

New York State Office of Cyber Security.txt

Subject: 6 CFR Part 29 - commenets
Date: Fri, 13 Jun 2003 12:15:09 -0400
From: "Kevin Hanratty" <KHanratty@security.state.ny.us>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Please find attached comments from the New York State Office of Cyber Security & Critical Infrastructure Coordination and the New York State Office of Public Security on the proposed federal rules regarding the receipt, care, and storage of Critical Infrastructure Information voluntarily submitted to the Federal Government. A previous version sent yesterday did not contain letterhead with contact info for the Office of Cyber Security & Critical Infrastructure Coordination. Thank you,

Kevin Hanratty
Deputy Counsel
New York State Office of Public Security
633 Third Avenue
New York, NY 10017
Ph: (212) 867-7762
Fax: (212) 867-1725

<<6 CFR Part 29 comments.doc>>

	Name: 6 CFR Part 29 comments.doc
6 CFR Part 29 comments.doc	Type: WINWORD File (application/msword)
	Encoding: base64
	Description: 6 CFR Part 29 comments.doc



George E. Pataki
Governor

New York State Office of Cyber Security & Critical Infrastructure Coordination

30 South Pearl Street
Albany, NY 12207-3425



William F. Pelgrin
Director

MEMORANDUM

TO: Associate General Counsel (General Law), DHS

FROM: New York State Office of Cyber Security & Critical Infrastructure Coordination
and New York State Office of Public Security

DATE: June 11, 2003

SUBJECT: 6 CFR Part 29- Department of Homeland Security

Comments:

The New York State Office of Cyber Security & Critical Infrastructure Coordination and the New York State Office of Public Security would like to thank the Department of Homeland Security for the opportunity to comment on the proposed rules regarding the receipt, care, and storage of Critical Infrastructure Information voluntarily submitted to the Federal Government. By encouraging input at the critical rulemaking stages, we can help to ensure that new rules are well suited to their purposes and that they are crafted to impose as minimal a burden as possible on those affected by such rules.

- (1) There are some potential ambiguities in the language of the regulations other than the definitions and we recommend the following modifications:
 - a) § 29.3 Effect of provisions: (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. The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information or any other such information to a Federal agency under any other provision of law. Moreover, when information is required to be submitted to a Federal agency to satisfy a provision of law, it is not to be marked by the submitter, by DHS, or by any other

party, as submitted or protected under the CII Act of 2002 or to be otherwise afforded the protections of the CII Act of 2002.

The attempts above to carve out the exception sweep broadly and could be construed to prevent the very effect they are intended to have—enable information voluntarily submitted to the DHS to be specifically exempted from FOIA. To clarify, the language could simply read:

(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 **[other than DHS]**. 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. The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information or any other such information to a Federal agency under any other provision of law. Moreover, when information is required to be submitted to a Federal agency to satisfy a provision of law, it is not to be marked by the submitter, by DHS, or by any other party, as submitted or protected under the CII Act of 2002 or to be otherwise afforded the protections of the CII Act of 2002 **[unless 29.5 is applicable]**.

b) § 29.5 Authority to receive Critical infrastructure Information:

(2) The Federal agency or DHS component forwarding the information to the CII Program Manager may not disseminate, distribute, or make public the information until the CII Program Manager has notified the agency or component that the Program Manager has acknowledged and validated the information.

The above language implies that once the information received by DHS is verified that it can then be made public. Presumably it is intended that it be made public consistent with the provisions in 29.8. Accordingly, it can be worded:

(2) The Federal agency or DHS component forwarding the information to the CII Program Manager may not disseminate, distribute, or make public the information **[consistent with 29.8]** until the CII Program Manager has notified the agency or component that the Program Manager has acknowledged and validated the information.

c) § 29.6 Acknowledgment, validation, and marking of receipt:

- (ii) contains a provision that if the CII Program Manager determines that the information is not protected and if the

submitter does not notify the CII Program Manager whether to either destroy the information or maintain it without protection, then the information is to be destroyed unless it is retained for national security reasons. It is unclear how information can be considered so important to be retained for national security reasons, yet not necessary to receive the protection by the CII program manager. There should be a provision that if information is needed for national security purposes, then it will be declared to be protected by the CII Program Manager.

- The CII Program Manager may reject the request for validation. There is, however, no appeal process specified in the regulations and indeed that could be useful. Additionally, there are no criteria set forth in the regulations that give the “submitter” a clear understanding of the information needed by the CII Program Manager to render his/her determination.

d) § 29.7 Safeguarding of protected Critical infrastructure Information.

- (a) provides that all persons in possession of information are responsible for the control and safeguarding. There could be a description of the consequences for negligence or deliberate acts of unauthorized release.
- (b) provides for the use and storage of CII. This section addresses secure containers and includes locked desks or file cabinets or secure facilities. All the specified examples relate to physical security. This appears then to contemplate that all information will be submitted in “non- electronic” formats; (section “e” as referenced below seems to contemplate otherwise.) If some CII information is to be submitted electronically, it will accordingly be stored as such and electronic security should then be addressed in this section of the regulations.
- (e) addresses the transmission of information in “secure” means electronic means. By whom will it be determined what “secure” means will constitute?

d) § 29.8 Disclosure of information.

- (b) contemplates the dissemination to State and Local government entities upon “express agreement”. The type and content of this agreement are not specified. May the State and Local entities draft different agreements or is the CII Program Manager responsible to develop an applicable MOU?
- (d) prevents disclosure by State and Local entities to other parties without the express consent from the original submitter. This will be difficult to obtain quickly in emergencies. Accordingly, it would be helpful to have a provision allowing dissemination of such information based on the determination of the CII Program Manager in the event of an urgent need to do so.