

Subject: Procedures for Handling Critical Infrastructure Information
Date: Fri, 13 Jun 2003 17:13:44 -0400
From: "Gary Warner" <gar@askgar.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>
CC: "Melani Hernoud" <m.hernoud@SECURENETSYS.COM>,
"Betty Pierce" <b.pierce@SECURENETSYS.COM>,
"Richard Clarke" <rac@goodharbor.net>

Mr. Frank Nolan
Associate General Counsel
General Law
Department of Homeland Security
Washington, DC 20528

Mr. Nolan,

Thank you for the opportunity to provide comments on the Procedures for Handling Critical Infrastructure Information. As concerned members of InfraGard, I have been joined by Betty Pierce and Melani Hernoud in preparing these comments. Mr. Richard Clarke, recently of the CyberSecurity office of the White House, served as our advisor in this process.

If there are further questions we would be happy to answer them at your convenience.

For your convenience, the comments of the attached word Document have been printed and will be delivered with original and 3 duplicates to the Remote Delivery Site (245 Murray Drive Bldg 410) via FedEx.

Thank you,

Gary Warner
Birmingham InfraGard
gar@askgar.com
205.326.8452

Betty Pierce
Denver InfraGard
b.pierce@securenetsys.com
303.637.7617

Melani Hernoud
Denver InfraGard
m.hernoud@securenetsys.com
303.637.7617

```

Name: DHS.response.PCII.doc
DHS.response.PCII.doc  Type: WINWORD File (application/msword)
                        Encoding: base64
                        Description: DHS.response.PCII.doc

```

Concerning the Implementation Of
The Critical Infrastructure Information Act of 2002
Procedures for Handling Critical
Infrastructure Information

RIN: 1601-AA14

Comments from

Gary Warner, Birmingham InfraGard
Betty Pierce, Denver InfraGard
Melani Hernoud, Denver InfraGard

Advisor:

Richard A. Clarke

DHS -- Procedures for Handling Critical Infrastructure Information

The authors would like to thank the Department of Homeland Security for the invitation to submit comments on the Procedures for Handling Critical Infrastructure Information.

Since its inception in 1996, InfraGard has been dedicated to increasing the security of the critical infrastructures of the United States of America. All InfraGard participants are committed to the proposition that a robust exchange of information about threats to and actual attacks on these infrastructures is an essential element to successful infrastructure protection efforts. InfraGard is committed to Information Sharing: sharing between our members and the National Infrastructure Protection Center; sharing between our members and the Federal Bureau of Investigation; and sharing between our members with each other and with other Infrastructure Providers in the private sector. With more than 8,200 members representing all of the nation's Critical Infrastructures, InfraGard is one of the largest and oldest existing groups committed to Infrastructure Protection through Information Sharing. This is why we are especially grateful that DHS has chosen to hear our voice and our concerns as we consider the Rulemaking at hand.

It is critical to our purpose that any action taken by DHS with regards to critical infrastructure information (CII) have the desired effect of increasing levels of sharing. In order to achieve this goal, we ask that we focus on three areas:

- I. Ensuring that private or sensitive information be protected, and that the status is known at all times to the submitter
- II. Ensuring the free flow of CII to needed parties, and preventing information from being shared with unwanted parties
- III. Ensuring that existing Information Sharing and Analysis Organizations (ISAO) be recognized and encouraged, rather than hindered by this rulemaking

I. Ensuring that private or sensitive information be protected, and that the status is known at all times to the submitter

The reason for the CII Act of 2002 to come into being is that companies and individuals hesitate to share information with the government which may later be revealed in such a way that may bring harm, risk, retribution, or retaliation against the submitting company. Because of this, there is strong language in the act to provide “Presumption of Protection”. This language is undermined within the same Act in ways which will cast doubt on the process and lead to less information sharing if the concerns raised are not adequately addressed.

Sec. 29.6 (b) Presumption of Protection. All information submitted in accordance with the procedures set forth herein will be presumed to be treated as Protected CII from the time the information is received by a Federal agency or DHS component. The information shall remain protected unless and until the CII Program Manager renders a final decision that the information is not Protected CII.,

Section 29.6 (e)(i)(D) Request the submitter to state whether, in the event the CII Program Manager makes a final determination that any such information is not Protected CII, the submitter prefers that the information be maintained without the protections of the CII Act of 2002 or be disposed of in accordance with the Federal Records Act.

Concern: Information intended to be “Protected” may not receive a Protected designation after review by the CII Program Manager. If the information was not submitted directly to DHS, but was referred through another Federal Agency or ISAO, what mechanism is in place to ensure that the desired will of the submitter is executed on copies of CII not in the possession of the DHS?

The inclusion of seemingly arbitrary clauses which allow information to become Unprotected after having previously received Protected status cause serious concerns and will potentially undermine the willingness of members to share information with DHS.

Sec 29.6 (f) In the event the CII Program Manager determines that any information is not submitted in good faith accordance with the CII Act of 2002 and these procedures, the Program Manager is not required to notify the submitter that the information does not qualify as Protected CII. This is the only exception to the notice requirement of these procedures.

Concern: “not submitted in good faith” is a very inadequate statement that creates a loophole large enough to invalidate all other portions of this Act. “Good faith” must

be defined, and perhaps illustrated with examples to help potential submitters understand that this will not be used in an arbitrary manner.

Sec 29.6 (g) Changing the status of CII to Non-CII. Only 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.

Concern: At the time of submission all information is considered PROTECTED until designated otherwise. The submitter has the means to indicate that if the Protected status is not granted, the information is to be destroyed. Does 29.6 (g) follow similar guidelines? If not, this clause carries a serious impact which could cause submitters to withhold their information. If such an event occurred, how would DHS ensure that previously disseminated copies of the PCII would also be destroyed?

II. Ensuring the free flow of CII to needed parties, and preventing information from being shared with unwanted parties

Our member companies have expressed, both through their membership in InfraGard, and their participation in our organization, a desire to do their patriotic duty and help protect the critical infrastructures of this nation. This patriotic desire is at times in conflict with the desire of our members' legal departments to ensure that no trade secrets, competitive information, or vulnerabilities be exposed to potential competitors, litigants, terrorists or enemies.

Sec. 29.8(e) Disclosure of information to appropriate entities and the general public. The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential threats to critical infrastructures as appropriate. In issuing a warning, the IAIP Directorate shall protect from disclosure the source of any voluntarily submitted CII that forms the basis for the warning; and any information that is proprietary, business-sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

Because of this need to protect our members from exposure, it has been the practice of InfraGard to accept two copies of information. One report, to be shared only within NIPC and other government agencies, contained full disclosure of the incident or event at hand. The other report, called a "Sanitized Report", was prepared BY THE MEMBER COMPANY in such a way that pleased their legal staff that no business sensitive or identifying information would be revealed.

Concern: Will the submitter be allowed to review information to be released? It may be that only the submitter may accurately identify something that would be "business sensitive" or "identifying" within their information. Could the InfraGard practice of submitting a "Sanitized Report" be adopted for this purpose?

The establishment of the CIIMS database seems to be to create consistent accountability for the stewardship of the CII data. However, this accountability may prove difficult to enforce once data is shared outside of DHS.

Sec 29.1 (4) ... "permits the sharing of such information within the Federal Government and with Foreign, State, and local governments"

Sec 29.4 (c) ... “The CII Program Manager shall establish procedures to ensure that any DHS component or other entity that works with Protected CII appoints one or more employees to serve as a CII Officer” . . . “Persons appointed to these positions shall be fully familiar with these procedures”

Sec 29.4 (e) ... “CIIMS, a system to record the receipt, acknowledgement, validation, storage, destruction, and disclosure of Protected CII.”

Concern: Information that has been shared voluntarily in good faith for the protection of the United States of America may be withheld if submitters realize the information may also be shared with Foreign Governments. Will Foreign Governments be required to establish and train CII Officers? Will they be given access to the CIIMS database?

Concern: Local governments often lack the sophistication to properly handle sensitive information. Will DHS require local governments to establish and train a CII Officer before being entrusted with PCII? Will they be given access to the CIIMS database?

Concern: In the event, as above, that CII loses its protected status, how will DHS ensure the destruction of copies of this information in the possession of Foreign, State, and Local governments?

Sec 29.8 (f) ... “Protected CII shall not, without the written consent of the person or entity submitting such information, be used or disclosed . . . except —

Concern: With so many exceptions . . . Anything Congress wants to do, Anything that evidences “a gross waste of funds”, an abuse of authority, etc., we have once again created a large “loophole” through which Protected CII may be shared, without disclosure, for purposes contrary to those for which the information was granted to DHS by the submitter. Because Congress, and anyone involved in the investigation of “gross waste of funds” or “investigation or prosecution of a criminal act” has other means of obtaining this same information from the original source, it is STRONGLY recommended that request for this information be referred to the original source, and sought under subpoena in the same fashion they would be sought if the information had not been shared with DHS.

III. Ensuring that existing Information Sharing and Analysis Organizations (ISAO) be recognized and encouraged, rather than hindered by this rulemaking

The authors consider InfraGard to be an Information Sharing and Analysis Organization and would request that we be recognized as such as per the definition and purposes of the Act.

Sec 29.8 (e) Disclosure of information to appropriate entities and the general public. The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential threats to critical infrastructure as appropriate. . .

We think InfraGard would benefit from being informed of important information as per 29.8 (e), we feel that our organization of 8,200+ members, many of whom have extensive backgrounds in cyber security, and many of whom have extensive industry-specific infrastructure backgrounds, may be able to provide assistance in areas that are only listed in Sec 29.8 (b) as follows:

Sec 29.8 (b) . . . “provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for other information purpose relating to homeland security.”

In the Act, Section 29.8 (c) allows for this type of information to also be shared with Federal contractors. Would InfraGard be allowed to receive information for analysis and study which would be disseminated internally only to members designated as CII Officers after appropriate clearances are obtained?

Sec 29.5 (b) (3) (i) In the case of written information or records, through a written marking on the information or records substantially similar to the following: “This information is voluntarily submitted to the Federal Government in expectation of protection from disclosure as provided by the provisions of the Critical Infrastructure Information Act of 2002”

Sec 29.5 (c) Information that is not submitted to the CII Program Manager, either directly by the submitter or indirectly through another Federal agency by request of the submitter, will not qualify for protection under the CII Act of 2002.

Sec 29.5 (c)(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.

Sec 29.6(d)(1) [The CII Program Manager shall] Contact the submitter . . . within 30 days of receipt

Concern: InfraGard is not a Federal Agency in the sense of the sections above.

To further enhance the sharing of information between InfraGard members and DHS, it is hoped that we can receive guidance from DHS to automatically submit information to be marked as “Protected” upon receipt by InfraGard or its agents, after receiving an appropriately worded request from the submitter. Perhaps this will be accomplished using our relationship with the Federal Bureau of Investigation to provide the required “Federal Agency”.

Concern: Unfortunately, the communication of threat information “within 30 days” is almost never an adequate timeframe to allow protective measures to be taken, especially with regards to cyber activities. How might information of a time-sensitive nature be escalated so that alerts may be disseminated to the InfraGard membership the same day, or perhaps the same hour, that they are received?

If InfraGard continues its practice of using a “Sanitized Report”, could the “Full Report” be submitted for Protection under the guidelines above, while the “Sanitized Report”, which contains no information deserving of special protection, be released to membership in a more timely fashion?

The authors would be pleased to provide any additional response or dialogue as requested.

Gary Warner
205.326.8452
gar@askgar.com

Betty Pierce
303.637.7617
b.pierce@securenetsys.com

Melani Hernoud
303.637.7617
m.hernoud@securenetsys.com