May 20, 2004

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

Emailed to: cii.regcomments@DHS.gov

Dear Ms. Pesyna:

OMB Watch appreciates the opportunity to comment on the Department of Homeland Security's (DHS) interim final rule for enacting the Critical Infrastructure Information (CII) subtitle of the Homeland Security Act of 2002. DHS clearly considered the comments it received during the public comment period for the CII proposed rule, and made several improvements to the rule as a result. OMB Watch believes that the rule still needs significant changes in order to produce a manageable CII program that will protect our country's infrastructure and citizens. We urge DHS to take this public comment opportunity to further refine the program.

OMB Watch is a nonprofit research and advocacy organization that has as its core mission government accountability and improving citizen participation. Public access to government information has been an important part of our work for more than 15 years. For example, in 1989, we launched RTK NET, an online service providing public access to environmental data collected by EPA, which has given us both practical experience and policy experience with disseminating government information. Additionally, OMB Watch has been very engaged in agency regulatory processes, encouraging agency rules to be sensible and more responsive to public need.

Overview

OMB Watch understands the desire to obtain more information about infrastructure vulnerabilities during these times of heightened security. Indeed, such actions seem prudent and well deserved. The CII program attempts to appease this want. The logical goal of this program must be two fold – identifying **and** addressing vulnerabilities and weakness within our nation's critical infrastructure. However, we are concerned that the CII program, as designed in the interim final rule, overlooks what should be the primary purpose of the program and instead caters to the interests of industry. It does this by prohibiting regulatory action on any problems identified in submissions. It does this by safeguarding industry from any civil action if a problem were to worsen. Without more significant safeguards against inaction, the CII program risks becoming a bureaucratic dead-end into which companies can dump their documents

1742 Connecticut Ave NW
Washington, DC 20009
tel: 202.234.8494
fax: 202.234.8584
email: ombwatch@ombwatch.org
web: http://www.ombwatch.org

detailing infrastructure weaknesses and the do little or nothing to correct the problems. This program should not recklessly diminish both the public's and the government's ability to act on threats.

Many of the CII program's worst flaws are dictated by congressional statute and lie outside DHS's authority to alter in this rulemaking. However, DHS retains a significant level of discretion concerning the program's definitions, details and procedures. OMB Watch urges DHS to improve these areas of program management and implementation.

The interim final rule contains notable management changes, improvements even, from the initial proposed rule. Unfortunately, the improvements are minor and do little to counter the more serious and fundamental flaws in the CII program. Among the improvements made in the interim CII rule:

- The program only allows direct submissions to DHS.
- The rule contains strengthened statements explaining that information required by any other federal agencies cannot qualify as protected CII.
- Submitters must provide a fairly strong express statement attesting that the submitted information meets the CII program criteria and is not required under law by any federal agency.
- The rule allows for the change in information's protection status if it becomes available through other legal means, it becomes customary for the information to be in the public domain, or DHS requires the submission of the information.
- The provision addressing disclosures includes an acknowledgement that certain unauthorized disclosures of CII would qualify as whistleblowing under the Whistleblowers Protection Act (WPA) and be exempt from any penalties.

Although OMB Watch commends DHS on instituting the above changes in response to public comments, these improvements do not ensure that irresponsible companies will not abuse the CII program by dragging their feet on fixing infrastructure problems. The remainder of this analysis will focus on the most troubling components of the interim final rule and recommend specific improvements the final rule should adopt.

Submission of Information

In the interim final CII rule, DHS states its intention to lift the restriction preventing companies from submitting CII through other federal agencies. The process DHS outlined in the proposed rule would allow federal agencies to accept CII submissions and forward them on to DHS. OMB Watch strongly objected to the definition of "submission to DHS" in the proposed CII rule, which included "indirect submissions" through any other federal agency. Even though the interim final rule restricts CII submissions, DHS stated in the "Discussion of Comments and Changes,"

> After the Protected CII Program has become operational, however, and pending additional legal and related analyses, the Department anticipates the development of

> appropriate mechanisms to allow for indirect submissions in the final rule and would welcome comments on appropriate procedures for the implementation of indirect submissions.

As the law does not allow regulatory agencies to use the information, it would be poor planning to allow CII submissions to flow through agencies to DHS. If other agencies receive and handle CII submissions it could create the appearance that the agencies are misusing the CII submissions when the agencies take regulatory action in the future. Such a system could severely restrict other agencies' abilities to operate effectively. Indeed such a provision could provide companies with enough of a legal excuse to challenge any regulatory actions in court and avoid compliance with any number of laws. For instance, if a chemical facility submitted CII through the Environmental Protection Agency (EPA), during EPA's next inspection of the facility the company could claim that EPA unfairly targeted them because of its CII submission. It could thereby potentially avoid responsibility for any problems discovered during the inspection.

In the "Discussion of Comments and Changes" section of the interim final rule, DHS recognized some of these problems and unintended consequences.

> Recognizing that, at this time, implementation of such a provision would present not only operational but, more importantly, also significant program oversight challenges, the Department has removed references throughout the rule to indirect submissions.

Unfortunately, DHS appears to believe that this is merely a simple procedural problem that would be easily fixed. Such an approach unwisely ignores the potential for these submissions to interfere with agencies' effectiveness, as outlined above. Additionally, a CII program that allows all federal agencies to accept and handle submissions would be much more difficult to manage. There is simply no reason to create an overly large and disjointed program that would be more prone to communication problems, uneven implementation, and diversion of agency resources from their primary duties. Maintaining the simpler and more efficient process of a single receiving agency minimizes confusion, delays, and other problems.

It should also be noted again that during the legislative process Congress considered and firmly rejected an amendment to allow all federal agencies to accept CII. Backtracking on this issue and allowing other regulatory agencies would be a breach of Congress' intent and an unwise management choice. 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.

Restriction on Use of Submitted Information

As stated above, the CII program's restrictions on the government's use of information raises serious concerns about the effectiveness of this program's ability to "protect" infrastructure. If problems are not corrected, national security is threatened. Specifically, local, state and federal agencies may not use protected CII for any regulatory action – inspections, fines, or lawsuits. The interim final CII rule contains no provisions that allow DHS to ensure that the public is

protected from dangers identified through the CII program. Companies could treat the program as a safe haven of secrecy and protection from government intervention.

OMB Watch worries that without the traditional "stick" of regulatory action that only "carrots" in the form of additional incentives will remain to encourage companies to fix vulnerabilities. Since infrastructure problems are often notoriously expensive to fix, the most likely incentive government could offer would be financial. Conceivably companies reluctant to improve old failing infrastructure could submit information to the CII program and seek financial assistance from the government. The company could attempt to leverage grants, low interest loans and other government resources, or threaten to leave the problem unresolved. Additionally, the CII program's restriction on disclosure would likely hide any such expenditures or costs.

OMB Watch acknowledges that restrictions on the use of submitted CII for a regulatory action derives directly from the legislative statute. However, DHS should utilize the definitions and procedures of the CII program to limit the risk of recalcitrant companies shirking their responsibilities.

In the end, the most important issue is fixing identified problems. Traditionally, regulatory actions—inspections, fines, and litigation— are simply means to that end. The CII rule should make the restriction from using submitted information in a regulatory matter, and all of the program's other benefits, conditional upon submitters taking all reasonable steps to address vulnerabilities identified in a submission. The good faith provision provides the most useful vehicle for this protection.

> 29.5 (d) All submissions seeking Protected CII status shall be regarded as submitted with the presumption of good faith on the part of the submitter.
> 29.5 (e) Submissions must affirm the understanding of the submitter that any false representations on such submissions may constitute a violation of 18 U.S.C. 1001 and are punishable by fine and imprisonment.

The good faith requirement is the only safeguard that specifically addresses the possibility that submitters may attempt to misuse the CII program for the incentives it offers. The interim final CII rule states that DHS would automatically presume all submissions to be made in good faith. OMB Watch urges DHS to significantly strengthen and expand the definition of "good faith" in the final CII rule. DHS should include a specific requirement that companies submitting information to the CII program must take all reasonable actions to fix problems identified in their submission. A 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 provide this program with some much needed teeth with which to deal with any bad actors looking to manipulate this new system and clearly establish that protection of infrastructure and the public is the ultimate goal of this program.

Review Procedures

The CII program is essentially a new and untested information management process. This information has never before been collected by the government and contains restrictions and handling requirements unlike any other category of information. Additionally, this unprecedented program is now managed by a new agency, DHS. In this context, there is a high potential for problems, miscommunications and disagreements. Therefore, the procedures for managing the information must be extremely clear and as close to flawless as possible. Unfortunately, the interim final rule still contains little clarity on the critical process of validating submissions.

When companies submit information under the CII program, DHS's first obligation is to review the information for validation under the program. Considering the importance Congress attached to getting this information, it is extremely troubling that the interim final rule still does not contain a deadline or specific process for review and validation of submissions. Currently, the interim final rule only requires that the information be reviewed "as soon as practicable."

> 29.6 (e) (1) The Protected CII Program Manager or the Protected CII Program Manager's designees shall be responsible for reviewing all submissions that request protection under the CII Act of 2002. The Protected CII Program Manager or the Protected CII Program Manager's designee shall review the submitted information as soon as practicable.

Establishing a timeframe for review and validation is basic program management. Programs with mandatory deadlines, such as the Freedom of Information Act, still jam with extensive backlogs and requests that go unresolved for years. Without a deadline, the CII program could have a backlog of non-qualifying information being protected indefinitely because it is never reviewed or rejected. The interim final rule contains a 30-day deadline just for notifying submitters that DHS has received the information. A 30-day deadline merely to acknowledge receipt of a submission sets a crawling pace for the entire CII program. The CII program should tighten the deadline for acknowledging receipt to 10 days and establish a specific deadline, perhaps 45 business days, for evaluating the validity of a submission.

The final rule should also include a standard re-review procedure so the CII program does not become a permanent black hole for information. DHS should periodically, perhaps every two years, re-review a submission to confirm that the information still qualifies for protection under the program. If over time information submitted would no longer qualify for protected CII status, the information from a single submitter should not remain secret and protected.

> 29.6 (f) Changing the status of Protected CII to non-Protected CII. Once information is validated, only the Protected CII Program Manager or the Protected CII Program Manager's designees may change the status of Protected CII to that of non-Protected CII and remove its Protected CII markings. Status changes may take place when the submitter requests in writing that the information no longer be protected under the CII Act of 2002 or when the Protected CII Program Manager or the Protected CII Program Manager's designee determines that the information was customarily in the public

> domain, is publicly available through legal means, or is required to be submitted to DHS by Federal law or regulation.

Even though the interim final rule acknowledges that changes may disqualify information already in the CII program from continued protection, DHS does not establish any procedures to discover such changes. If DHS acknowledges that the status of protected CII can change over time, it must take the next step and establish procedures to periodically re-review the information. The government already has procedures to regularly consider declassifying secret documents, and DHS would be shortsighted if it did not establish similar procedures for this program. It also seems reasonable that requests for any information protected under the CII program, such as FOIA requests, should also trigger a re-reviewed to confirm the information's qualification and protection.

Additionally, DHS needs to change a clause within its list of items that may change the status of protected CII to non-protected CII. The final item in the list states that status of protected CII may change if the information "is required to be submitted to DHS by Federal law or regulation." While the basic issue is correct, DHS has written the clause far too narrowly by limiting the point to only DHS's reporting requirements instead of those of all federal agencies. As written, information like pollution or accident data could continue to qualify for the CII program even after agencies such as EPA or OSHA mandate the reporting just because this much of this information would not be "required to be submitted to DHS." Congress made its intentions clear in both the statute and during its extensive deliberations over CII – the program should not override established reporting programs in other agencies. It follows that it also should not trump those reporting requirements yet to be written. DHS should re-write the clause to read "is required to be submitted to any federal agency by federal law or regulation." Hopefully this is merely an oversight in writing on DHS's part.

Definition of Critical Infrastructure Information

There can be no more fundamental necessity for the final CII rule then a clear and understandable definition of "critical infrastructure information." However, DHS continues to use overly broad and vague language when defining the term. Without a clear definition of what constitutes CII, DHS officials will be unable to reliably evaluate corporate submissions. Coupled with the interim final rule's provisions for automatic deference to submitters' good faith and protection of information, it seems unlikely that any information would be rejected from the program. The interim final rule defines CII as:

> 29.2 Critical Infrastructure Information, or CII means information not customarily in the public domain and related to the security of critical infrastructure or protected systems.

Other portions of the rule define or explain in greater detail various aspects of the definition, such as what constitutes "critical infrastructure" or what type of "security" information qualifies. However, nowhere in the interim final rule does DHS define the term "not customarily in the public domain." Without a specific explanation of what does and does not qualify as "customarily in the public domain" that portion of the definition becomes effectively useless. Congress established the limitation that the CII program may only cover information "not

customarily in the public domain." DHS should not disregard Congress' intentions and abandon this limitation by refusing to define the term.

In response to similar comments on the proposed CII rule, DHS refused to define "not customarily in the public domain" in order to preserve the "flexibility necessary to further promote information sharing by providing submitters with an opportunity to provide the information they believe meets the definition and should be protected." However, the belief of a submitter should not be the deciding factor. Information should only be protected in the CII program if it qualifies by meeting well-defined criteria, including "not customarily in the public domain."

Considering the speed and range that information can duplicate and spread in the modern information age, a reasonable definition of customarily in the public domain might be as simple as a single official release. DHS should include a clear and reasonable definition of "customarily in the public domain" along with an explanation of how the submissions will be checked against the definition.

The interim final rule also contains another term, "voluntary," that still requires a more clarified definition. As mentioned above, Congress clearly did not intend for the CII program to over-ride other laws and programs in place. Limiting the program to only voluntarily submitted information was one way that Congress protected information collected by other agencies under a host of regulations and laws. However, DHS continues to define this limiting term only in reference to its own agency and not the entire federal government.

> 29.2 Voluntary or Voluntarily, when used in reference to any submission of CII to DHS, means submitted in the absence of DHS's exercise of legal authority to compel access to or submission of such information;

Using this definition the only information that would not be considered voluntarily submitted would be that information specifically requested by DHS, and DHS only. In effect all other information collected by all other government agencies would be considered "voluntary" and could be submitted to the CII program. This means that information from hazardous waste generation to worker safety status could be accepted into the CII program. DHS should follow Congress' intention and clearly exclude all information collected by any Federal agency. OMB Watch recommends that DHS reword the definition to read, "submitted in the absence of any federal agency's exercise of legal authority to compel access to or submission of such information."

Concluding Comments

The interim final CII rule still requires significant revisions to create an efficient program that ensures the protection of citizens and infrastructure, does not interfere with the operations of other agencies, and prevents misuse by corporations. Since many of the changes needed are clarifications and refinements of existing provisions, DHS can easily accomplish this without disturbing the basic operation of the program that is already in place.

Recommendations for the final CII rule:

- 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.
- Strongly define good faith with a provision that identified infrastructure submission and how submissions will be tested against the definition.
- Establish a deadline for evaluating the validity of submissions.
- Establish a schedule for automatic re-review of CII submissions to evaluate if the information qualifies for continued protection.
- Reword the provision for changing status of protected CII to non-protected CII to include new reporting requirements by other federal agencies as a reason for changing status.
- Include a clear and reasonable definition of "customarily in the public domain" along with an explanation of how the submissions will be checked against the definition.
- Clarify the definition of voluntary to exclude information collected by any Federal agency other than DHS.

OMB Watch sincerely hopes DHS will take this opportunity to further improve the CII rule prior to finalization. The issues raised in these comments are significant problems that remain in the interim final rule which threaten the manageability and effectiveness of the entire program. The changes recommended will reduce the opportunity for less conscientious participants to misuse and manipulate this innovative program. These recommendations create a program that ensures infrastructure and citizens will not go unprotected, and that problems and vulnerabilities will not go unaddressed. This is the heart of DHS's very mission and should manifest itself in all of its rulemakings.

Thank you for consideration of our views.

Sincerely,

Sean Moulton
Senior Policy Analyst