Respectfully submitted,

The Coalition Of Journalists For Open Goverment

By: Pete Weitzel

American Society of Newspaper Editors
Associated Press Managing Editors
Reporters Committee for Freedom of the Press
Radio-Television News Directors Association
Society of Professional Journalists
Society of Environmental Journalists
National Press Club
Investigative Reporters and Editors
Criminal Justice Journalists
Education Writers Association
Brechner Center for Freedom of Information
Freedom of Information Center, University of Missouri

Newspaper Association of America
National Freedom of Information Coalition

May 18, 2004

Before the
Department of Homeland Security
Washington, D.C. 20528

In the Matter of	)	
	)	
PROCEDURES FOR HANDLING	)	RIN-1601-AA14
CRITICAL INFRASTRUCTURE	)	
INFORMATION; INTERIM RULE	)	

To: Office of the General Counsel

COMMENTS OF THE COALITION OF JOURNALISTS FOR OPEN GOVERNMENT

The newly formed Coalition of Journalists for Open Government, along with the below named national journalism organizations, the Newspaper Association of America, and the National Freedom of Information Coalition, hereby submit comments on the above referenced Interim Rule establishing procedures for handling Critical Infrastructure Information (CII). We recognize the need for new and effective measures to protect our nation's infrastructure from terrorist attack, but we are concerned that some of the measures proposed by The Department of Homeland Security (DHS or the Department) will make the public more vulnerable to harms of equal or greater magnitude.

We are also concerned that a program this sweeping, one that puts a shroud of secrecy on a vast quantity of information concerning potential dangers to our critical infrastructure – and thus to ourselves and our fellow citizens – is moving forward with no public benchmarks, with no indicators of progress or success. The Interim Rule as adopted makes no provision for accountability, only for keeping information from the public. The rule does not even allow the Department of Homeland Security (DHS or the Department), in issuing a warning to the public, to identify the source of the information, which, of course, is the loci of the problem it would be warning the public about.

We do not believe that a public kept uninformed is a public kept safe.

We believe the rule remains overbroad and its language subject to interpretations that could push implementing measures far beyond the intent of the law.

We are concerned that DHS, in its desire to create security partnerships with the private industries that own or control 85 percent of this nation's critical infrastructure, may inadvertently cause public oversight to be ceded, resulting in unintended and unresolved dangers in areas that have nothing to do with terrorism.

There is little in the Interim Rule, or in the commentary accompany it on February 20, that is reassuring in this regard. The Interim Rule assumes – more broadly than the initial draft – the "good faith" of every private entity that may choose to submit CII. Recent, albeit select, corporate misfeasance suggests the Department's leap of faith could be disastrous. Moreover, the presence of federal and state oversight laws covering the infrastructure and these industries should remind us that the government has previously acknowledged serious public concerns about the actions of many of these industries.

Our concerns are especially exacerbated by the Department's stated intent to reconsider expanding the CII filing process, allowing other federal and state agencies to receive this sensitive information and refer it DHS for CII designation. We fear that extending the CII processing field will compromise the specific oversight responsibilities of these agencies and place a shroud of secrecy over their operations.

Extending the CII process and protection through indirect filings would be unwise – even if it were not an act that directly defies Congress, which specifically voted down an amendment to the Homeland Security Act that would have allowed the practice. To permit indirect filings will almost certainly create legal complications. The Department of Justice states in its March 3 FOIA Post that the Protected CII exemption "applies to information held by DHS only."

Extending the process could prove a needless administrative nightmare, as well. What is the rationale for expanding participation in a remedial program that the department itself has defined as targeted and requiring maximum possible secrecy? Expanding the program to multiple agencies and to personnel with no specific training and or trained supervision can only complicate and delay rather than simplify and expedite the program's implementation.

We frankly fear that information previously available to the public will be declared confidential by these other agencies, acting in an abundance of caution, eliminating from public view information critical to understanding of safety, health and other concerns. We believe that the simple awareness among agency personnel that the agency is now handling CII can only put a chill on the disclosure of even nominally related information that comes to the agency in the normal course of its business.

Imagine the conflict for EPA, charged with both warning and protecting the public against environmental dangers, when it is suddenly given information about a potential disaster but must regard the information as potentially Protected Critical Infrastructure Information that must remain confidential.

The Department of Homeland Security Should Not Ask Other Agencies to Sacrifice Independent Missions to Protect CII

DHS, in its Order, explained that it wants to take advantage of the good relationships that existing oversight agencies have established with private industry. Apparently DHS believes private industry will be more willing to volunteer information to a known quantity, where there is a basis for trust, than to a new and untested department still trying to pull programs together.

That is understandable, but what it really says is that DHS is reluctant to take the time to establish those working relationships on its own. We are not questioning whether DHS should consult with another agency on technical or remedial issues in which that agency may have a particular experience or expertise. However, in authorizing indirect filings, DHS would be asking other agencies, largely for the short-term convenience of DHS, to become facilitators and processors of vast amounts of information that might otherwise not be available to those agencies. They would be required to honor a confidentiality not of their making, and in so doing might well avoid oversight actions they would otherwise take. That creates all manner of conflicts, including those of mission.

In so expediting and delegating its own work, DHS might well diffuse and dilute the other agencies' responsibility for remedial action involving the submitter companies. It quite possibly could soften the resolve of those agencies in dealing with non-terrorist-related threats and dangers. It will almost certainly sow confusion and create conflicts of

interest. Inevitably, some of these agencies may be put in a position that compromises their primary mission.

None of this will be good for governance. Or for the public, put at separate risk. The public will also find itself clearly and purposefully shut out of the knowledge loop by the expanded secrecy. And public accountability will be lost.

Only Information Submitted Directly to the Department of Homeland Security Should Be Considered for Protected Critical Infrastructure Information Status.

We believe that the Protected CII designation should and must be an exclusive determination of DHS, and that its use should not extend beyond the Department except in the implementation of specific and carefully contained remedial measures. That would best serve the interest of confidentiality the private companies and DHS both seek. That would best serve the interests of site-specific security and of national security. That would also best assure that both the private company and the appropriate government agency are held accountable should there be a disaster of any kind. And that would best assure the American people that the CII-sharing process itself will not become compromised.

The Homeland Security Act was not intended to give private industry a means to bypass its obligations to protect its neighbors and customers from dangers resulting from its own malfeasance or nonfeasance. Those obligations include not only remediation but also warning the public. DHS must be judicious in its actions to avoid creating such a bypass, either in fact or in perception, because public confidence is critical to the success of both DHS and the other oversight agencies.

The receipt and analysis of CII is the responsibility of DHS and its responsibility alone. DHS can assure the American people that end runs are not possible by prohibiting indirect filings of Critical Infrastructure Information.

That does not mean DHS cannot or should not consult with other agencies when their knowledge and expertise would facilitate the analysis. DHS could share CII outside the department on a tight, need-to-know basis when it needs analytical help or when it seeks support for remediation. Such consultation with other departments and agencies could be critical to making a proper determination on confidentiality of materials submitted and more importantly in determining remedial actions that might be taken to

mitigate the threats revealed. What is important here is that, in this approach, it is DHS, not the private company, which decides what information to share and how to share it.

The concerns we have expressed are prompted in large measure by the unprecedented nature of what is being proposed and by the ambiguity in some areas of implementation of the necessarily complex rule. In writing this response, if not before, we have come to appreciate the difficulties of anticipating and providing for unintended consequences. Toward that end, we will cover a number of specific issues in the pages that follow, but we would primarily ask that DHS consider making strong and definitive statements that go to the integrity of the FOIA process on infrastructure information outside of DHS and the CII process and that DHS do this both within the text of the regulations and in a preamble.

Specifically, we urge a strong, unequivocal statement in Section 29.1 that the Final Rule covers only the information that is submitted directly to the Department of Homeland Security and that the designation "Protected Critical Infrastructure Information" applies specifically and singularly to information held by DHS, even if the Department discreetly shares it with others.

We would also urge that DHS include a clarification, or restatement, in that section, affirming the independence of other governmental agencies and of any and all information they receive directly from private entities and affirming the department's recognition of the public's rights to know under the FOIA on all matters where Protected CII is not at issue.

<u>The Department of Homeland Security Should Not Leave the Determination of "Public Domain" to Submitters Who Potentially Benefit From Confidentiality.</u>

The Interim Rule extends extensive protection to voluntarily submitted CII without sufficient safeguards designed to prevent abuses that could shield corporations from liability and deprive the public of information vital to its health and safety. The clear intent of the Act was to explicitly preserve the normal use of information customarily in the public domain. That intent, however, is not manifest in the Department's Interim Rule – the language remains imprecise and ambiguous.

In response to comments urging the Department to sharpen its definition of CII, limiting its scope and minimizing the potential for misuse of the statute's protections, DHS implied its hands had been tied by Congress. They were not. The real problem is a

permissive construction of the statutory language that allows private companies to decide what should be protected.

Notably, CII is defined as "information *not customarily in the public domain* and related to the security of critical infrastructure or protected systems." The Department, however, has rejected requests that a detailed explanation of "not customarily in the public domain" be incorporated into the rule and that it develop procedures for evaluating whether information is, in fact, in the public domain. DHS says the rule as written permits "an appropriate degree of flexibility necessary to further promote information sharing by providing submitters with an opportunity they believe meets the definition and should be protected." We believe that this imprecise definition gives overly broad discretion to submitters to unilaterally determine what is CII, thus opening the door to broad and careless implementation of the rule.

For example, it is possible that if information is public, but not widely available, a submitter could aver that it is not "customarily" in the public domain. Similarly, if information has been disseminated to the public without the submitter's consent, the submitter could argue that it is not its "custom" to disclose the material.

We urge the Department to revise its rule to provide that information is "customarily" in the "public domain" when:

- it is information submitted to another government agency to which FOIA exemptions do not apply or have not been applied;
- it is information to which the public has a legal right, even if it has not been accessed;
- it is information that has been disseminated to the public in any form, with or without the submitter's consent;
- it is information for which the submitter has not taken steps to protect ~~its~~ confidentiality; or
- it is a type of information that has been made available to the public in the past.

In addition, we believe the rule should clearly state that once Protected CII enters the public domain, it automatically loses all of the inherent protections.

Similarly, the implementing regulations make no attempt to limit what information is considered as "related to" the security of critical infrastructure. Given that "related to" arguably can be interpreted to mean "having even the most tenuous connection," this imprecise language affords corporations wide latitude to "document dump." Once the information is accepted as voluntarily submitted CII, the Department and possibly other agencies may well be constrained in the corrective or punitive action they could take should a vulnerability to infrastructure not be remedied. Moreover, the public, having no knowledge of any of this, is unable to act on its own behalf.

The potential for misuse inherent in the broad language of the rules is further exacerbated by the Department's determination that all submissions will be presumed to have been made in "good faith," its failure to define good faith, and the lack of any real sanctions for "bad faith" submissions. We believe the government must define good faith – at the very least – to mean that the information is truthful, that the submitter has conducted an audit to determine vulnerabilities, and that the submission relies on representations by a person or persons with actual knowledge and authority. Most importantly, we believe each submission should be accompanied by a "good faith" pledge to work with DHS, and anyone it designates, to remedy the vulnerability in a reasonable amount of time. The Final Rule should advise that any private entity that fails to follow through on that good faith pledge loses its protection from governmental sanction or the use of its CII protection in civil actions.

The Language in of the Interim Rule is Ambiguous and Could Be Subject to Conflicting Interpretations.

Section 29.3(a) currently provides that a company may not mark as CII any information it submits to DHS if that information has already been sent to another agency as required by law. It then says a company cannot file information as CII with DHS in lieu of its obligation under another statute to submit that same information to an oversight agency. And it says that a company cannot mark the information it sends to another agency as CII. It also provides that the information a company submits to another agency is not protected.

Those are worthy protections. But the rule offers a "provided," clause with language that could be read to negate the safeguards just put in place:

"provided, however, that such information, if it is separately submitted to DHS pursuant to these procedures, may upon submission to DHS be marked as Protected CII."

That permits precisely what the rule just said was impermissible. It gives Protected CII status to information the submitter is required by law to provide to other agencies. The language also could be read to imply that DHS believes it has the authority to tell another agency which of its documents must be treated as confidential.

The clauses that follow *"provided, however"* should be struck from the Final Rule.

Section 29.3(d) Independently obtained information. It states:

These procedures shall not be construed to limit or in any way affect the ability of a Federal, State, or local government entity, agency, or authority, or any third party, under applicable law, to otherwise obtain CII by means of a different law, regulation, rule, or other authority, including such information as is lawfully and customarily disclosed to the public. Independently obtained information does not include any information derived directly or indirectly from Protected CII subsequent to its submission. Nothing in these procedures shall be construed to limit or in any way affect the ability of such entities, agencies, authorities, or third parties to use such information in any manner permitted by law.

The underlined portion seems to say, despite the title of the subsection, that information cannot be independently obtained once it has been submitted to DHS and designated as Protected CII. We hope this is just a misreading of an ambiguous sentence, but we would urge that it be deleted, or modified to make clear that Protected CII applies only to information held by DHS, and not to identical information that already may be on file elsewhere, and that can otherwise be lawfully obtained .

In this regard, we note the language of 214(c) of the Act:

Independently Obtained Information.--Nothing in this section shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by subsection (a), including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.

Section 29.4(iii) states that the submitter must alert DHS if the information being submitted is required by another agency, provide the name of that agency and cite its legal authority. Elsewhere, the rule states that information already filed with another agency will not be considered Protected CII. What is unclear is what happens with information that *is required to be filed but has not yet been filed* with another agency. The Interim Rule at that point is silent on what happens next.

The Final Rule should, to be consistent, clearly state that this information may not be considered for Protected status.

The Final Rule Should Establish a Concrete but Practical Deadline For Review and Processing of Submitted CII.

The Interim Rule does little to change infirmities in the rules as originally proposed. It gives submitters too much control of information at all stages of the CII handling process. From submission to analysis to distribution in time of emergency, the reliance placed upon submitters' good faith endangers the public.

DHS can – and must – ensure that submitted information can be utilized efficiently and effectively by federal, state and local governments. It can do this by seeing that intake processing of the information begins at DHS, not at another agency, and that DHS moves expeditiously. Important CII documents should not languish on a DHS employee's desk. The viability of the entire CII program is threatened by delays that would render the information useless if it sits in a lengthy processing queue before being utilized to protect the infrastructure. The Department's modification of Section 29.6, allowing the program manager to determine "as soon as practicable" whether protection applies, is a standard with no teeth.

This "change" does nothing more than provide a recipe for abuse. The lack of a processing time limit will allow submitters to hide their shortcomings from future public oversight. Confident that the information they submit will be presumed "Protected" under the CII rules, submitters will have license to dump any and all information related to critical infrastructure on the CII Program Manager's desk. With no time limit, there is no mandate to process all submissions in a timely manner.

The lack of a time standard also runs afoul of the Freedom of Information Act (FOIA), which will be implicated when submitted information becomes the subject of a FOIA request. Under Section 552(a)(6)(A)(i) of FOIA, the government must determine whether to comply with a request for information within 20 working days of its receipt. This time limit can only be extended in "unusual circumstances" 5 U.S.C. § 552(a)(6)(B)(i). A delay of the government's own making does not constitute an unusual circumstance. The "as soon as practicable" standard in Section 29.6(e)(1) potentially conflicts with the FOIA requirements for reviewing that same information. Congress in 1996 extended the deadline for response to FOIA requests to 20 working days to "help Federal agencies in reducing their backlog." While we are cognizant of the almost routine failure of agencies to comply with the 20-day deadline, it is nonetheless inappropriate for an agency to adopt by regulation a different time limit. We imagine, that agencies without a mandate to find otherwise, will never find the 20-day limit "practicable." Then a formal time limit for making a Protected CII designation, within the FOIA 20-day limit, might serve to minimize backlog.

The Final Rule should contain a deadline certain by which submitted information is labeled "Protected CII" or rejected as unworthy of protection. This deadline can be flexible, with the rules containing a procedure whereby submitters can request expedited processing in the event of a demonstrated need for immediate analysis and use of submitted information by the government in situations where delays would threaten public health or safety. Likewise, the rules should allow the CII Program Manager to extend the processing deadline upon a specific, demonstrated need for more time to review the information; any requested extension should be subject to certification by the submitter that no immediate danger exists. It would be appropriate for DHS to revisit this issue after the program has been in place for a short period of time in order to determine what a proper deadline would be.

The justification for Section 214 of the Homeland Security Act and for these implementing regulations is that the specific information at issue could be used by terrorists to exploit vulnerabilities and that threats to the infrastructure from disclosure were immediate. The lack of a processing deadline in the Interim Rule belies that rationale.

A Second Review of Protected CII, Upon the Filing of a Freedom of Information Act Request, Would Add a Layer of Needed Protection.

There is a similar lack of oversight once CII has been accepted by the government. FOIA procedures need to be incorporated into the rules to ensure that information is not overly protected and that it is released when the need for confidentiality no longer exists. This will ensure that national security goals are met without aborting the public's right to know.

Protected CII is not subject to disclosure under the Freedom of Information Act. That is a statutorily mandated requirement under Section 214 of the Homeland Security Act. However, there is no statutory requirement that the FOIA officer turn a blind eye to the contents of information stamped "Protected CII" when a FOIA request is made for records which also contain information that is not protected or should not be protected. In such an instance, redaction of the exempt information and release of the unprotected information assures both security imperatives and the integrity of the CII process. It strikes a balance between protection of Critical Infrastructure Information and the disclosure of relevant, unprotected information which should be released under FOIA.

The Department should endorse the full inclusion of FOIA procedures in the Final Rule as both a practical tool and a solid statement against potential abuse of the confidentiality provisions.

It should also establish a specific time period during which any "Protected CII" designation will continue. At the end of that time period, the protection should disappear, unless the Department determines that security concerns have not yet been resolved or the submitter can show justification for an extension of the protected status. A review of Protected CII status at the time of a FOIA request is filed permits an analysis of whether protection remains warranted. It also provides a new framework for assessing the protection grant by evaluating the generic claim under the real-life context of how the information will potentially be used to benefit the public

As part of the FOIA review, the CII Program Manager or the Department's FOIA officer should solicit the views of the submitter. In some cases, the submitter may well benefit from release of the once-protected information. Demonstration that the submitter

has identified and corrected a potential security problem could provide positive publicity and credibility for the submitter and for DHS as well.

The benefits derived by requiring a review of Protected CII when there is a FOIA request would be enhanced if these rules allow for disclosure of information that is not Protected CII but had been submitted to DHS in the CII process. As noted above, there exists vast potential for submitters to abuse the protections offered under Section 214. In these instances, the critical review of Protected CII at the time of a FOIA request, combined with judicious redaction of ~~t~~ the limited information which should rightly be protected would provide a valuable check against submitters seeking to take advantage of the "good faith" standard. Redaction is standard practice under FOIA, a law that embodies our democratic belief that "disclosure, not secrecy, is the dominant objective." Department of the Air Force v. Rose, 425 U.S. 352 (1976). If FOIA contained no allowance for redaction, it is highly likely that no government information would ever be released to the public, as even the slightest amount of exempt material would result in the denial of most FOIA requests. While there must be protection for critical infrastructure information, this protection should not be all-encompassing, especially with a ready-made tool that will satisfy both those seeking protection of and access to Protected CII.

If a subsequent review of Protected CII status is implemented at the time of a FOIA request, DHS must provide for an independent appeals process allowing both the submitter and the requestor to obtain review within DHS.

In requesting a FOIA exemption for critical infrastructure information, private industry claimed that it would voluntarily share such sensitive information with the government only if it could be sure the information would not fall into the wrong hands and if the information could not be used to penalize the company in a civil lawsuit. But allowing infinite protection of this information does nothing to protect critical infrastructure. In fact, it breeds complacency.

DHS should sunset the protection it grants for CII, just as the "classified" status of national security-related documents is sunset. This would ensure an incentive for the submitter to actively attempt to fix a threat to the critical infrastructure. A reasonable time limit –some number of years – would spur submitters into actively attempting to fix a problem. Revealing a problem that has persisted past its sunset would both publicly

expose companies who fail to aggressively correct infrastructure problems and allow the public to assess and assist in remedying a problem. If a company could show that (1) it had actively worked to solve the problem, (2) there were continuing sensitivities, and (3) the problem was close to resolution, then DHS could extend the protection on a yearly basis. The declassification program has worked to the general benefit of both the intelligence community and those who request and use government documents. A sunset period for Protected CII status would do the same.

The Rule Must Facilitate the Government's Ability to Use the Protected CII Ensure Public Safety and Ensure Homeland Security.

The dangers inherent in granting Protected status are exacerbated by vesting submitters with excessive control of the eventual use of the information. The Interim Rule does not afford the government enough leeway to meaningfully use submitted information in some instances. The rule handcuffs federal, state and local governments when trying to warn the public or take action against a recalcitrant submitter.

Section 29.8(e) of the Interim Rule contemplates that the government can only give the public what amounts to a general warning about an attack on that infrastructure identified in Protected CII.[1] When an attack on the infrastructure is imminent or actually occurs, the foremost concern of the government should not be the protection a company's interests but the public's health and safety.

Exceptions should be drafted into the Final Rule that allow for the disclosure of specific information to first responders and to the public, including the news media, when there is an emergency that threatens widespread injury or loss of life. The disclosure of such information must not be contingent on the prior written consent of the submitter, as contemplated in Section 29.8(d)(2).[2] That restriction on adequate warning is an invitation to far greater disaster. If DHS is truly serious when trumpeting the sharing of CII as a

[1] Section 29.8(e) states: "The IAIP Directorate may provide advisories, alerts, and warnings to relevant companies, targeted sectors other governmental entities, ISAOs or the general public regarding potential threats and vulnerabilities to critical infrastructure as appropriate. In issuing and warning, the IAIP Directorate shall protect from disclosure the source of any Protected CII that forms the basis for the warning as well as any information that is proprietary, business sensitive, relates specifically to the submitting person or entity, and is not customarily in the public domain."

[2] Section 29.8(d)(2) states: "The Protected CII Program Manager or a Protected CII Program Manager's designee may not authorize State and local governments to further disclose the information to another party unless the Protected CII Program Manager or a Protected CII Program Manager's designee first obtains the written consent of the person or entity submitting the information."

safeguard against attacks on the nation's critical infrastructure, it will ensure that necessary warning and other useful information gets into the hands of those who can effectively use that information as a tool for the public benefit. The Interim Rule, as written, shifts the focus of the CII program from one which promotes safety and security of the public to one which promotes the public relations and the safety and fiscal security of private corporate interests.

The Department of Homeland Security Should Build Reasonable Public Accountability Standards into the Final Rule.

In reviewing these regulations, we continually came back to questions of accountability not addressed in the Interim Rule. What happens, we wondered, if a company submits Protected CII to DHS but for any reason is unwilling to follow through with the remedial actions DHS deems necessary to resolve or significantly mitigate the security threats identified?

In other circumstances, a federal agency might take legal action. Or impose some safety measures that would immediately affect the public. Or issue a warning to the public. All of these, incidentally, necessitate identifying the company – the source of the information. But that is prohibited under the Interim Rule.

We have suggested a number of revisions to the Interim Rule to deal with accountability issues, including a good faith standard, a pledge of concerted remedial action by the submitter, loss of "Protected" status for the information in certain circumstances, internal processing deadlines, the authority to identify the submitter when the nature of a warning warrants such action, and full and aggressive FOIA reviews, and a time for sunset, and a specific time limit for remediation. These would work to keep DHS aggressive and keep the submitters honest.

We also believe that DHS should establish a way to hold itself accountable, perhaps by reporting annually on the number of CII filings it is processing, and in general on the progress being made. This might indicate the amount of time "cases" have been outstanding as well as the number where threat concerns have been resolved and the case closed.

Respectfully submitted,

The Coalition Of Journalists For Open Goverment

By: _____

American Society of Newspaper Editors
Reporters Committee for Freedom of the Press
Radio-Television News Directors Association
Society of Professional Journalists
Society of Environmental Journalists
National Press Club
Investigative Reporters and Editors
Criminal Justice Journalists
Education Writers Association
Brechner Center for Freedom of Information
Freedom of Information Center, University of Missouri

Newspaper Association of America
National Freedom of Information Coalition

May 18, 2004