled to confidential treatment. *See, e.g.*, 12 C.F.R. § 261.15(c) (Federal Reserve Board); 17 C.F.R. § 200.83(c) (Securities and Exchange Commission); 49 C.F.R. § 512.4(a) (Department of Transportation); 10 C.F.R. § 2.790(b)(1)(ii) (Nuclear Regulatory Commission); 12 C.F.R. § 404.7(b) (Export-Import Bank). The DHS procedures should also provide that the Program Manager will identify any segregable information that the Program Manager determines is not Protected CII and mark the information so that it is clear that the segregable information is not protected by the CII Act.

4. The Proposed Regulations Improperly Suggest That the CII Act Protects Information If DHS Has Not Determined That the Information Meets the Requirements of the Statute.

A number of the proposed regulations are devoted to discussing the protections that apply to information that has been submitted to DHS with a request that it be treated as Protected CII, but the Program Manager has not made an “initial validation determination” that the information satisfies the requirements for protection under the CII Act. Proposed § 29.6(e)(1). Under the proposed regulations, after such “proposed-Protected CII” is submitted, there are a number of steps that the Program Manager must take to acknowledge receipt and evaluate (“validate,” in the regulations) whether the information should be protected. The period required to complete these steps may be substantial. Even if the Program Manager undertakes to make prompt determinations, communications with the submitter may be needed to determine the basis for the

of some Protected CII does not result in protection of the entire submission.

submitter's claim, and backlogs may develop if submissions are voluminous. *See* Proposed § 29.6. Remarkably, DHS has not imposed any time limit on these determinations, and so the period during which the status of information is undecided is indefinite.

The language in the proposed regulations is inconsistent on the issue of how information should be treated prior to the Program Manager's determination. Proposed § 29.5(d)(1)(i) states that information shall be maintained as protected by the provisions of the CII Act only when it has been marked "Protected CII" by the Program Manager or his designee. However, another provision states that CII voluntarily submitted with a request that it be treated as Protected CII "maintains its protected status" unless the Program Manager "renders a final decision that the information is not Protected CII." Proposed § 29.2(f). Yet another provision states that all information submitted in accordance with the regulations "will be presumed to be treated as Protected CII" from the time the information is received by a Federal agency until a final decision by the Program Manager that the information is not protected. Proposed § 29.6(b).

The provisions suggesting that information is Protected CII because the Program Manager has not rendered a final decision misstate the law and should be deleted. The CII Act does not protect information merely because it has been submitted with a request for protected status and the Program Manager has not acted on the request. Nor does the statute authorize a "presumption" of protection pending a final decision. Instead, the restrictions on application of the FOIA, criminal penalties, and other matters set forth in the statute apply *only* if the information meets the requirements of 6 U.S.C. § 133(a).

More specifically, neither DHS nor any other Federal agency could lawfully deny a FOIA request on the basis that the information requested was tendered for protection under the CII Act,

and the Program Manager has not decided whether the information does, in fact, meet the requirements under the CII Act. Similarly, an employee who disclosed such information could not be criminally prosecuted under 6 U.S.C. § 133(f) on the theory that the information “maintains its protected status” or that there is a “presumption” that the information is Protected CII until the Program Manager renders a final decision to the contrary. The CII Act also does not restrict the use of information in a civil action, or preempt State and local law disclosure obligations, merely because the information has been submitted to DHS and is awaiting a validation determination. Proposed § 29.2(f) and § 29.6(b) are erroneous and misleading because they suggest that information that does not satisfy the statute is subject to these statutory restrictions merely because the Program Manager has not issued a final decision and the submitter has requested that it be treated as Protected CII.

In addition to removing the inaccurate language in proposed §§ 29.2(f) and 29.5(b), DHS should amend the procedures for validation (§ 29.6) to provide both that the Program Manager shall promptly make initial decisions on whether information meets the requirements for protection under the CII Act, and that the Program Manager will expedite these determinations when the information is being sought by any interested party, including members of the public, other Federal agencies, components in DHS that have identified a use for the information, and state and local officials. If the information is responsive to a request submitted under the FOIA or similar statutes, such statutes require prompt determination of whether information is subject to any restrictions on disclosure. *See* 5 U.S.C. § 552(a)(3) and (a)(6)(a)(i) (providing that agencies shall make records available promptly and provide determinations within 20 working

days).³ Nothing in the CII Act repeals these requirements, either expressly or by implication, and it may be necessary to expedite the Program Manager's decision to satisfy such deadlines.

Priority should also be given to deciding the status of information if another Federal agency, state or local government, or component of DHS is seeking to use the information in connection with matters that it is actively pursuing and needs to know what constraints apply.

5. The Proposed Regulations Should Clearly State the Authority of Government Officials to Use Protected CII.

Because the ultimate objective of the CII Act is to ensure that Federal, State and local authorities have as much information as possible to address security issues, the regulations should clearly state the authority of officials to use information under the Act. If the regulations discourage the use of information because they are ambiguous or overstate the restrictions imposed by the CII Act, authorities will be discouraged from taking corrective action, and the objectives of the Homeland Security Act and other laws will be thwarted.

The proposed regulations do not provide such a clear statement and, instead, contain statements about officials' authority to use Protected CII that are, at best, confusing. For example, proposed § 29.8(b) is entitled "Federal, State and Local Government Access," but this section does not acknowledge that Federal, State and local authorities are authorized to use Protected CII in furtherance of the investigation or prosecution of a criminal act. 6 U.S.C. §

³ We do not think that a Federal agency could properly withhold information under the FOIA solely on the basis that the source of the information claims that the information is Protected CII, and the government is not prepared to take a position on whether this claim is valid. *Cf. Grove v. Department of Justice*, 802 F. Supp. 506, 518 (D.D.C. 1992) (agency may not decline to release documents on the basis that they have been referred to other agencies for their views on whether any exemption applies); *Matter of Wade*, 969 F.2d 241, 247-48 (7th Cir. 1992) (same).

133(a)(1)(D)(i) and (E)(iii). A statement that Federal officers and employees may use Protected CII for criminal investigations appears in proposed § 29.8(f), but this paragraph is entitled “Access by Congress and whistleblower protection” – a title that might lead readers to overlook this paragraph or wonder whether the authority is limited to Congress or whistleblowers. The regulations acknowledge the authority of State and local governments to use Protected CII for criminal investigations in the third subsection of proposed § 29.8(d), but only after stating that State and local authorities must obtain authorization from the CII Program Manager and the entity submitting information to make use of Protected CII. A reader might conclude (erroneously, we believe), that State and local authorities are permitted to use Protected CII in criminal investigations only if they obtain prior authorization from the Program Manager and/or submitter of the information.

These provisions should be revised so that they are clear, consistent with the statute, and do not discourage the use of Protected CII for all purposes that are consistent with the Act. The statute identifies three circumstances in which both officers or employees of the United States and State or local officials may use Protected CII:

1. In furtherance of the investigation or prosecution of a criminal act. 6 U.S.C. § 133(a)(1)(D)(i) and (E)(iii);
2. For the purpose of protecting critical infrastructure or protected systems, *id.*; and
3. For any purpose with the written consent of the person or entity submitting such information. *Id.* § 133(a)(1)(D) and (E)(ii).

Federal officers and employees may also use Protected CII “for the purposes of this subtitle” (that is, “the security of critical infrastructure and protected systems, analysis, warning,

interdependency study, recovery, reconstitution, or other informational purpose,” *id.* § 133(a)(1)); when providing information to the Congress, congressional committees and the Comptroller General for certain purposes, *id.* § 133(a)(1)(D); and when providing “advisories, alerts, and warnings” that are consistent with 6 U.S.C. § 133(h).

Because Protected CII can be used for these purposes, there is no justification for restricting use of proposed Protected CII for these purposes. The regulations should make clear that authorities are permitted to use both Protected CII *and* information awaiting validation as Protected CII for these purposes.

We also note that Proposed § 29.8(1)(ii) purports to impose a new requirement that if information is disclosed in furtherance of an investigation or prosecution of a criminal act, or to Congress or the Comptroller General for purposes authorized by 6 U.S.C. § 133(a)(1)(D), then:

prior written authorization must be obtained, in consultation with the DHS Office of the General Counsel, from the DHS Secretary, DHS Deputy Secretary, Under Secretary for IAIP, the DHS Inspector General, or the CII Program Manager.

The statute does not authorize imposing this additional requirement of written consent on uses that are explicitly exempt from the restrictions on the use of Protected CII. In other words, if federal officials or employees seek to use information for purposes described in 6 U.S.C. § 133(a)(1)(D) (or any other authorized purpose), DHS does not have authority to condition such use on obtaining written consent from DHS officials. DHS might include in its regulations a provision that states that officials who make use or disclose Protected CII for these purposes should notify DHS of their action in order to keep DHS’s records on the care and maintenance of CII accurate, but DHS may not restrict the use of CII by imposing conditions that are not authorized by statute.

6. The Proposed Regulations Overstate the Extent to Which the Database Tracking CII Submissions Is Protected.

The proposed regulations provide for the creation of a database known as the “Critical Infrastructure Information Management System” (CIIMS) which will store information on “the receipt, acknowledgement, validation, storage, destruction, and disclosure of Protected CII.” Proposed 29.4(e). The procedures also provide that this data “shall be protected by the provisions of the CII Act of 2002.” *Id.*

This proposed regulation is flawed insofar as it labels information that does not satisfy all the requirements of the statute as Protected CII. For example, if a business submits information to DHS with an express request that it be labeled as Protected CII, and DHS concludes that the information was not voluntarily submitted, entries in DHS’s database describing this information would not be protected under 6 U.S.C. § 133(a).

Moreover, although the statute provides for protection of the identity of a person or entity that submits CII to DHS in accordance with 6 U.S.C. § 133(a)(1), it does not provide that *all* information regarding submissions is Protected CII. Information that describes the agency’s handling of such information -- such as how long DHS took to validate the information and who was responsible for validation, whether the information has been stored or destroyed, and the disclosure of the information -- does not fall within the statute’s protection. In general, information that describes DHS’s activities cannot be treated as Protected CII because only CII that is voluntarily submitted to DHS is covered by 6 U.S.C. § 133(a). DHS should delete the proposed language or amend the regulations to make clear that only information in the database that meets the requirements of the CII Act is Protected CII.

7. The Proposed Regulations Should Be Amended to Allow Any Interested Party to Request Review of Whether Information Marked Protected Qualifies under the Act.

The proposed regulations acknowledge that the Program Manager’s ‘initial validation determination’ may be changed. *See* Proposed 29.6(g) (“[o]nly the CII Program Manager or the Program Manager’s designee may change the status of Protected CII to non-Protected CII and remove its Protected CII markings.”) However, they do not provide a procedure for initiating review of whether information has been inaccurately marked Protected CII. Because the initial determination may be based on inadequate information or representations by the submitter that are incomplete or inaccurate, it is important that the proposed regulations provide an effective mechanism for reviewing initial determinations and promptly correcting errors. Moreover, a mechanism for subsequent review is needed because the CII definition provides that CII is limited to information that is not customarily disclosed to the public, and the status of information may change because of subsequent disclosures to the public.

DHS should adopt procedures analogous to those that provide for ongoing review of national security classification markings. *See* Executive Order 13,232, § 1.9, § 3.5, 68 Fed. Reg. 15315 (March 28, 2003); 28 C.F.R. § 17.31. More specifically, the procedures should make clear that:

(1) DHS has an obligation to review a determination whenever information that calls into question whether information qualifies as Protected CII is brought to DHS’s attention;

(2) Officials and employees who believe that information has been improperly marked as Protected CII are “encouraged and expected to challenge” the designation by requesting review

and setting forth the reasons why they believe that the information is not subject to 6 U.S.C. § 133(a)(1). *Cf.* Executive Order § 1.9(a).

(3) Any interested party, whether he or she has access to the information or not, may request review of whether the information meets the requirements for protection. *Cf.* Executive Order 13232, § 3.5.

(4) DHS will automatically review whether information is properly marked protected whenever the information falls within the scope of a request under the FOIA, is subject to a request under any State or local law requiring disclosure of information or records, or is sought for use in a civil action.

8. The Proposed Regulations Should Be Amended to Require Submitters to Verify That Submissions Satisfy the Requirements for Protection under the CII Act.

Ordinarily, DHS will not, by itself, have sufficient information to evaluate claims that information qualifies as Protected CII. Instead, DHS will need to obtain information from the submitters to determine whether particular information qualifies. Two changes should be made to the proposed regulations in this respect.

First, the regulations should require that submitters provide DHS with a sworn statement attesting that critical requirements of the statute are met. The statement should also provide sufficient details to allow the Program Manager to evaluate the claims. Agencies that routinely receive requests that information be protected as trade secrets or confidential business information require such statements by regulation. *See, e.g.*, 49 C.F.R. § 512.4(b) (Department of Transportation); 17 C.F.R. § 200.83(c)(2) (Securities and Exchange Commission). Such requirements are vital to discourage unjustified claims for protection and to enable the agency to

make an informed decision on whether the restrictions applicable to Protected CII need to be imposed on the government and the public. Without such verification, submitters may seek to secure Protected CII status for their own purposes, not to advance the interests of the security of critical infrastructures.

The verification by the submitter should include statements demonstrating that (i) all of the information for which protection is sought falls within the definition of CII, 6 U.S.C. § 131(3); (ii) the submitter is not required to provide the information to any other agency and the information is not being submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings; (iii) the information is not included in the securities or banking documents or materials identified in 6 U.S.C. § 131(7)(B)(i); (iv) the submitter is providing the information for the use of the DHS in connection with the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution or other informational purpose, and is not submitting the information in order to prevent its use in civil proceedings or disclosure to the public; and (v) the submitter is not seeking protection for any reasonably segregable information that does not qualify for protection.

In addition, because information only qualifies as CII if it is “not customarily in the public domain,” the regulations should require that the submitter provide a detailed statement to allow DHS to determine whether this requirement is met. The regulations of other Federal agencies that require such information be provided can be used as models. Those regulations require that the submitter describe:

1. Measures taken by the submitter to ensure that the information has not been disclosed or otherwise made available to any one other than the submitter;

2. The extent to which the information has been disclosed, or otherwise become available, to persons other than the submitter, and why such disclosure or availability does not compromise the ability of the information to qualify as Protected CII;
3. The extent to which the information has appeared publicly (regardless of whether the submitter has authorized that appearance or confirmed the accuracy of the information), and an explanation of why such disclosures do not compromise the ability of the information to qualify as Protected CII; and
4. Prior determinations by agencies or courts relating to the confidentiality of the submitted information or similar information possessed by the submitter.

See 49 C.F.R. § 512.4(b)(3); *see also Smith v. BIC Corp.*, 869 F.2d 194, 199 (3d Cir. 1989); 10 C.F.R. § 2.790(b)(4) (factors considered by NRC in making confidentiality determinations).

Second, the provision in the proposed regulation stating that the Program Manager “shall give deference to the submitter’s expectation that the information qualifies for protection,” Proposed § 29.6(e), should be deleted. There is no basis for giving deference to the submitter’s judgment about whether the submission is voluntary, whether it qualifies as CII, or other requirements of the CII Act. Moreover, nothing in the statute authorizes giving any weight to the submitter’s “expectation” in this context. If the submitter’s subjective expectations are not supported by an objective showing that the requirements for protection are satisfied, the statute provides no protection.

9. The Proposed Regulation Concerning Destruction of Submissions That Do Not Qualify as CII Misstates the Law.

Proposed § 29.6(e)(1) and § 29.6(f) provide that, in the event the CII Program Manager makes a final determination that information tendered by a submitter is not Protected CII, the Program Manager shall either “maintain the information without the protections of the CII Act of 2002” or “dispose of it in accordance with the Federal Records Act” based on the submitter’s preferences. If the submitter’s preferences cannot be determined, the regulations provide that the Program Manager “shall destroy the information in accordance with the Federal Records Act unless the Program Manager determines that there is a need to retain it for law enforcement and/or national security reasons.”

These provisions contemplate a choice where the law provides no choice. The Federal Records Act and the CII Act do not represent alternative schemes between which DHS or the submitter may choose; the CII Act addresses limitations on disclosure (but not disposition) and the Federal Records Act governs disposition (but not disclosure). Both statutory schemes are mandatory. If the information does not qualify as Protected CII, the DHS has no choice but to maintain it “without the protections of the CII Act of 2002.” In addition, because materials submitted under the proposed regulations are agency records, 44 U.S.C. § 3301, DHS is required to retain and dispose of these materials, including those found not to be Protected CII, in accordance with the Federal Records Act even if the submitter would prefer that they be destroyed.

Disposal of the information “in accordance with the Federal Records Act” does *not* mean that information is destroyed if it is determined that it does not qualify for the protections of the

CII Act. To the contrary, disposal in accordance with the Federal Records Act requires maintaining records of value for an extended period of time, and sometimes requires permanent retention. The relevant portions of the Federal Records Acts, 44 U.S.C. § 3301-3314 (known as the Records Disposal Act), provide that agency records may only be destroyed in accordance with record schedules approved by the Archivist. When an agency prepares a proposed schedule, the Archivist conducts an appraisal of the value of the records and solicits public comment on how long the records should be preserved. 36 C.F.R. § 1228.30. If the Archivist agrees with the agency's assessment that the records will lack "sufficient administrative, legal, research, or other value to warrant their continued preservation" after the period specified in the schedule, the Archivist approves the schedule and gives the agency authorization to destroy the records. 44 U.S.C. § 3303a(a). The Federal Records Acts provide that the schedule approved by the Archivist is mandatory; destruction of records prior to the period specified in the schedule is unlawful, and records must be maintained indefinitely if no schedule has been approved or if the Archivist concludes that the records have permanent value. *See* 44 U.S.C. § 3314; 36 C.F.R. §§ 1220.38(b), 1228.50. Destruction of agency records without such authorization is a crime. 18 U.S.C. § 2071.

Accordingly, proposed § 29.6(e)(1) and § 29.6(f) should be removed entirely, or replaced by a statement that simply declares that all information submitted with a request that it be protected under the CII Act will be disposed of in accordance with the Federal Records Acts regardless of whether it is or is not determined to be protected CII.

10. The Regulations Should Be Amended to Correct Miscellaneous Errors and Inconsistencies.

The proposed regulations should also be revised to correct several errors and inconsistencies:

- The proposed definitions appropriately distinguish between “CII” and “Protected CII,” Proposed §§ 29.2(c), (f). However, in the remainder of the proposed regulations, “CII” sometimes appears where “Protected CII” is intended. For example, Proposed § 29.6(c) states that, “[t]he CII Program Manager shall mark CII materials as follows: ‘Protected Critical Infrastructure Information.’” “CII” in this sentence should be “Protected CII.” Similarly, proposed § 29.3 states that “[f]ederal agencies shall not utilize CII for regulatory purposes without the written consent of the submitter.” This provision is inaccurate because the Act only restricts the use of “Protected CII.” In addition, this sentence should be deleted because the Act does not contain a restriction on use for all regulatory purposes. Indeed, some purposes that might be considered “regulatory,” such as criminal investigations, are purposes for which Federal agencies are authorized to use Protected CII. *See, e.g.*, 6 U.S.C. § 133(a)(1)(D)(i).
- Proposed § 29.6(e)(1) misstates what the Program Manager must determine in making a validation decision. The second sentence states that the Program Manager shall review the information “to validate the satisfaction of the definition of CII as established by law.” However, satisfying the definition of CII in 6 U.S.C. § 131(3) is not sufficient; to qualify as “Protected CII” the conditions set forth in 6 U.S.C. § 133(a)(1) must also be satisfied (*e.g.*, voluntary submission to DHS for use by DHS for specified purposes). The

last sentence of the proposed regulation correctly suggests that, before “validating” a submission, the Program Manager must determine that the information meets “the requirements for protection under the CII Act of 2002” -- not just the definition of CII. The second sentence, therefore, should be amended to conform with the last sentence so that it provides that the Program Manager shall review whether all of the requirements of the Act for Protected CII are met.

Conclusion

For the reasons stated above, Public Citizen and the Freedom of Information Clearinghouse urge DHS to revise its proposed regulations to comply with the Critical Infrastructure Information Act of 2002.

Respectfully submitted,

Michael Tankersley
Scott L. Nelson
Amanda Frost
Public Citizen Litigation Group
1600 20th Street, NW
Washington, DC 20009
(202) 588-1000

June 16, 2003