WORKING GROUP ON COMMUNITY RIGHT-TO-KNOW

218 D Street, SE
Washington, DC 20003

www.crtk.org

Telephone: (202) 544-9586
Facsimile: (202) 546-2461

May 20, 2004

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

Re: Procedures for Handling Critical Infrastructure Information (69 FR 8073)

We are writing to urge the Department of Homeland Security (DHS) to limit the Critical Infrastructure Information program to prevent manipulation by irresponsible companies.

First, DHS should reinstate the definition of "good faith" to exclude from protection as CII any information that describes or implies a violation of any law. Since the CII program exempts submitters from civil liability, it is not "good faith" to submit information in order to take advantage of this exemption. The clearest standard that DHS could apply would be to reject and return to the submitter any CII that discloses a violation of law. In addition, DHS should require companies that submit CII to take reasonable steps to address vulnerabilities identified in a submission. Failure to do so should constitute a breach of "good faith" and remove any restriction on the government's use of the information to warn the public, take regulatory action, or litigate.

Second, in the final rule, DHS should not allow companies to submit CII information to or through other agencies. DHS is considering extending the program to include information submitted to other federal agencies. However, this policy is not authorized in the statute. This policy would have negative consequences on other agencies' efforts to protect the public. This policy would hamper agencies' ability to conduct inspections and enforce laws. Since CII information cannot be used for any regulatory action, allowing the information to pass through regulatory agencies would taint the actions of these agencies, making enforcement more difficult. DHS must acknowledge that substantive work protecting critical infrastructure takes place through the enforcement by other agencies of laws and regulations. DHS should not allow the CII program to interfere with the work of regulatory agencies to protect the nation from critical infrastructure vulnerabilities.

Third, DHS should periodically review submitted CII to make sure that it still qualifies as CII. Because CII information is exempt from disclosure under the Freedom of Information Act, DHS will need to determine both that submitted CII meets the FOIA exemption standard and that it meets the FOIA exemption standard over time. For this reason, DHS should establish a re-review process to confirm that the information still qualifies for protection. This re-review process should be both periodic and triggered

upon receipt of FOIA inquiries. If the type of information submitted by a single submitter becomes commonly public over time, then the CII submission should no longer remain secret.

Fourth, DHS should require submitters to mark the specific portions of a submittal that the submitter intends should qualify as CII. Essentially the whole submission will be secret as proposed now, rather than just the CII portions. DHS has not justified its assertion that "requiring submitters to 'portion mark' material at the time of submission may impede the full disclosure of information." Any burden of portion marking material would be nominal at best. Nor has DHS explained why the agency cannot portion mark information if requiring the submitter to do so is too much of a burden. The real problem seems to be that DHS does not have the necessary information systems in place to manage information that is part secret and part public.

Fifth, DHS should summarize and report on the general scope of information submitted as CII, such as the number of CII submissions, the number of companies submitting CII, and the industry sectors represented. Most importantly, DHS should periodically report on the number of submissions that did and did not result in action to fix critical infrastructure vulnerabilities, and the general nature of any such actions.

Sincerely,

Paul Orum, Director
Working Group on Community Right-to-Know
218 D Street, SE; Washington, DC 20003
orum@crtk.org