From: James Benton [mailto:jbenton@commoncause.org]
Sent: Tuesday, May 18, 2004 2:15 PM
To: Janice Pesyna
Subject: Limit the CII Program and Stop Irresponsible Companies

James Benton
Legislative Representative/Research Analyst
Common Cause
1250 Connecticut Avenue NW
Washington, DC 20036

May 18, 2004

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

Dear Pesyna:

I am writing to urge DHS to limit the Critical Infrastructure Information (CII) program so it accomplishes its task of securing our nation's critical infrastructure. DHS should also keep the CII program from becoming so broadly structured that it becomes a "safe haven" for companies dragging their feet to correct infrastructure problems that threaten our security. Likewise, it should not be allowed to become a shield from criminal or civil punishment for corporate malfeasance.

DHS can help accomplish this by drafting a final rule that requires any and all CII program submissions be made directly to the DHS, not through any other federal agencies. I understand that DHS is considering expanding the program to allow submissions through other federal agencies in the final rule. It would be poor planning -- not to mention redundant and potentially dangerous -- to allow CII submissions to flow through these agencies to DHS. The law does not allow these regulatory agencies to use the information. When the agencies take regulatory action in the future it could create the appearance that the agency is misusing the CII submission it received. Indeed, such a provision could provide companies with a poor legal excuse to challenge any regulatory actions in court, therefore avoiding compliance with any number of laws. Furthermore, as daily references to the increased possibility that terrorists may again try to mount an attack on U.S. soil, it is critical that DHS be able to move swiftly to secure elements of our nation's infrastructure that may be at risk. We have learned from the 9/11 commission that a lack of

coordination among agencies, combined with turf battles and the failure of top leaders to pay attention to the warning signs helped allow the 9/11 attacks, and may have prevented prophylactic antiterrorism measures. DHS does not have the time or money to develop this program broadly, especially given the warnings of a potential terrorist attack, and therefore should keep the CII program narrowly focused.

The final rule should include a standard review procedure to keep the CII program from becoming a permanent black hole for information. DHS should periodically re-examine a submission to ensure the information still qualifies for CII protection. 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 a assessment process to confirm the information still qualifies for protection.

I encourage DHS to state in the final rule that submitters must take all reasonable steps to address vulnerabilities identified in a submission. Failure to do so should constitute a breach of good faith and revoke 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.

Over the life of the Department of Homeland Security, many Americans have watched this department morph into a "superagency" that operates in private and consumes billions of dollars each year -- all without demonstrating to the American public that it is taking concrete steps to make the country safe from terrorist attack. By taking the above actions requested on the CII program, you will ensure that this innovative and well-meaning program will protect citizens while remaining as impervious as possible to fraud, misuse or manipulation.

Thank you.

Sincerely,

James C. Benton
Legislative Representative/Research Analyst
Common Cause