From: Matthew Bartkewicz [mailto:matt_bartkewicz@HOTMAIL.COM]
Sent: Wednesday, May 19, 2004 3:50 PM
To: Janice Pesyna
Subject: Limit the CII Program and Stop Irresponsible Companies

Matthew Bartkewicz
321 Main St.
Port Monmouth, NJ 07758

May 19, 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 program and not allow it to become a safe haven for irresponsible companies dragging their feet on fixing infrastructure problems.

The final rule should retain the requirement that any and all submissions to the CII program must be made directly to the DHS and 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 to allow CII submissions to flow through these agencies to DHS, as the law does not allow 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.

The final rule should include 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 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 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.

I sincerely hope DHS will make these changes to reduce the risk that this innovative and well-meaning program will not be vulnerable to misuse and manipulation.

Thank you.

Sincerely,

Matthew Bartkewicz