

Qwest.txt

Subject: "Procedures for Handling Critical Infrastructure Information," 68 Fed. Reg. 18,524 (April 15, 2003)
Date: Mon, 16 Jun 2003 16:08:42 -0400
From: "Meade, Christopher" <Christopher.Meade@wilmer.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Dear Sir or Madam:

Attached please find (1) a cover letter and (2) comments prepared by Wilmer, Cutler & Pickering, on behalf of Qwest Communications, on the Department of Homeland Security's "Procedures for Handling Critical Infrastructure Information," 68 Fed. Reg. 18,524 (April 15, 2003).

> > <<Comments on 68 Fed. Reg. 18524.pdf>>
> > <<DOC003.tif>>

Comments on 68 Fed. Reg. 18524.pdf

Name: Comments on 68 Fed. Reg. 18524.pdf
Type: Acrobat (application/pdf)
Encoding: base64
Description: Comments on 68 Fed. Reg. 18524.pdf

DOC003.tif

Name: DOC003.tif
Type: TIFF image file (image/tiff)
Encoding: base64
Description: DOC003.tif

WILMER, CUTLER & PICKERING

2445 M STREET, N.W.

WASHINGTON, DC 20037-1420

TELEPHONE +1 (202) 663 6000

FACSIMILE +1 (202) 663 6363

WWW.WILMER.COM

RANDOLPH D. MOSS
(202) 663-6640
RANDOLPH.MOSS@WILMER.COM

June 16, 2003

399 PARK AVENUE
NEW YORK, NY 10022-4697
TELEPHONE +1 (212) 230 8800
FACSIMILE +1 (212) 230 8888

100 LIGHT STREET
BALTIMORE, MD 21202-1036
TELEPHONE +1 (410) 986 2800
FACSIMILE +1 (410) 986 2828

1600 TYSONS BOULEVARD
10TH FLOOR
TYSONS CORNER, VA 22102-4859
TELEPHONE +1 (703) 251 9700
FACSIMILE +1 (703) 251 9797

4 CARLTON GARDENS
LONDON SW1Y5AA, ENGLAND
TELEPHONE +44 (0) 20 7872 1000
FACSIMILE +44 (0) 20 7839 3537

RUE DE LA LOI 15 WETSTRAAT
B-1040 BRUSSELS, BELGIUM
TELEPHONE +32 (0) 2 285 49 00
FACSIMILE +32 (0) 2 285 49 49

FRIEDRICHSTRASSE 95
D-10117 BERLIN, GERMANY
TELEPHONE +49 (30) 20 22 6400
FACSIMILE +49 (30) 20 22 6500

By Email and Facsimile

Associate General Counsel
(General Law)
Department of Homeland Security
Washington, DC 20528

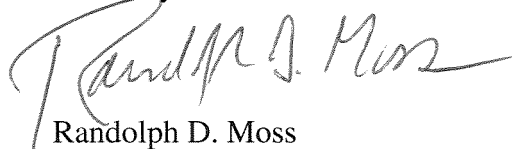
RE: "Procedures for Handling Critical Infrastructure Information,"
68 Fed. Reg. 18,524 (April 15, 2003)

Dear Sir or Madam:

Attached please find comments prepared by Wilmer, Cutler & Pickering, on behalf of Qwest Communications, on the Department of Homeland Security's "Procedures for Handling Critical Infrastructure Information," 68 Fed. Reg. 18,524 (April 15, 2003).

Qwest is committed to working with the Department, on an on-going basis, to protect critical infrastructure. If Qwest can be of any assistance to the Department – now or in the future – please do not hesitate to contact Qwest's liaison on these issues, David J. Heller (Vice President of Risk Management and Security), at 303-672-2943.

Sincerely,



Randolph D. Moss

Associate General Counsel
(General Law)
Department of Homeland Security
Washington, DC 20528

RE: Comments by Qwest Communications on the “Procedures for Handling Critical Infrastructure Information,” 68 Fed. Reg. 18,524 (Apr. 15, 2003)

We are writing to comment on the proposed regulations entitled the “Procedures for Handling Critical Infrastructure Information,” 68 Fed. Reg. 18,524 (Apr. 15, 2003), which were drafted to implement the Critical Infrastructure Information Act of 2002 (“CII Act” or “Act”).

BACKGROUND

Even before 9/11, the Federal Government recognized the importance of assessing and responding to possible vulnerabilities in our Nation’s critical infrastructure. *See National Plan for Information Systems Protection, Version 1.0: An Invitation to Dialogue* (White House 2000). This need, of course, became even more stark after the attacks of 9/11. After much consideration and deliberation, Congress passed the Critical Infrastructure Information Act of 2002, which seeks to promote the protection of critical infrastructure through an innovative partnership between Government and private industry.

In the Act, Congress designed a statutory scheme that encourages industry to submit information voluntarily to the Government. Congress recognized, however, that companies might hesitate in submitting information if there were inadequate protections against the disclosure of sensitive information (which could, *inter alia*, lead to competitive harm). The statute therefore provides a number of protections to ensure that voluntarily submitted

information is not disclosed to the public or competitors, or used for purposes unrelated to critical infrastructure protection.

As designed, the Act will further the protection of critical infrastructure if, and only if, private industry in fact submits information to the Government. If private industry, as a whole, feels that the Act and the regulations promulgated thereunder provide inadequate protections for sensitive business information, industry might not submit information (or might submit less information), and the purposes of the Act will be thwarted. It is therefore essential that private industry can be confident that material will be treated confidentially and will be adequately protected.

Finally, it should be noted that the Act in no way limits the Government's powers regarding information that is already in its possession. Rather, the Act provides incentives for the voluntary submission of *additional* information, so as to increase the flow of potentially significant information to the Federal Government.

COMMENTS

As a whole, we commend the proposed regulations: by providing strong protections for information voluntarily submitted to the Government, the regulations will encourage industry to provide critical infrastructure information and, therefore, will aid the protection of our Nation's critical infrastructure. Qwest, like other members of private industry, is committed to protecting critical infrastructure, and the CII Act and the Department's implementing regulations will help it to do so.

We are concerned, however, that a number of the provisions could lead industry to hesitate before providing information to the Government and, therefore, could undermine the

statutory and regulatory scheme. These issues require clarification in order to give the Act its intended effect. We first address a few general issues regarding supplemental protections; then comment on provisions relating to disclosures by State and local governments; and finally address additional provisions that we believe would benefit from clarification or modification.

Supplemental Protections

The regulations should be clear that the protections of the Act are a floor, and not a ceiling, with respect to the protections available to sensitive information. The regulations should therefore state that the Act and regulations supplement, but do not supercede, other legal and regulatory protections of sensitive information, including the Trade Secrets Act, the Privacy Act, and exemptions to the Freedom of Information Act.

In addition, it may at times be appropriate for entities to enter into separate agreements with governmental entities relating to the sharing of information. Members of private industry have entered into such agreements in the past, and the regulations should expressly state that the Act and regulations do not preclude such agreements. For example, a new provision could read as follows: “Nothing in these regulations shall be construed to limit the authority of DHS or a Federal agency to enter into a binding agreement with a submitting person or entity that supplements the protections under these regulations.”

Protections Against Disclosure by State and Local Governments

Significantly, the proposed regulations provide very limited assurances that State and local governments will not disclose Protected CII (as defined in § 29.2(f)). For example, there is no enforcement mechanism in the event that a State or local government violates a provision of

the statute or regulations. *See* § 29.9(d). Thus, an entity might feel confident that the *Federal Government* will protect its sensitive information, but might conclude that there are inadequate protections against State and local governmental disclosure. As a result, entities might not disclose information and the statutory scheme would be undermined.

We therefore recommend the following clarifications and modifications:

- Section 29.8(b) allows disclosure of Protected CII to a State or local government pursuant to the governmental entity's express agreement acknowledging its understanding and responsibilities with respect to that information. The regulations should require that the submitter first provide written consent before Protected CII can be disclosed to a State or local government so the submitter can retain control of its voluntarily provided information. Such a provision would be consistent with § 29.8(d)(2), which prohibits the State or local government from disclosing or distributing the information to another party "unless the Program Manager first obtains the written consent of the person or entity submitting the information." Alternatively, the submitter should receive written notification from the Program Manager of all State and local governments to whom its Protected CII has been provided. This would at least allow the submitter to track the retransmission of its information.
- Section 29.8(d)(1) states that State and local governments shall not disclose Protected CII without "first obtaining authorization" from the CII Program Manager. The regulations should clarify that "written" authorization is required (so that the State or local government would be required to "first obtain[] written authorization" from the CII Program Manager). This would make the provision consistent with § 29.8(f)(1)(ii), which requires written authorization before certain disclosures can be made.

- The proposed regulations are ambiguous regarding whether information may be shared with State or local contractors. Given the difficulty that DHS would have monitoring State and local contractors, the regulations should make clear that Protected CII shall not be disclosed to State or local contractors. A new provision should be added to § 29.8 stating that “State and local governments shall not disclose Protected CII to contractors or subcontractors.” This clarification would be consistent with § 29.1(b), which does not mention State or local contractors as within the “scope” of the regulations. (If this change is made, the words “or contractor” should be deleted from § 29.8(g)(1).)
- As noted, the proposed regulations do not contain an enforcement mechanism in the event that a State or local entity violates the statute or regulations. To correct this:
 - Section 29.9 should explicitly state that the DHS Inspector General, CII Program Manager, or IAIP Security Officer shall investigate unauthorized disclosures by State or local governments.
 - If it is determined that a State or local government violated the statute or regulations, the regulations should provide that such State or local government shall not receive Protected CII in the future unless (a) the submitter expressly consents or (b) the CII Program Manager has certified that appropriate remedial measures have been taken.
 - Section 29.9(d) (the penalty provision) should be clarified to state that it applies to Federal officers or employees who disclose Protected CII to another person or entity, including a State or local official, knowing that such person or entity will make an unauthorized disclosure.

Comments on Additional Provisions

In addition to the above, we have the following comments on the proposed regulations. This section addresses the regulations in sequential order.

Section 29.2: “Definitions”

The definition of “Protected CII” in § 29.2(f) states that only the CII Program Manager may make a final decision that information is not Protected CII. This provision should also state that, before such a decision is made, “notice to the submitter” and “an opportunity for the submitter to withdraw the submission” is required.

Section 29.3: “Effect of Provisions”

Section 29.3(a) – which refers to “information that must be submitted to a Federal agency” – is ambiguous. On the one hand, it could refer to information that is actually submitted pursuant to a legal requirement. On the other hand, it could refer to information that DHS later concludes *should have been* submitted to a Federal agency. The latter interpretation is at odds with the plain terms and purpose of the statute: it would generate substantial uncertainty as to whether a submission *should have been* made pursuant to some separate legal requirement and whether the submission is thus not protected. To correct this ambiguity, the phrase “information that must be submitted to a Federal agency” should be replaced with “information that was submitted to a Federal agency pursuant to a legal requirement.” (The next sentence, beginning with “Similarly,” should then be deleted as redundant.) For the same reasons, the phrase “when information is required to be submitted,” which appears a few sentences later, is ambiguous. The provision should strike “is required to be” (so that it will read “when information is submitted”).

Sections 29.3(c) and (d) also require clarification to ensure that the regulations provide the full level of protection contemplated by the statute. Section 29.3(c) contains the prohibition that “Federal agencies shall not utilize CII for regulatory purposes,” but should add “or any purpose unrelated to critical infrastructure protection” to this prohibition.

Section 29.3(d) then states that governmental entities and third parties may still “independently obtain[]” information using other laws, regulations, rules, or other authorities. These regulations need to clarify the meaning of “independently obtained information.” For example, if a governmental entity learns of information only because it was submitted as Protected CII, it should not be permitted to turn around and seek that same information through another means. Such information cannot be said to be “independently obtained” within the meaning of the statute. *See* 6 U.S.C. § 133(c). Moreover, such an interpretation would permit governmental entities and third parties to do an end-run around the statute and regulations, and would thereby discourage the voluntary submission of CII.

To correct this ambiguity, § 29.3(d) should be amended to state, consistent with the statute, that it applies only to “independently obtained information”: “These 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, from independently obtaining information.” The terms “independently obtained information” and “independently obtaining information” should then be defined (in either § 29.2 or § 29.3(d)) to exclude information that has been directly or indirectly derived from Protected CII. If any question arises whether the information was “independently obtained,” the governmental entity or third party should be required to demonstrate that the information was obtained from an independent source.

Finally, § 29.3(e) – involving private rights of action – introduces an ambiguity that is not present in the statutory language. We would recommend that this provision track the statutory language, by (1) amending the title to “no private right of action” and (2) deleting the first sentence of the provision. Consistent with congressional intent, the provision would then more closely track section 215 of the CII Act, 6 U.S.C. § 134.

Section 29.5: “Authority to Receive Critical Infrastructure Information”

We believe that the procedures regarding the marking and validation of Protected CII are too rigid and should grant the CII Program Manager more flexibility. The strict procedural requirements create the possibility that information will be denied protected status because of a technical or procedural defect, even though it meets the substantive requirements of the statute and regulations; this information will likely be destroyed, *see* § 29.6(e)(1)(ii), and the Government will not receive any benefit from the submitted information. Rather than having rigid procedural requirements, it would be more consistent with the statute to grant the CII Program Manager more flexibility. For example:

- We recommend that the word “only” be deleted from the introductory sentence of § 29.5(b).
- In the case of written information or records, § 29.5(b)(3)(i) should be clarified to state that a submitter need not mark each and every page with the request for CII protection. The provision should state that a cover letter seeking protection, or a marking on the first page of the document, is sufficient to constitute a request for protected status.
- In the case of written information or records, § 29.5(b)(3)(i) should provide that a submitter may seek protection at the time of submission, or within fifteen (15) calendar

days. This modification will make § 29.5(b)(3)(i) consistent with the rule for oral information, *see* § 29.5(b)(3)(ii).

- In the case of oral information, the requirement in § 29.5(b)(3)(ii) that a submitter provide a “written or otherwise tangible version of the oral information initially provided” is overly burdensome. Such a requirement will make oral communications of CII less likely, and will therefore impede the flow of information to the Government. The provision should be amended so that the submitter of oral information may submit a written statement that “fairly describes” the oral information provided.
- Finally, § 29.5(d)(2) is ambiguous and should be revised. The provision appears to be designed to protect information pending a decision by the CII Program Manager, but it might be read to authorize disclosures after the CII Program Manager’s decision. The regulation should be amended to clarify that it is meant to provide a “stay” pending decision and does not provide any authority for disclosures. For example, it could read: “Pending a decision by the CII Program Manager, the Federal agency or DHS component forwarding the information to DHS shall treat the information as Protected CII, and shall not disseminate, distribute, or make public the information.”

Section 29.6: “Acknowledgement, Validation, and Marking of Receipt”

Section 29.6 should make clear that information that is submitted under the Act and regulations remains the property of the submitter, unless the submitter expressly indicates an intention to the contrary.

Section 29.6(e)(1)(i) should provide that, after notice but before a final decision is made, the submitter “shall have an opportunity to withdraw” the submission.

Similarly, in §§ 29.6(e)(1)(i)(D) and (e)(1)(ii), the regulations should state that, if the CII Program Manager makes a final determination that information is not Protected CII, the submitter shall have the option of having the information returned. These provisions should also state that information shall be destroyed in accordance to the Federal Records Act “to the extent applicable.” As modified, § 29.6(e)(1)(i)(D) would read: “in the event the CII Program Manager makes a final determination that any such information is not Protected CII, the submitter [should indicate whether it] prefers that the information be returned to the submitter, maintained without the protections of the CII Act of 2002, or , to the extent applicable, be disposed of in accordance with the Federal Records Act.” (A similar change should be made in § 29.6(e)(1)(ii).)

We believe that the “good faith” provision of § 29.6(f) should be deleted. The provision sets a nebulous standard: if the CII Program Manager “determines” that information is not submitted in good faith, notice need not be provided to the submitter. Since this good faith determination is being made by a single individual – who could easily make an erroneous assessment of good faith – the provision leaves those who would otherwise submit information without the clear assurances they might need before making voluntary submissions to the Government. As a result, this provision could potentially chill the submission of voluntary information to the Government under the Act. The “good faith” standard, moreover, is not found in the statute.

If § 29.6(f) is not omitted, it should, at a minimum, provide notice to the submitter and an opportunity to be heard, since the Program Manager might lack significant information relating to the submission which could lead to an erroneous determination regarding good faith. The provision should also specify that if, after notice and an opportunity to be heard, the CII Program

Manager determines that the information was not submitted in good faith, such information shall be returned to the submitter or destroyed. Such a modification is critical: absent such clarification, a submitting entity could rightfully be concerned that an erroneous determination by the CII Program Manager regarding good faith could result in the disclosure of sensitive information.

Finally, § 29.6(g) should be clarified to state that the CII Program Manager may change the designation from CII to non-CII “only at the request of the submitter.” If this change is not made, the regulation should state that the CII Program Manager must provide notice to the submitter, and an opportunity for the submitter to withdraw the submission, before changing a designation from CII to non-CII.

Section 29.8: “Disclosure of Information”

Section 29.8 addresses issues that are critical to the effective operation of the statute, but provides inadequate assurances of protection.

- Section 29.8(a) states that DHS may “chose to provide or authorize access” of Protected CII “when it is determined” that access supports a lawful and authorized purpose as set forth in the CII Act or any “other law, regulation, or legal authority.” At best, this provision is ambiguous; read broadly, it could completely undermine the protections of the Act. We recommend that this provision be deleted. If, however, this provision is retained, it must be clarified to be consistent with the Act. It should state that any disclosure or use of Protected CII within the Government is limited by the terms of the Act; and any advisories, alerts, or warnings issued to the public pursuant to § 29.8(e) shall not disclose “the source of any voluntarily submitted critical infrastructure

information that forms the basis for the warning” or “information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately within the public domain.” *See* 6 U.S.C. § 133(g).

- Since the Federal Government has less control over a Federal contractor than one of its officers and employees, the regulations should provide additional protections regarding disclosures to Federal contractors. Section 29.8(c) should be amended to require that the Federal contractor “sign a statement” agreeing that it will not disclose Protected CII unless expressly authorized in writing by the submitter. The regulations should also provide that if a Federal contractor is found to have violated the statute or regulations, such Federal contractor shall not receive Protected CII in the future unless (a) the submitter expressly consents or (b) the CII Program Manager has certified that appropriate remedial measures have been taken by the contractor.
- Any disclosure to Congress or the General Accounting Office under § 29.8(f) should be accompanied by notice to the recipient that states that the material is protected and that disclosure of such information could result in criminal or other penalties.
- The first clause of § 29.8(f)(2) (the so-called “whistleblower” provision) is superfluous and should be deleted. More importantly, the last sentence of the introductory paragraph to § 29.8(f)(2) should clarify that it is modified by the previous sentence. That sentence should be amended to read: “Disclosure may be made to the DHS Inspector General or to such employee designated by the Secretary of Homeland Security by any officer or employee of the United States who reasonably believes” Without such a clarification, the sentence might be read to permit “any officer or employee of the United

States” to disclose information to the public, which, needless to say, would completely undermine the protections of the Act.

- Section 29.8(g)(2) – regarding “[i]nformation independently obtained” by a State or local government – is redundant, as this protection is already provided in § 29.3(d). Having two provisions stating the same principle (although worded slightly differently) could lead to confusion; we therefore recommend that this provision be deleted. If, however, this provision is not omitted, the provision should be clear that “independently obtained information” does not include information that has been directly or indirectly derived from Protected CII. (See the discussion of § 29.3(d), above.)
- Section 29.8(i) refers to information submitted in good faith for “homeland security purposes.” “Homeland security purposes,” however, is not a defined term and could lead to confusion. Thus, we recommend that the provision be amended to refer to information submitted in good faith “under this Act.”
- Section 29.8(j), regarding warnings to foreign governments, should add an additional sentence to clarify that protected information shall not be disclosed: “pursuant to the authority to issue advisories, alerts, and warnings under § 29.8(e), the CII Program Manager or the Program Manager’s designee shall not disclose to a Foreign Government in any such advisory, alert, or warning: (1) the source of any voluntarily submitted critical infrastructure information that forms the basis for the warning or (2) information that is proprietary, business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately within the public domain.” *See* 6 U.S.C. § 133(g).

Again, we commend the proposed regulations, as they provide protections for information voluntarily submitted to the Government and are consistent with Congress's purpose in passing the CII Act. We ask that you consider our proposed clarifications and modifications, as we believe that these changes are necessary to give the Act its intended effect.