WILMER CUTLER PICKERING LLP
2445 M STREET, N.W.
WASHINGTON, DC 20037-1420
TELEPHONE 1 202 663 6000
FACSIMILE 1 202 663 6363
WWW.WILMER.COM

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
SUITE 1000
McLEAN, VA 22102-4859
TELEPHONE 1 703 251 9700
FACSIMILE 1 703 251 9797

4 CARLTON GARDENS
LONDON SW1Y5AA, ENGLAND
TELEPHONE 44 20 7872 1000
FACSIMILE 44 20 7839 3537

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

FRIEDRICHSTRASSE 95
D-10117 BERLIN, GERMANY
TELEPHONE 49 30 20 22 64 00
FACSIMILE 49 30 20 22 65 00

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

May 19, 2004

By Email and Federal Express

Janice Pesyna
Office of the General Counsel
Department of Homeland Security
Washington, DC 20528

RE: "Procedures for Handling Critical Infrastructure Information; Interim Rule," 69 Fed. Reg. 8,074 (Feb. 20, 2004) (RIN 1601-AA14)

Dear Ms. Pesyna:

Attached please find comments prepared by Wilmer Cutler Pickering LLP, on behalf of Qwest Communications, on the Department of Homeland Security's "Procedures for Handling Critical Infrastructure Information; Interim Rule," 69 Fed. Reg. 8,074 (Feb. 20, 2004).

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/cm

Randolph D. Moss

Attachment.

May 19, 2004

To: Janice Pesyna
Office of the General Counsel
Department of Homeland Security
Washington, DC 20528

From: Qwest Communications
1801 California Street, Suite 1160
Denver, CO 80202

Re: Comments by Qwest Communications on the "Procedures for Handling Critical Infrastructure Information; Interim Rule," 69 Fed. Reg. 8,074 (Feb. 20, 2004) (RIN 1601-AA14)

We are writing to comment on the interim regulations entitled the "Procedures for Handling Critical Infrastructure Information," 69 Fed. Reg. 8,074 (Feb. 20, 2004), which were promulgated to implement the Critical Infrastructure Information Act of 2002 ("CII Act" or "Act").

COMMENTS

As a general matter, we commend the interim regulations, as they generally strike the correct balance between encouraging the voluntary submission of critical infrastructure information and permitting the disclosure of information in certain limited circumstances, in furtherance of the protection of our Nation's critical infrastructure. We are concerned, however, that a few of the provisions could lead industry to hesitate before providing information to the Government and, therefore, could thwart the purpose of the Act. We therefore ask that the Department of Homeland Security ("DHS" or "Department") consider the following comments, modifications, and clarifications.

Clearly Setting Out Prohibition Against Disclosure

Perhaps most notably, the interim regulations fail to set out clearly the operative rule of the CII Act, namely, that Protected CII shall not be used or disclosed by any officer or employee of the United States except in certain limited circumstances. Rather, the operative rule is buried in the "exception" provision of § 29.8(f)(1) ("Exceptions for disclosure"). We propose that the rule be set forth clearly in its own section (perhaps in a new § 29.8(a)), that would read: "Pursuant to section 214(a)(1)(D) of the CII Act of 2002, Protected CII shall not, without the written consent of the person or entity submitting such information, be used or disclosed by any officer or employee of the United States for purposes other than the purposes of the CII Act of 2002, except as specifically designated in [§ 29.8(f)(1)]."

Protections Against Disclosure by State and Local Governments

While the interim regulations provide some protections against disclosures of Protected CII by State and local governments, the protections in the regulations are inadequate. 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:

- The interim regulations require that, before Protected CII may be shared with State or local governments, those entities must enter into a written agreement with DHS. 6 C.F.R. § 29.8(b). While the Supplemental Information in the Federal Register contemplates that

additional protections are required, and therefore details the requirements of the writing requirement, the regulations do not. To correct this problem, we suggest amending § 29.8(b) to incorporate the language used in the prefatory comments. Specifically, we suggest that the following should be added to the end of § 29.8(b) (a suggestion modeled on the language in 69 Fed. Reg. at 8,077):

> "The written agreement shall:
>
> > "(i) detail the responsibilities for handling, using, storing, safeguarding, disseminating, and destroying Protected CII;
> >
> > "(ii) require State and local governments to put in place procedures similar to those in § 29.9 for investigating suspected or actual violations of Protected CII procedures;
> >
> > "(iii) establish penalty provisions for unauthorized disclosure similar to those in § 29.9 and section 214 of the CII Act of 2002.
>
> "State or local governments that do not sign such an agreement with the Department shall not have access to Protected CII."

- The Supplemental Information in the Federal Register states that State and local governments "will be asked to track further disclosures." 69 Fed. Reg. at 8,079. Merely requesting the further tracking of information, however, is insufficient. Since DHS must grant permission before any further disclosure is made, 6 C.F.R. § 29.8(d)(2), DHS is in a better position to track the further disclosure of Protected CII than a State or local government; moreover, consistent with the Act, requiring DHS to track further disclosures will provide a central repository of this CII information. The regulation should therefore provide, in § 29.8(d)(2), that the Protected CII Program Manager (or his

or her designee) "shall track any further sharing of Protected CII and maintain a central record of any such sharing."

- 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.
- 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.
- We do not suggest in any way that States may only receive information related to critical infrastructure protection from DHS. Entities may decide to provide this information directly to the States in certain circumstances (if, for example, the State provides protections similar to those in the CII Act by statute, regulation, or binding agreement with the submitting entity).

Disclosures to Foreign Governments

Section 29.1(b) states that the procedures in the interim regulations apply to entities that "handle, use, or store Protected CII," including foreign governments, "pursuant to any necessary express written agreements, treaties, [or] bilateral agreements . . . ." 6 C.F.R. § 29.1(b). The Supplemental Information further states that "[a]s the Program evolves and agreements with additional entities are finalized, the disclosures of [Protected CII] information will expand . . . eventually to foreign governments," and that "[t]he Department believes that through the

establishment of formal agreements with foreign governments," Protected CII can be shared with foreign governments. 69 Fed. Reg. at 8,077.

It is unclear whether DHS contemplates disclosures of Protected CII to foreign governments beyond the limited "advisories, alerts, and warnings" specified in § 29.8(j). If so, it is doubtful whether such disclosures are permissible under the CII Act. In the Act, Congress designed a carefully calibrated scheme, balancing the necessity of encouraging the submission of information with the need for disclosures in certain limited circumstances. In striking such a balance, Congress permitted disclosures of Protected CII to State and local governments in certain situations, authorizing "the sharing of such information within the Federal Government and with *State and local governments*," 6 U.S.C. § 133(e)(2)(D) (emphasis added). There is, however, no analogous provision relating to the general sharing of information with foreign governments; rather, only limited "advisories, alerts, and warnings" to foreign governments are authorized. *See* 6 U.S.C. § 133(g) (permitting "advisories, alerts, and warnings" to "governmental entities"); *see also* 6 C.F.R. § 29.8(j).

Because of the ambiguity introduced by § 29.1(b) and the Supplemental Information, § 29.8(j) (which only permits limited "advisories, alerts, and warnings" to foreign governments) should be amended. The following sentence should be added to § 29.8(j): "Besides the disclosures relating to advisories, alerts, and warning detailed in this section, there shall be no disclosures of Protected CII to foreign governments without the written consent of the person or entity submitting such information."

If, however, DHS takes the position (contrary to the plain terms of the statute) that Protected CII may be shared more broadly with foreign governments if there is a sufficient written agreement between the United States and the foreign government, the regulations must

detail the requirements of such a writing. Such a writing must, *inter alia*, detail the procedures for handling, using, storing, safeguarding, and destroying Protected CII; state that such information must be held by a small number of high-level officials; state that Protected CII may not be further disclosed absent express written authorization from the CII Program Manager (which shall only be granted with written consent from the submitter); require criminal penalties in that country in the event that an officer or employee of the foreign government makes an unauthorized disclosure of Protected CII; and establish penalty provisions, including sanctions by the United States, if the foreign government (or one of its officers or employees) makes an unauthorized disclosure. *See also, e.g.,* "Protections Against Disclosure by State and Local Governments," *supra*. Absent such details, submitters will not be able to make informed judgments about whether the agreements with foreign governments will provide adequate protections; such uncertainty will likely discourage the submission of Protected CII to the Government, thereby undermining the purpose of the Act.

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, the regulations should be clear that entities may enter into separate binding agreements with governmental entities relating to the sharing of information. Members of private industry have entered into such agreements in the past and, since the clear intent of the

CII Act was to encourage the sharing of information with the Government, the regulations should expressly state that the Act and regulations do not preclude such agreements. 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."

"No Private Right Of Action" Provision

The first sentence of § 29.3(e) – involving private rights of action – contains a problematic ambiguity that is not present in the statutory language. The Department recognized this ambiguity when it changed the title of this provision from "No private rights or privileges" (in the proposed regulations) to "No private right of action." 69 Fed. Reg. at 8,081 ("The Department received one comment concerning the ambiguity introduced by the proposed rule's reference to 'no private rights or privileges' . . . . The Department agreed with this comment and has revised the interim rule to ensure that the regulation is consist[ent] with the statutory language."). However, while recognizing the ambiguity in the proposed regulations, DHS failed to correct the whole problem, as the first sentence of § 29.3(e) still refers to "privilege[s]." It is unclear what this sentence means: the statute does in fact grant providers of information certain rights and privileges, but states that there is no private right of action to enforce these rights and privileges. At best, the first sentence of § 29.3(e) introduces an ambiguity that is not present in the statute; at worst – and inconsistent with congressional intent – it may limit the scope of the statute's protections. The first sentence of § 29.3(e) should therefore be deleted, so that the provision more closely tracks section 215 of the CII Act, 6 U.S.C. § 134.

Affirmation Requirement

The interim regulations add an affirmation requirement, requiring that submitters state that "any false representations on such submissions may constitute a violation of 18 U.S.C. 1001 and are punishable by fine and imprisonment." 6 C.F.R. § 29.5(e). Such an affirmation requirement is at odds with the goal of the statute. As the regulations generally recognize, the success or failure of the Act depends on whether companies make voluntary submissions of Protected CII to DHS. There can be little doubt that § 29.5(e) – which implicitly threatens the possibility of criminal sanctions with each submission – will discourage the submission of information and, therefore, frustrate the purposes of the Act.

As an initial matter, § 29.5(e) misstates the law under 18 U.S.C. § 1001. Section 1001 does not apply to "any false representation[]," as § 29.5(e) suggests, but only to "knowingly and willfully" making a "materially" false statement. Given these threshold requirements, it is unclear whether the types of certifications required under § 29.5(a)(4) – which are generally akin to conclusions of law – could ever trigger § 1001. *See, e.g.*, 6 C.F.R. § 29.5(a)(4)(iii) (requiring certification whether the "information is or is not required to be submitted to a Federal agency" and, if so, requiring the identification of "the Federal agency requiring submission and the legal authority that mandates the submission"). The mere suggestion that § 1001 could apply in this context, however, will likely chill submissions of Protected CII, as companies might decide, in an abundance of caution, that the safer course is not to submit the information to DHS.

Requiring such an affirmation is also inconsistent with the spirit of the Act. The Act seeks to promote the protection of critical infrastructure through an innovative partnership between Government and private industry. The interim regulations accurately capture this spirit by adding § 29.5(d): "All submissions seeking Protected CII status shall be regarded as

submitted with the presumption of good faith on the part of the submitter." Requiring the affirmation, however, treats each submission with suspicion and, therefore, runs counter to the spirit of the Act.

These costs are not justified, as the affirmation provides no benefits. To the extent that the criminal provisions of 18 U.S.C. § 1001 even apply in this context, they apply whether or not there is an affirmation; therefore, the affirmation is either misleading or not needed. Moreover, the affirmation is not needed to counter the problem that DHS seeks to address. According to the Supplemental Information in the Federal Register, "[t]he intent of [this] provision is to provide a remedy to prevent a party [1] from repetitively submitting information in bad faith solely to consume agency resources and [2] from submitting information in an attempt to shield from the public any evidence of wrongdoing." 69 Fed. Reg. at 8,077. As to the latter concern, no such contingency is possible, as the CII Act in no way limits the Government's powers regarding information that is already in its possession, nor does it relieve entities from complying with independent regulatory requirements. As to the former concern – that some entities may "repetitively submit[] information in bad faith solely to consume agency resources" – the possibility of such a scenario is beyond remote. If an entity submits information that does not qualify for protection, it will simply not receive the protection of the Act. Indeed, it is hard to imagine how or why the contingency that DHS is concerned about could come to pass. Simply put, the important goals of the Act should not be frustrated in order to protect against a speculative (and extremely unlikely) hypothetical. The affirmation requirement of § 29.5(e) should be eliminated.

Comments on Additional Provisions

Section 29.3(d): "Independently obtained information"

We support the change from the proposed regulations that clarifies that "[i]independently obtained information" does not include any information derived "indirectly from Protected CII." 6 C.F.R. § 29.3(d). This provision, however, should be further clarified to state that information derived "indirectly" from Protected CII (and therefore not independently obtained) includes information that the Government learns of only because of its submission to the Government under the Act. In other words, if the Government learns of information only because it was submitted as Protected CII, the regulation should expressly prohibit the Government from seeking that information through another means. Section 29.3(d) should also state that, if any question arises whether the information was "independently obtained," the governmental entity should be required to demonstrate that the information was not obtained indirectly from the submission of Protected CII.

Section 29.5: "Requirements for Protection"

Section 29.5(a)(4) states that the submission of CII shall be accompanied by a certification. That section should also state that such certification shall be treated as Protected CII to the same extent as the underlying information.

Section 29.6: "Acknowledgment of Receipt, Validation, and Marking"

Section 29.6(c) states that Protected CII must be marked with, *inter alia*, the following words: "Unauthorized release may result in civil penalty or other action." This marking,

however, does not properly state the range of possible penalties under § 29.9(d) and section 214(f) of the Act, 6 U.S.C. § 133(f), which explicitly delineates certain criminal and administrative penalties. The marking of § 29.6(c), therefore, should capture the range of penalties set forth in § 29.9, and state that "[u]nauthorized release may result in criminal penalties, including imprisonment and fines, and civil and administrative penalties, including removal from office or employment."

Section 29.6(e)(2)(E) should be amended to state that, in those instances in which the CII Program Manager determines that information is not Protected CII, DHS must return the information to the submitter. According to the Supplemental Information, DHS rejected this suggestion due to the "significant administrative burden[s]" such a requirement would place on DHS. 69 Fed. Reg. at 8,080. It is hard to see how requiring the return of the information would entail a "significant administrative burden" on the agency: in fact, requiring the return of information would seem less administratively burdensome than the other alternatives. To minimize any administrative burden, DHS could require that the submitter arrange to have the information picked up from the Department or pay the costs associated with the return of information. Return of the documents is particularly important because DHS may be unable to insure immediate destruction of the documents under the Federal Records Act, thus leaving submitters at risk that sensitive information may be subject to a FOIA request or other disclosure. The prospect that a submitter might face such a risk will likely discourage submission of CII to DHS.

Section 29.6(f), which states that the CII Program Manager or its designee may change the designation from CII to non-CII, should be clarified. First, submitters of information need to be confident that this important decision is made by the CII Program Manager him or herself,

and not by one of many designees. Second, as written, the CII Program Manager may make this decision without any input from the submitter and, as such, there is a high risk of erroneous determinations. As a result, the regulation should state that the CII Program Manager must provide notice to the submitter, and an opportunity for the submitter to be heard, before changing a designation from Protected CII to non-Protected CII. If, after such consideration, the information is deemed to be non-protected, then the information should be returned to the provider.

Conforming Changes: "Executive Order 12886 Assessment," "Costs," and the "Initial Regulatory Flexibility Determination"

Finally, there are inconsistencies – relating to the storage of Protected CII – between the interim regulations and the accompanying text in the Federal Register that should be clarified.

In the proposed regulations, § 29.7(b) stated that a "locked desk or file cabinet" would constitute a "secure" environment for the storing of Protected CII. 68 Fed. Reg. 18,524, 18,527 (Apr. 15, 2003) (proposed rules). In response to comments, *see* 69 Fed. Reg. at 8,079, the interim regulations deleted this language, now providing that Protected CII must be stored in a "secure environment that affords it the necessary level of protection commensurate with its vulnerability and sensitivity." 6 C.F.R. § 29.7(b).

However, the "Executive Order 12886 Assessment," "Costs," and the "Initial Regulatory Flexibility Determination" in the Federal Register all reflect the previous iteration of the regulation, and presume that a locked drawer or file cabinet provides sufficient safeguards. *See* 69 Fed. Reg. at 8,081 (Executive Order 12866 Assessment) ("Under the rule, a locked drawer or cabinet is an acceptable means of complying with the requirement to secure Protected CII . . . ."); 69 Fed. Reg. at 8,081 (Costs) ("[A] normal filing cabinet with a lock may be used to safeguard

Protected CII . . . ."); 69 Fed. Reg. at 8,082 (Initial Regulatory Flexibility Determination) ("[A] normal filing cabinet with a lock may be used to safeguard Protected CII."). These descriptions should be amended to conform with the interim regulations, so that the regulations and accompanying analysis are consistent.

* * * * * *

We again commend the interim regulations, but ask that you consider our proposed clarifications and modifications in order to give the Act its intended effect.

Submitted by:

Qwest Communications
1801 California Street, Suite 1160
Denver, CO 80202