May 20, 2004

Ms. Janice Pesyna
Ofiice of General Counsel
Department of Homeland Security
Wsahington DC 20528

Filed by Electronic Mail to cii.regcomments@DHS.gov

Subject: Department of Homeland Security Procedures for Handling Critical Infrastructure Information; Interim Rule published February 20, 2004

Dear Ms. Pesyna:

This letter describes the comments of Environmental Defense on the Department of Homeland Security's (DHS) Interim Rule to Implement the Critical Infrastructure Information (CII) Act. Environmental Defense, a leading national nonprofit organization, represents more than 400,000 members. Since 1967, Environmental Defense has linked science, economics, law and innovative private-sector partnerships to create breakthrough solutions to the most serious environmental problems.

We are concerned that some of the overly broad provisions of the rule may provide irresponsible corporations with a way to hide wrongdoing and avoid taking reasonable steps to eliminate or significantly reduce infrastructure vulnerabilities. Our specific comments are below.

1. Limit CII protections to information submitted directly to DHS and not to other federal agencies. The Interim Rule contains an appropriate limitation on the use of other federal agencies as conduits for CII. I understand however, the DHS is considering such an extension to other federal agencies. Such an action is contrary to the legislative history of the Homeland Security Act and is bad policy. Because the agencies cannot use the information, it confers no benefit to them and potentially hamstrings their efforts to carry out their mandate. To avoid any implication that they are misusing CII-protected information, agencies will be reluctant to pursue enforcement or other important regulatory actions. It also could give irresponsible companies an excuse to challenge agency actions and avoid compliance.

Further hampering the actions of other federal agencies is wording in Section 29.3(a) of the Interim Rule which appears to allow companies to hide even information that is legally required to be submitted. The sentence that reads:

> "Information submitted to any other Federal agency pursuant to a federal Legal requirement is not to be marked as submitted or protected under the CAA Act of 2002 or otherwise afforded the protection of the CII Act provided however, that such information, if it is separately submitted to DHS pursuant to these procedures may upon submissions to DHS be marked as Protected CII or otherwise afforded the protections of the CII Act of 2002."

This provision is contrary to the letter and intent of the CII Act and should be fixed. For information to be protected it must be "voluntarily submitted." That means that information that is legally required should NOT be accorded CII protections no matter where what agency receives it.

2. Require a standard re-review procedure so that the CII program does not become a permanent black hole for information. DHS should periodically re-review a submission to confirm that the information still qualifies for protection under the program. If over time the type of information submitted becomes commonly found in public domain, the information from a single submitter should not remain secret and protected. In addition to the scheduled re-review, it seems reasonable that requests for any information protected under the CII program trigger an assessment process to confirm the information still qualifies for protection.

3. Require that submitters fix the vulnerability identified in the submission. For example, our recent report, *Eliminating Hometown Hazards* (available at www.environmentaldefense.org/go/hometownhazards), describes what some wastewater facilities are doing to adopt cost-effective approaches that eliminate the risk of a terrorist attack. However for every one facility that has eliminated the risks, three more continue to use deadly chemical in heavily populated areas, despite the widespread availability of safer options. It would be a distortion of DHS's mission if those recalcitrant facilities used the CII Act protections to hide the potential consequences and avoid taking steps to reduce their vulnerabilities.

Failure to take all reasonable steps to reduce infrastructure vulnerabilities should constitute a breach of good faith and remove all restrictions on the government's use of the information to warn the public, take regulatory action, and litigate. Such a provision would clearly announce that this program will not become a safe haven for violators and laggard companies looking to avoid their responsibilities.

Thank you for the opportunity to comment on the Interim Rule. I hope DHS will make these changes to ensure that the vulnerabilities to potential terrorist attacks are eliminated or significantly reduced and that the program is not misused or corrupted by irresponsible companies.

Sincerely,

Carol Andress
Environmental Defense
1875 Connecticut Ave
Washington DC 20009