

United Parcel Service.txt

Subject: NPRM, Procedures for Handling Critical Infrastructure Information
Date: Mon, 16 Jun 2003 15:47:26 -0400
From: "Bergman Bob (nat5rxb)" <nat5rxb@UPS.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Dear Sir/Madam:

Attached please find the comments of United Parcel Service regarding the NPRM on Procedures for Handling Critical Infrastructure Information. We will follow with a signed original and three copies.

Robert A. Bergman
Vice President
United Parcel Service
316 Pennsylvania Ave., SE, Suite 300
Washington, DC 20003
202-675-3354
202-675-4230 (fax)
bbergman@ups.com

<<CII - Comment 6 CFR Part 29_v1_.doc>>

	Name: CII - Comment 6 CFR Part 29_v1_.doc
	Type: WINWORD File (application/msword)
CII - Comment 6 CFR Part 29_v1_.doc	Encoding: base64
	Description: CII - Comment 6 CFR Part 29_v1_.doc

Comments of United Parcel Service
Notice of Proposed Rulemaking
Procedures for Handling Critical Infrastructure Information
Department of Homeland Security
RIN 1601-AA14

June 16, 2003

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

Re: Proposed Rules, 6 C.F.R. Part 29, Procedures for Handling Critical
Infrastructure Information

Dear Sir/Madam:

United Parcel Service is pleased to present written comments to the Department of Homeland Security (the "Department"), pursuant to 68 Fed. Reg. 18524-01 (2003), concerning proposed 6 C.F.R. Part 29 (the "Proposed Regulation"), which sets forth Procedures for Handling Critical Infrastructure Information ("CII") to implement 6 U.S.C. §133(e)(2002).

Section 214 of the Homeland Security Act, codified at 6 U.S.C. § 133, is, in our understanding, reflective of Congress's recognition of the importance of information held by the private sector to the nation's security from terrorist attacks. Accordingly, the statute delegates authority to the Department to provide for a process to receive and protect CII that the private sector voluntarily submits to the Department to assist the government and the private sector in countering terrorist attacks to our critical infrastructure.

Congress also recognized in Section 214 that the voluntary submission of CII creates certain risks for private enterprise. In many cases, CII may include information that a private enterprise would consider a trade secret or confidential, or potentially damaging to the business if made known to competitors or other third parties. This creates a risk for corporate management, which owes a legal duty to shareholders to use reasonable care to protect the assets of the company. For example, improper disclosures of important corporate information can result in crippling litigation, which ultimately can lead to personal liability on the part of directors and officers.

Section 214 was designed to eliminate such risks through providing a mechanism to shield such information both from public disclosure and from use in subsequent civil litigation. UPS believes that the Proposed Regulation is an excellent initial attempt to fulfill this goal, and submits the following suggestions for the Proposed Regulation's improvement:

1. The Proposed Regulation Should Take Additional Steps to Protect CII that the Department Shares with State, Local, or Foreign Governments. Section 214 requires the Department to specify procedures regarding the protection of CII to permit sharing of the information with States and localities, among others. 6 U.S.C. § 133(e)(2). Such procedures are important because under the proposed regulation, sensitive information that a party submits to the Department to aid the Department in its efforts to protect the nation's security may, in theory, be shared with any governmental entity anywhere in the world. 6 C.F.R. § 29.8 (Proposed). This concern, if not addressed, could be a barrier to the attainment of the Department's goal of "encourag[ing] the voluntary submission of CII" 6 C.F.R. § 29.1 (Proposed).

The Proposed Regulation restricts the further disclosure of CII by States and localities, but only provides penalties for the improper disclosure of CII by Federal employees. In addition, private enterprise is left largely powerless to prevent improper disclosures or use by states, local or foreign governments. Without additional protections, private enterprise would be subject to an undue risk of improper disclosure of CII that UPS submits could be addressed through mechanisms that are within the discretion Congress afforded to the Department.

UPS therefore recommends that the Final Regulation include additional measures to protect the confidentiality of CII in connection with the sharing of that information with State, local, and foreign governments. UPS submits that the Proposed Regulations should provide that the Department would share CII with State, local, and foreign governments only under the following circumstances:

- a. The party submitting the CII to the Department consents to the disclosure; or
- b. The Department: (i) takes measures to protect from disclosure the source of the CII in accordance with proposed 6 C.F.R. § 29.8(e), which pertains to disclosures in connection with advisories, alerts, and warnings to certain entities and the general public; and (ii) provides the submitting party with an opportunity in advance to review the proposed disclosure to assist in the identification of proprietary and business-sensitive information.

2. The Proposed Regulation Should Prohibit the Transmission of CII Other Than by Secured Internal Federal Government Delivery Systems or Encrypted Electronic Communications. The Proposed Regulation provides an exclusive list of methods by which the Department may transmit CII, including first class or certified U.S. Mail. 6 C.F.R. § 29.7(e) (Proposed). This is less security than many private enterprises require internally for the transmission of information that may fall within the definition of CII. The Proposed Regulation as a result requires the private sector to assume an unnecessary heightened risk of loss or interception of that information.

UPS submits that the Proposed Regulation should require more secure means for the transmission of CII by the Department and any authorized parties that receive CII.

These methods could include, for example, internal Federal Government delivery systems and encrypted electronic communications.

3. Disclosure of Information to Federal Contractors Should Be Permitted only as Necessary, Pursuant to a Written Confidentiality Agreement, with a minimum set of protections and Subject to Criminal Penalties for Improper Use or Disclosure. The Proposed Regulation currently permits disclosure of CII to federal contractors as long as “the contractor is performing services in support of the purposes of DHS.” 6 C.F.R. § 29.8(c) (Proposed). This proposed Section provides that the contractors shall not further disclose CII, but does not limit the initial disclosure to contractors to the extent necessary, does not require a written agreement with a minimum set of protections with contractors to govern the disclosure (which agreement would not necessarily need to be tailored to each specific disclosure), and does not provide for an enforcement process for violations by contractors. UPS respectfully submits that these additional protections are reasonable and not overly burdensome, and would lessen the risk of improper disclosure or use of CII.

4. The Reservation of a Right to Use CII in Criminal Investigations and Prosecutions Makes It Less Likely That the Proposed Regulation Will Further the Policy of “Encourag[ing] the Voluntary Submission of CII” Private enterprises will be more reluctant to share CII voluntarily, will share less CII, and will take longer to share CII as a result of the Department’s reservation of a right for the Federal, State, and local governments who receive CII to use the information to investigate and prosecute alleged crimes. While this reservation originated in Section 214 of the Homeland Security Act, UPS submits that the Department has discretion to clarify this reservation in a manner that will provide increased certainty to private entities considering the voluntary submission of CII. The failure to do so, UPS submits, may unintentionally thwart the policy of encouraging the voluntary submission of CII.

As framed currently, one can interpret the exception for use in connection with criminal proceedings to apply to proceedings involving any entity, not just the submitting party. 6 C.F.R. §§ 29.8(d)(3), (f)(1)(i)(A) (Proposed). This significantly expands the risk for the private sector of disclosure of CII beyond the intended recipients. As a result, UPS submits that the Department should clarify the Proposed Regulation to provide that the exception for use of CII “in furtherance of the investigation or the prosecution of a criminal act” applies only to criminal proceedings involving conduct of the submitting party.

5. The Department Should Issue Guidelines Regarding Internal Handling of CII. Guidelines that specify the measures the Department takes to protect the secrecy of CII will increase the confidence of private enterprise in disclosing sensitive information under the Regulation. We recommend that such Guidelines specifically address information security, and cover the following areas:

- a. Establishment of a comprehensive written information security program, which includes security controls that are consistent with published National Institute of Standards and Technology (NIST) guidance.

- b. Implementation of the program, employee training, and internal audit processes.
- c. A process for identification, assessment, and correction of program and implementation deficiencies.
- d. A process for periodic requests, no less than annually, for an audit by the General Accounting Office of the program and the Department's information security practices with respect to CII.

In furtherance of creating an integrated set of security procedures governing CII submitted under Section 214, such Guidelines could be appropriately included in the commentary that would accompany the final CII regulation.

* * *

Thank you for your consideration of the foregoing comments in the Department's continued development of proposed 6 C.F.R. Part 29. If you have any questions, please contact me at 202-675-3354.

Sincerely,

Robert A. Bergman
Vice President