OMB WATCH

Analysis of Department of Homeland Security's Proposed Rule on Critical Infrastructure Information

As of June 9, 2003

The Department of Homeland Security (DHS) proposed its rule for handling Critical Infrastructure Information (CII) as required by the Homeland Security Act of 2002. The CII provisions were widely criticized during the development of the legislation. The details of the proposed rule heighten many of the concerns raised by the legislative proposals. Overall, the CII program proposed granting corporations that voluntarily submitted information on infrastructure vulnerabilities secrecy, civil immunity, preemption of state and local disclosure laws, and protection from whistleblowers. The proposed rule contains these provisions, but has expanded the scope of exemptions in a number of areas.

While it is encouraging that DHS is engaging in an open rulemaking process, complete with a public comment period, the content of the proposed rule is troubling and has far-reaching implications. The proposed rule's numerous shortcomings can be roughly grouped into three main categories:

- **Scope of the CII Program**
- **Use of Information**
- **Procedures for Managing CII**

This analysis identifies the troubling components of the proposed rule, examines the detrimental impact they will have to openness and good government, and recommends specific improvements that the final rule should incorporate.

Scope of the CII Program

Extension to All Federal Agencies

The scope of the CII program has been, and remains, a major concern. Beginning with the initial legislative debate, the question of which federal agencies would be covered by the CII provisions was intensely deliberated. An amendment that allowed all federal agencies to accept CII was voted down. Despite this, the proposed rule DHS suggests the CII program would apply to any agency that handles such information.

> 29.1 (b) Scope. These procedures apply to all Federal agencies that receive, care for, or store CII voluntarily submitted to the Federal Government pursuant to the CII Act of 2002.

This section does not specify what it means to "receive" CII information. This section could mean that companies would be free to submit CII to any and all Federal agencies. However, the section could also be interpreted as meaning while only DHS could directly receive CII from companies, other agencies could have CII forwarded to them by DHS and then those agencies would still be bound to protect the information as detailed in the proposed rule.

Definition of Submitted to DHS

Unfortunately, later in the proposed rule DHS puts all the questions of scope to rest with a definition for "submission to DHS" that allows CII submissions to any federal agency. Essentially, DHS attempts to skirt around the restriction of the program by redefining "submission to DHS" as being either directly from companies or indirectly through other agencies.

> 29.2 (i) Submission to DHS as referenced in these procedures means any transmittal of CII from any entity to DHS. The CII may be provided to DHS either directly or indirectly via another Federal agency, which, upon receipt of the CII, will forward it to DHS.

The expansion to allow all agencies to receive CII submissions is the single most significant problem with DHS's proposed rule. There are several reasons that this new program should remain very limited in its scope. First, a program that allows all agencies to receive CII directly might result in extending the CII protections to non-CII and even required submissions. For instance, if a required report were filed with some additional critical infrastructure information in the report, then required portions of the report, or possibly the entire report, could be withheld from the public under the CII protections. If the program were limited to only direct submissions to DHS, then there would be less possibility of this confusion. Limiting submissions to DHS would immediately prevent this confusion in addition to the possible overuse of CII protections for key issues covered by other agencies such as environment, worker safety, and health threats. Currently DHS doesn't require any information to be submitted, so the CII provisions won't overlap with required submissions if limited to that agency. Second, is the possibility that a broad CII program across all Federal agencies will create greater difficulty in managing information and efficiently determining what may and may not be made public. This would cause significant delays in the proper sharing of information to other federal agencies and to the public. For the establishment of an efficient and manageable program that is in keeping with the spirit of what Congress passed the proposed rule should only allow direct submissions to DHS.

Definition of Critical Infrastructure Information

In addition to the issue of the scope Federal agencies that can receive CII submissions is the issue of the scope of information that qualifies for the program. The first step in establishing that scope is defining the term "critical infrastructure information." Regrettably, DHS employs some vague and undefined language in this definition that prevents it from being reliably used to exclude submissions.

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

The initial line of the definition limits CII to information that is "not customarily in the public domain." However, the proposed rule does not include a definition of "customarily in the public domain." Without a detailed explanation of what does and does not qualify as "customarily in the public domain" CII program managers can apply the clause far too arbitrarily. The proposed rule must define the phrase and/or establish clear evaluation procedures. Considering 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 low as a single official release.

Definition of Voluntary

The next definition in the proposed rule compounds the problem of expanding the CII program to all Federal agencies. In order to qualify as CII, information must be submitted voluntarily. After widely expanding the scope of the CII program, the proposed rule defines voluntary in a way that allows too much information to fall into the category.

> 29.2 (j) 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;

DHS effectively defines voluntary to include just about any information submitted by excluding very little. According to the definition the only information that is not "voluntary" is that which DHS has exercised legal authority to obtain. This miniscule exclusion means that all other information submitted to the government for any reason qualifies as voluntary. It is incomprehensible why only DHS's required information is excluded from the definition of voluntary. These provisions would allow companies to hide, as CII submissions, information required by any number of laws including environmental, health and safety, labor, transportation, and energy laws. Originally the requirement that submitted information had to be voluntary was intended to protect information currently collected across government agencies from disappearing. In order to fulfill that purpose, the definition of voluntary should clearly exclude all information collected by any Federal agency.

More generally, the definition of voluntary should not merely exclude information that an agency has exercised its legal authority to obtain. The term "exercise of authority" can be interpreted too narrowly. In a recent FERC rulemaking, the agency noted that simply because an agency has authority to require submission and the information was submitted does not mean that agency "exercised" its authority to compel the submission. One example given is information that was subpoenaed by an agency was still deemed voluntary because the agency had not taken steps to enforce the subpoena. Voluntary should be defined as submitted in the absence of authority to compel access or submission of the information.

The definition later includes a statement that could be interpreted as a slightly broader protection extending to other agencies. However, it is neither explicitly written to cover all agencies, nor

even if it did extend to all agencies, would it cover all authorities and actions of an agency that might require the information to be submitted.

> The term does not include information or statements submitted or relied upon as a basis for making licensing or permitting determinations, or during regulatory proceedings.

This portion of the definition only applies to information required for regulatory decisions such as permits. Also, considering that the earlier portion has already limited the definition to DHS, this portion could easily be interpreted to also be limited to permitting determinations and regulatory proceedings for DHS only—even though they do not currently have any of either. If the statement were limited to DHS's permitting and regulations, then the regulatory process of every other Federal agency would be vulnerable to losing vital information to the CII program. Under this definition far too much information can be deemed voluntary, even when an agency requires the information under another law. Potentially allowing information required by other agencies under various laws and for any number of regulatory purposes invites abuse by submitting corporations.

Restriction of Scope

Unlike the overly broad definition of voluntary which would allow almost any type of information to qualify as "voluntary", section 29.3 (a) of the proposed rule establishes very specific restrictions on the government information that receives the CII program's protections such as exemption from FOIA.

> Sec. 29.3 (a) Freedom of Information Act access and mandatory submissions of information. The CII Act of 2002 and these procedures do not apply to or affect any requirement pertaining to information that must be submitted to a Federal agency or pertaining to the obligation of any Federal agency to disclose such information under the Freedom of Information Act. Similarly, the CII Act of 2002 and these procedures do not apply to any information that is submitted to a Federal agency pursuant to any legal requirement. The fact that a person or entity has voluntarily submitted information pursuant to the CII Act of 2002 does not constitute compliance with any requirement to submit that information or any other such information to a Federal agency under any other provision of law. Moreover, when information is required to be submitted to a Federal agency to satisfy a provision of law, it is not to be marked by the submitter, by DHS, or by any other party, as submitted or protected under the CII Act of 2002 or to be otherwise afforded the protections of the CII Act of 2002.

In this section, DHS clearly establishes that submitters cannot hide information by labeling it as CII if other law or regulations require the submission. This is the only section of the proposed rule that decisively restricts the scope of information that may be submitted under the CII program. The section recognizes the necessity for information to be available and usable to agencies and the public. The section also represents the only section that could reasonably be expected to limit the amount of abuse that the CII program could invite from bad actors. The restrictive scope of this section is indirect contrast to the broad open-ended sections of "voluntary" and "submissions to DHS." The proposed rule's inconstancies should be resolved so that other sections reflect the reasonable and protective restrictions outlined in this section.

Protected Critical Infrastructure Information
A key distinction is the acknowledgement that not all Critical Infrastructure Information receives this program's protections. Likely there is a great deal of CII that companies are required to regularly submit to the government under various laws and regulations. The proposed rule lays out the requirements that information must meet, in addition to being CII, in order to receive the program's protections.

> 29.2 (f) Protected Critical Infrastructure Information or Protected CII means CII (including the identity of the submitting person or entity) that is voluntarily submitted to DHS for its use regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement as described in Sec. 29.5 of this chapter. This information maintains its protected status unless the CII Program Manager renders a final decision that the information is not Protected CII.

Essentially these additional requirements are that the information is a) voluntary b) submitted to DHS and c) that it be accompanied by a clear declaration of its CII status. If the CII also meets these three requirements than it qualifies as "protected CII." This important distinction is muddled in the rest of the proposed rule as different sections refer simply to "CII" when they should utilize the term "protected CII." Very likely this problem is a basic drafting mistake, however DHS must clarify the distinction between CII and protected CII and utilize the later term whenever referring to information managed by the program.

Burden on Other Agencies
The proposed rule's expansion to allow other agencies to receive submissions of CII includes with it the issue of additional burdens on those agencies.

> 29.4 (c) Appointment of CII Officers. The CII Program Manager shall establish procedures to ensure that any DHS component or other entity that works with Protected CII appoints one or more employees to serve as a CII Officer for the activity in order to provide proper management and oversight. Persons appointed to these positions shall be fully familiar with these procedures.

The proposed rule implies that one or more CII officers will be required for any "other entity" that handles CII without any consideration of the burden this shifts to other agencies. The Homeland Security Act squarely placed the responsibility for CII upon DHS, which is expected to be the second biggest Federal agency and therefore have more extensive resources available. Other agencies are already struggling to meet commitments and responsibilities central to their primary missions. As resource demands of this new CII program are unknown, it is possible that some agencies may work with extensive amounts of CII and therefore be forced to reallocate resources away from existing priorities. Only DHS received funds to manage a CII program. In an already overburdened federal government it is unreasonable of DHS to suddenly shift responsibility for this program to other agencies without committing resources from the program's budget. The rule should limit the receiving and management of CII submissions to DHS, where the resources have been allocated to address this program.

Use of Information

Restrictions on Use of Information

Aside from the restrictions on public access that a broader CII program would entail, another prominent complaint focuses on the government's ability to use the submitted information. One of the "incentives" that the legislative provisions contained to encourage corporations to submit information was the promise that the information could not in turn be used against the companies. The proposed rule details these use restrictions.

> 29.3 (c) Restriction on use of protected CII by regulatory and other federal agencies. No Federal agency shall request, obtain, maintain, or use information protected under the CII Act of 2002 as a substitute for the exercise of its own legal authority to compel access to or submission of such information. Federal agencies shall not utilize CII for regulatory purposes without the written consent of the submitter.

The restrictions on using and sharing the information raise questions about the value of collecting vulnerability information if the government is unable to assure that the identified problems will be fixed. The simple but extremely broad statement that no Federal agency may use CII for any regulatory purpose would include, assessing fines until vulnerabilities are fixed, filing notices of non-compliance, and even scheduling inspections of facilities. Even if an inspection or information request were submitted separate from the CII submission, a corporation could make the case that its CII submission was used to plan the inspection or officially request additional information, which are considered "regulatory purposes." The proposed rule places the burden on the agency to prove that the department inspecting or requesting information did not have any knowledge of the CII submission. Proving a negative is an extremely difficult, if not impossible, standard to meet and would provide an easy legal challenge for any company. This use restriction, regardless of the rule's attempt to allow agencies to independently obtain the information, creates an effective blanket protection from any regulatory repercussions from incriminating information submitted under the CII program.

Approved Use of Information

After noting the extensive restrictions on the government's ability to use the submitted CII, the next logical question is what can the government do with the information. Unfortunately, the limited list of approved uses for CII specified in the proposed rule reinforces the problematic restrictions on CII use. The approved purposes for use of CII apply to DHS and any other government agencies granted access to submitted CII.

> 29.8 (b) Federal, State and Local Government access. The CII Program Manager may provide Protected CII to an employee of the Federal Government, or of a State or local government, provided that such information is shared for purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purpose relating to homeland security.

None of the approved uses of the information allow the government to ensure that the vulnerability identified in submitted information is addressed and resolved. The most active response agencies are allowed to take is "securing the critical infrastructure" which seems far too

limited, only covering actions such as posting additional guards or other security measures. Most of the approved uses for CII appear limited to informational ones such as analysis and study. The only open and flexible use listed, "another informational purpose relating to homeland security," is an informational use rather than an active protection of the public. It is irresponsible of the government to collect information on infrastructure vulnerabilities around the country only for the purpose of studying and warning. Limiting the actions government agencies can take to reduce and eliminate these vulnerabilities once they are identified, just to provide an incentive for companies to submit information, is shortsighted in the extreme. This point is further borne out in the limitation placed on state and local use of CII.

State & Local Use of Information

While State and local authorities are likely to find the most use for information submitted to the CII program, DHS proposes even stricter limitations on them. The proposed rule severely narrows the options of actions that State and local authorities can take in response to CII submissions that are released to them. Essentially DHS eliminates their ability to use their own discretion or judgment based on the information and their experience.

> 29.8 (d) (3) State and local governments may use Protected CII only for the purpose of protecting critical infrastructure or protected systems, or in furtherance of an investigation or the prosecution of a criminal act.

The proposed rule explicitly limits State and local authorities' use of CII to "protecting" the infrastructure with the one caveat of investigation of a crime. There can be little doubt that protecting is confined to keeping people away from the infrastructure rather then working to fix the problem. The proposed rule also imposes excessive restrictions on the State and local authorities ability to share or distribute the information.

> 29.8 (d) (2) The CII Program Manager may not authorize State and local governments to further disclose or distribute the information to another party unless the Program Manager first obtains the written consent of the person or entity submitting the information.

These restrictions prevent State and local authorities, which are the most knowledgeable about communities and nearby infrastructure, from in any way informing the public about potential risks identified in CII submissions. Even the Program Manager does not have the authority to allow them to distribute the information to anyone or issue alerts to the public. Only with written permission from the CII submitter may local authorities be granted to authority to distribute information about risks threatening their communities. This excessively bureaucratic procedure indicates that DHS is more interested in appeasing the concerns of corporations then allowing local communities to be fully protected and aware for the dangers they face.

Warnings

Warnings, alerts and advisories are the most obvious and practical use for the information that the government expects to collect under the CII program. However, the rule proposed by DHS would significantly limit the government's ability to warn or alert the public to risks they may unknowingly face everyday.

> 29.8 (e) Disclosure of information to appropriate entities and the general public. The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors, other government entities, or the general public regarding potential threats to critical infrastructure as appropriate. In issuing a warning, the IAIP Directorate shall protect from disclosure the source of any voluntarily submitted CII that forms the basis for the warning; and any information that is proprietary, business-sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

The section limits the authority to warn or alert companies, industry sectors, other government agencies and the public to the Information Analysis Infrastructure Protection Directorate. The provisions also limit the type of warning that the IAIP Directorate may issue. The alerts must protect the source of the information from disclosure as well as any business-sensitive information. Once again the priorities of the proposed rule seem inappropriate, with greater importance given to protecting corporate identities and business information then protecting the public's safety. The rule should state that if possible the identity of the submitter and related sensitive information will be protected but that the first priority when a warning is warranted is to adequately inform the public. It is particularly disturbing given the investigations into the September 11th attacks revealed that the lack of information sharing likely contributed to our inability to prevent those attacks that DHS would ignore those lessons and propose establishing limited warning procedures.

Whistleblowers

Whistleblowers have been and continue to be extremely useful in revealing illegal or inappropriate government actions. Whistleblowers have revealed such things as an attempted cover-up of safety hazards at the Hanford Nuclear Site, the United States' primary plutonium production facility, which could have caused accidents on the scale of Chernobyl. The proposed rule seems to have included some provisions similar to traditional whistleblower protections, they have severely limited their application. Essentially, the proposed rule does not protect whistleblowers that disclose CII and does not allow previously established whistleblower protections to apply to CII.

The proposed procedures for the CII program do not typically allow disclosure of submitted information without the written consent of the submitter. However limited exceptions are made for disclosures that assist investigation or prosecution of a criminal act; disclosures to Congress; and disclosures to the Comptroller General of the General Accounting Office. However, the proposed rule immediately places requirements on these exceptions that effectively eliminate the exceptions usefulness for whistleblowing.

> 29.8 (f) (1) (ii) If any disclosure is made pursuant to these exceptions, prior written authorization must be obtained, in consultation with the DHS Office of the General Counsel, from the DHS Secretary, DHS Deputy Secretary, Under Secretary for IAIP, the DHS Inspector General, or the CII Program Manager.

This provision does not allow for whistleblowing of any kind, even to Congress. The concept behind whistleblowing is that the powers of authority are concealing important information that necessitates the unconventional disclosure by a lower level government official. Considering the purposes for these exceptions are for investigation and review, replacing the requirement of written consent from the submitter with a requirement for written authorization from top DHS officials seems overly bureaucratic. A more reasonable approach would be to allow the CII Program Manager to approve information disclosures to criminal investigations, Congress or the GAO with a provision that acknowledges that if unauthorized disclosures are made to such parties then those disclosures would be covered under the Whistleblower Protection Act. Later in this section of the proposed rule the possibility of disclosure without any written approval is addressed.

> 29.8 (f) (2) Consistent with the authority to disclose information for any purpose described in Sec. 29.2(h), disclosure of Protected CII may be made, without the written consent of the person or entity submitting such information, to the DHS Inspector General, or to any other employee designated by the Secretary of Homeland Security. Disclosure may be made by any officer or employee of the United States who reasonably believes that such information:
>
> 29.8 (f) (2) (ii) Evidences mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety affecting or relating to the protection of the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, or reconstitution.

The first section establishes the possibility for disclosures made without consent or permission, which is certainly similar to how whistleblowing could be described. The second section establishes a set of reasons for which the unapproved disclosure of information is allowed. The list clearly parallels justifications for whistleblower activity, such as abuse of authority and specific danger to public health or safety. However, the first section only protects disclosures to the DHS Inspector General or an employee chosen by the Secretary of Homeland Security. Limiting whistleblower disclosures to those immediately in charge of a program runs counter to the entire concept of whistleblowing. DHS should expand these provisions to allow disclosure to Congress, other agencies and the public when it is reasonably believed to evidence the troubling situations listed.

Criminal Penalties for Unauthorized Disclosure

Significant concerns have been raised about the criminal penalties for disclosure of CII by a civil employee. Under the proposed rule's current provisions, CII that evidences waste, fraud or serious public safety risks could not be disclosed to the public, other agencies or even Congress without written consent from the corporation that submitted the information. In fact, if a government employee did whistleblow to Congress or another Federal agency or anyone other than the Inspector General or a designee of the Secretary of DHS, then they would face criminal charges.

> 29.8 (f) (3) Disclosures of the above nature are authorized by law and therefore are not subject to penalty under section 214(f) of the Homeland Security Act of 2002.

In the past the government has seen the value of unauthorized disclosures for appropriate purposes, whistleblowing, and has protected them under the Whistleblower Protection Act. Unfortunately, the Whistleblower Protection Act only applies to information without specific protections from disclosure, such as protections for classified information and national security information. Therefore, the criminal penalties in the CII program will take priority over the whistleblower protections unless DHS specifically states that the criminal penalties do not apply to legitimate whistleblower activities as described in the Whistleblower Protection Act. Without the protections that normally are granted to government employees, there is no freedom to report on government misconduct in order to protect civil society.

FOIA Requests

One of the protections that protected CII submission receive from this program is an exemption from disclosure requirements under FOIA. However, the proposed rule does not establish any procedures for management of protected CII requested under FOIA except to say that it shall be treated as exempt.

> 29.8 (g) Responding to requests made under the Freedom of Information Act or State/local information access laws. (1) Protected CII shall be treated as exempt from disclosure under the Freedom of Information Act and, if provided by the CII Program Manager, or the Program Manager's designee, to a State or local government agency, entity or authority, or an employee or contractor thereof, shall not be made available pursuant to any State or local law requiring disclosure of records or information. Any Federal, State, or local government agency with questions regarding the protection of Protected CII from public disclosure shall contact the CII Program Manager, who may in turn consult with the DHS Office of the General Counsel.

The proposed rule should make it clear that protected CII that is responsive to a FOIA request will be submitted to the FOIA officer handling the request. The FOIA request should trigger a re-review of the CII by the FOIA officer to confirm that the information continues to meet the requirements for the CII program. The FOIA officer should submit an evaluation of the information to DHS, which working off the agency recommendations would be responsible for either confirming the protected CII status or begin procedures to remove the protected CII status. The proposed rule should also establish procedures for the partial release of information submitted under the CII program if pieces of a submission do not qualify as protected CII. Such procedures would be in keeping with standard practice for exemptions under FOIA.

Ex Parte Communications

An extremely troubling but infrequently discussed aspect of the CII program is the possibility of using CII submissions as ex parte communication. This would allow corporations to influence the regulatory rulemaking process with secret CII submissions. The proposed rule does little to address the risks of misusing such a new capability.

> 29.8 (h) Ex parte communications with decision-making officials. Pursuant to section 214(a)(1)(B) of the Homeland Security Act of 2002, Protected CII is not subject to ``any

agency rules or judicial doctrine regarding ex parte communications with a decision-making official."

Given the fluctuating scope of the proposed rule, with submissions being allowed to any agency but exercise of authority limited to DHS authority, it is unclear if the ex parte communications are allowed for just DHS rulemaking or if they would apply to any and all federal agencies. We hope that this uncertain trait of the CII program would be limited to DHS rulemaking. It would seem contradictory if DHS proposes to allow CII to be used as ex parte communication for any federal agency when previous sections of the proposed rule specifically prevent Federal agencies from using CII in any regulatory proceeding. And it would be exceedingly unbalanced if DHS intends to allow corporations to only beneficially influence regulatory rulemaking while at the same time preventing agencies from holding those corporations accountable for the information submitted. The section also does not offer any indication that if CII were to be used to influence a rulemaking what efforts would be made to release the information. The proposed rule should detail that if the Program Manager deems the information appropriate for public release that the submitter would be contacted and urged to allow the dissemination as befits the public rulemaking process.

Procedures for Managing CII

Control Shifted to Corporations

While there have been long standing concerns about the influence of corporations and big business on the development of government policies, the CII program went even further by granting corporations increased control over the information process. In the supplementary information provided prior to DHS's proposed rule on CII, the agency makes a troubling statement about the reliance on the submitters towards the end of the Background section. The statement, as well as other sections of the proposed rule, touches on one of the major problems with the CII program, shifting authority and control over submitted information from the government to corporations.

> I. Background
> "Although the Homeland Security Act establishes a working definition of critical infrastructure information, the Department relies upon the discretion of the submitter as to whether the volunteered information meets the definition of critical infrastructure information."

The Freedom of Information Act has a well-established system in which companies submit information to a government agency. The companies have the ability to label information as confidential business information or proprietary, but it is ultimately the government's judgment once the information is requested as to whether the claim is valid and if the information should be released. The CII procedures shift far more power in the control of information to corporations. This claim that DHS must rely and trust corporations submitting information is disconcerting, especially considering the string of corporate deception scandals such as Enron that have cast real doubt on corporations' ability to consistently act responsibly and in the public's best interest.

Implementing Directives
A troubling procedure detail in DHS's proposed rule is the reference to "implementing directives" for the proper treatment of CII. This means that numerous details of great concern to parties interested in how the CII program will be managed may be handled in these implementing directives rather than the rulemaking. There is no mention that these directives or the training materials will be developed with any public scrutiny.

> 29.4 (b)(3) Promulgate implementing directives and prepare training materials as necessary for the proper treatment of Protected CII.

The CII program was an extremely controversial issue with many concerns that the proposals would be overly vague, poorly developed, and have inadequate safeguards for potential misuse. Under these circumstances, there is an even greater then normal need for transparency in the development of CII policies and procedures. If policy directives are to be developed after the CII rule, then DHS should clearly commit to allowing public comment on those directives in order to ensure balanced standards that will minimize potential misuse of the program.

Requirements for Submitters
As already examined, the proposed DHS rule widens the scope of the CII program by opening up the number of agencies to which CII can be submitted, and allows a great amount of information to be deemed CII. DHS does suggest some restrictions and requirements on information submission, but those detailed in the proposed rule are far too vague and weak.

> 29.5 (c) Information that is not submitted to the CII Program Manager, either directly by the submitter or indirectly through another Federal agency by request of the submitter, will not qualify for protection under the CII Act of 2002.

When coupled with the expansion to all federal agencies, this restriction means that in order to qualify for the programs protections a submitter must only identify or label the submission as CII. This provision, once again, places too much trust in corporations and makes the program too vulnerable to abuse by submitters. DHS should take this opportunity to specify strict requirements and procedures that corporations must follow in order to qualify for the CII protections.

One such procedure that should be in place is that if submissions through other agencies continue to be allowed then those agencies should review the material before passing the submission along to DHS. The recipient agency would deliver to DHS, along with the company's CII submission, a recommendation for any material the agency believes should not be granted protected CII status as it is either a required submission or does not meet the CII definition in some way. Since the information is being submitted though another agency it is likely that it relates to the matters regulated by that agency and it would be prudent of DHS to engage their experience and expertise in evaluating the information as soon as possible in the process.

Presumption of Protection
Another over-expansive aspect of the proposed rule is the presumption that all information submitted qualifies as CII. DHS proposes that standard procedure for all information submitted

should be that it automatically receives the CII protections. The protections are only eliminated when the Program Manager renders a decision that the information does not qualify for the protections.

> 29.6 (b) Presumption of Protection. All information submitted in accordance with the procedures set forth herein will be presumed to be treated as Protected CII from the time the information is received by a Federal agency or DHS component. The information shall remain protected unless and until the CII Program Manager renders a final decision that the information is not Protected CII.

This presumption of protection is overly simplistic and unbalanced. While it is reasonable that submitted information be afforded confidentiality it should not be an open-ended status. There is no requirement that the information be evaluated within a certain timeframe. Without a deadline, non-qualifying information could potentially receive the CII protections while the Program Manager considers the determination for years. Under FOIA, even with a mandatory deadline there are requests that have remained undecided for years; consider how much worse the process would be without the deadline. The CII program should have specific requirements for evaluating the validity of a submission.

Validation Procedures

Before DHS released the proposed rule, concerns raised by members of Congress as well as public interest groups about possible misuse of this program demanded that DHS establish strong validation procedures. Validating the submitted information is necessary in order to ensure that companies are not abusing the program to hide misconduct or avoid responsibility. The procedures suggested in the proposed rule for validating submitted information are meager and inadequate to the point the point of being meaningless.

> 29.6 (e) (1) Validation of information. (1) The CII Program Manager shall be responsible for reviewing all submissions that request protection under the CII Act of 2002. The Program Manager shall review the submitted information to validate the satisfaction of the definition of CII as established by law. In making this initial validation determination, the Program Manager shall give deference to the submitter's expectation that the information qualifies for protection.

One problem with the listed validation procedures is again, that only the Program Manager may validate information submitted. This procedural bottleneck creates a strong possibility for delays and backlogs in validating information, especially if the CII program receives extensive information. DHS should amend the proposed rule to allow the Program Manager to designate and train Validation Officials in order to expedite the process of evaluating CII submissions.

This raises the question as to whether a single manager can possess all the various expertise to accurately evaluate the legitimacy and good faith of submissions from a variety of industries and overlapping with a multitude of regulatory functions. The procedures should include a requirement that the Program Manager and his Validation Officials confirm the reporting requirements, the current status of the facility, and ongoing or planned regulatory actions with regulatory agencies appropriate to the type of information submitted.

Another problem with the validation procedures listed in the proposed rule is the instruction that the Program Manager shall give deference to the submitter's expectation that the information qualifies for protection. The government's first priority should be to safeguard the regulatory processes and the integrity of this program from misuse. Therefore the Program Manager should give no deference to a submitter's expectation, but should instead be instructed to give deference to any regulatory or oversight function that the submitted information might overlap.

The procedures only vaguely require that the Program Manager validate that the information meets the definition of CII. Instead, the procedures should breakdown the major issues and aspects that need to be checked and the actions that should be taken to confirm those issues. For instance, the procedures should explain that for each submission it must be confirmed that the information covers critical infrastructure, that it is voluntarily submitted, that it is a good faith submission. The procedures should also detail standard steps in the validating these aspects of the submission.

While the Program Manager is obligated to review and validate the CII submissions, there is no listed obligation to notify anyone as to decision. The proposed rule should contain a specific requirement that if a CII submission comes through an agency, then DHS must immediately inform that agency of the validation decision.

Re-Reviews

While the information within the CII program receives various protections, it should not receive these protections in perpetuity. The government already has procedures to regularly consider declassifying secret documents and DHS would be acting short-sightedly if it did not establish similar procedures for this program. Currently proposed rule only contains a preliminary evaluation of information when it is originally submitted. There are no procedures for re-review of the information and its qualifications for protected status. Obviously as time passes what constitutes critical infrastructure will change as society transitions from one technology or industry to another. The information that qualifies for protected CII will also change over time as what information that is "customarily in the public domain" changes. The proposed rule should have a deadline on the protected status requiring a re-review to continue the protections. This would be similar to the required 25-year mandated review for declassification of information. However, given the speed of technological innovation a much shorter period, for instance 5 years, would be reasonable for the re-review of information in the CII program.

In addition to the time required re-review, FOIA requests for CII should trigger an new evaluation of information's qualification for CII protections. In order to expedite this process the proposed rule could establish procedures for FOIA officers to conduct an initial re-review of CII status when a FOIA request triggers the reevaluation. Those FOIA officers could submit their recommendations to DHS for final judgment.

Incomplete Validation Information

A strange and troubling section of the proposed rule simply reads "reserved." The entry is listed under section "29.6 Acknowledgment, validation, and marking of receipt" and seems to be the second major entry directly under the validation of information portion.

29.6 (e) (2) [Reserved]

There are several possible interpretations for this entry. First, that it is meant to operate as a placeholder in the rule reserving the area for language that will be forthcoming. Second, that the language is being held from the general public and reserved for certain reviewers only. Either possibility is a problem for the proposed rule. The first indicates that the rule is incomplete still and that DHS should not yet be proposing the rule. The second possibility would be an even bigger problem indicating that the secrecy that the administration has been using far too often and too easily after the September 11th attacks is now being applied to a public rulemaking.

Good Faith Standard

The good faith requirement remains in the proposed rule, as it was in the legislation, the only safeguard specifically addressing the possibility that submitters may attempt to misuse the CII program for the incentives it offers. Unfortunately, the proposed rule does little to detail or clarify the simple good faith requirement that was written in the legislation.

> 29.6 (f) In the event the CII Program Manager determines that any information is not submitted in good faith accordance with the CII Act of 2002 and these procedures, the Program Manager is not required to notify the submitter that the information does not qualify as Protected CII. This is the only exception to the notice requirement of these procedures.

There is no explanation of the test the Program Manager should utilize in considering the good faith of a submission. The section does not list the attributes or characteristics of either a good faith or bad faith submission. The definitions section of the proposed rule does not contain entries for either "good faith" or "bad faith." The potential for this program to be abused should be obvious to DHS and therefore they should set up more detailed standards to prevent misuse and identify bad actors that attempt to exploit the program.

Destruction of Information

The CII program's over-reliance on corporations reveals itself again in the way government intends to handle submitted information that is deemed to be non-CII. The treatment of submitted information that did not qualify as CII was never discussed during the legislative debate over CII. Therefore, DHS had an opportunity to establish any procedures it deemed appropriate in the rule. Unfortunately, DHS maintains its unswerving commitment to procedures that benefit submitters of the information first and users of the information, such as the government and communities the information could help protect, second. The proposed procedure for information that does not qualify as CII allows the submitter to choose if the information is retained by the government without the CII protections, or if the information should be destroyed.

> 29.6 (e) (1) (i) (D)) Request the submitter to state whether, in the event the CII Program Manager makes a final determination that any such information is not Protected CII, the submitter prefers that the information be maintained without the protections of the CII Act of 2002 or be disposed of in accordance with the Federal Records Act.

The process should consider the reason that the submitted information did not qualify for CII status before offering the submitter a choice. If the information cannot be considered voluntary because of ongoing regulatory process or overlaps with required submissions, then the Program Manager should have the option of transferring the information to the appropriate regulatory agency. Also, if the information does not cover critical infrastructure but still addresses vulnerabilities or issues of concern, there should be a balancing test in which the Program Manager considers the public benefits of the information before offering submitters the option of destroying the information. Discretion in handling of non-CII information that is still potentially important should not be handed over to corporations that are working in their own best interest, but should instead reside with government agencies that focus on the public's best interest.

The proposed rule cites very clearly that the submitter should state his or her preference for whether information that does not meet the requirement for CII protections should be destroyed, or maintained without the protections. However, a situation could arise where the submitter does not state a preference to DHS. Again DHS had the ability to adopt any procedure in the proposed rule, but the department elected to have an automatic presumption that submitters would prefer to have the information destroyed rather than retained by the government without the CII protections.

> 29.6 (e) (1) (ii) If the submitter, however, cannot be notified or the submitter's response is not received within thirty (30) days after the submitter received the notification, the Program Manager shall destroy the information in accordance with the Federal Records Act unless the Program Manager determines that there is a need to retain it for law enforcement and/or national security reasons.

These procedures seem to assume that submitters are recalcitrant corporations more concerned with hiding information and receiving immunity then allowing the government to have and act appropriately on information about vulnerabilities. If these companies are truly submitting the information in "good faith" to assist the government in addressing infrastructure vulnerabilities and protecting against terrorism, the presumption should be that "good faith" submitters would remain committed to that purpose even without the CII protections.

Conclusion

The CII rule proposed by DHS requires significant revisions to create an efficient program that does not reduce openness, interfere with the operations of other agencies, or allow misuse by corporations. This analysis identifies the troubling components of the proposed rule, examines the detrimental impact they will have to openness and good government, and recommends specific improvements that the final rule should incorporate.

Generally, within the three main categories discussed in this analysis DHS should:

- **Scope of the CII Program**
  The scope of the CII program should be much more limited then currently proposed. Since CII is a new and unproven program it seems prudent to create a limited program

and verify its effectiveness. Limiting the program's scope also addresses many of the concerns about the program interfering with the operation of other agencies.

- **Use of Information**
  Government agencies should be able to use the information submitted under the CII program more freely then the proposed rule would currently allow. The overall purpose of this program, and the Department of Homeland Security itself, is to make the public more secure. Agencies should have flexibility to use the submitted vulnerability information in any manner that is deemed appropriate to the primary purpose of protecting the public. Otherwise the effectiveness of the entire program will be questioned.

- **Procedures for Managing CII**
  The procedures are essential to ensure that the CII program is not overly vulnerable to misuse or mismanagement. DHS must increase and clarify the program's procedures which prevent misuse by corporations such as verification process and good faith test. The procedures for handling submissions must also ensure that submitted information is quickly processed, shared with appropriate parties, and put to good use.

Since DHS is utilizing the rulemaking process to develop its CII policies it has an opportunity to revise the proposed rule substantially. If enough public comments consistently raise the types of concerns examined in this analysis, then DHS will be forced to at least publicly address the issues in its response to comments.