

American Society of Newspaper Editors.txt
Subject: Comments of the American Society of Newspaper Editors
Date: Sat, 14 Jun 2003 14:25:26 -0400
From: "Kevin M. Goldberg" <KMG@cohnmarks.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Pursuant to the Notice of Proposed Rulemaking dated April 15, 2003, on behalf of the American Society of Newspaper Editors, attached below are comments in the proceeding entitled "Procedures for Handling Critical Infrastructure Information." These comments are being filed in both Microsoft Word and .PDF format, as the Notice of Proposed Rulemaking did not specify the format preferred by the Department of Homeland Security. If you have any questions, technical or otherwise, please contact the undersigned counsel.

Kevin M. Goldberg
Cohn and Marks LLP
1920 N St., N.W.
Suite 300
Washington, DC 20036
(202) 452-4840
kmg@cohnmarks.com

<<DHS CII Comments.doc>> <<DHS CII Comments in PDF.pdf>>

DHS CII Comments.doc Name: DHS CII Comments.doc
 Type: WINWORD File (application/msword)
 Encoding: base64
 Description: DHS CII Comments.doc

DHS CII Comments in PDF.pdf Name: DHS CII Comments in PDF.pdf
 Type: Acrobat (application/pdf)
 Encoding: base64
 Description: DHS CII Comments in PDF.pdf

BEFORE THE DEPARTMENT OF HOMELAND SECURITY

In the matter of:)
)
Procedures for Handling)
Critical Infrastructure Information)
)
6 C.F.R. Part 29)
)
Notice of Proposed Rulemaking)
_____)

To: Associate General Counsel (General Law)

COMMENTS OF THE AMERICAN SOCIETY OF NEWSPAPER EDITORS

The American Society of Newspaper Editors ("ASNE") is a professional organization of approximately 800 persons who hold positions as directing editors of daily newspapers in the United States and Canada. The purposes of ASNE include assisting journalists and providing an unfettered and effective press in the service of the American people.

On April 15, 2003 the Department of Homeland Security ("DHS") released a Notice of Proposed Rulemaking ("NPRM") regarding procedures for handling critical infrastructure information ("CII"). This NPRM implements Section 214 of the Homeland Security Act of 2002 regarding the receipt, care, and storage of CII that has been voluntarily submitted to the government.¹ ASNE has worked with Congress and executive agencies for several years to achieve a proper balance between protecting homeland security and fulfilling the public's right to know where CII is involved and, therefore, understands the unique nature of this information. In fact, when advocating against passage of the Homeland Security Act of 2002 in its present form, ASNE representatives repeatedly iterated that its members are less concerned with the

¹ Title II, Subtitle B of the Homeland Security Act is also known as the "Critical Infrastructure Information Act of 2002."

details of any possible vulnerability to the infrastructure than being able to simply ascertain that a vulnerability exists in a given community. Unfortunately, the rules proposed in the NPRM will permit private industry, with government assistance, to hide all vulnerabilities from the public with little to no oversight. The Proposed Rules allow submitting entities to retain too much control over their information in a manner that binds the hands of the government to use that information. DHS will also be prevented from engaging in any meaningful use of CII in its possession because it will be overwhelmed by a flood of paperwork, leaving the agency ill-equipped to process all CII and the information in a state of limbo, of no use to the protection of homeland security.

The Proposed Rules Will Overburden the Department of Homeland Security in a Manner That Will Endanger Homeland Security.

Several of the Proposed Rules combine to create a situation in which just one DHS employee will be responsible for handling a massive amount of information received from a multitude of sources. That employee will not have the time, resources, or expertise to accomplish his or her job. The net result will be that information submitted to the government in an attempt to fix a vulnerability will flounder in an agency backlog and be useless to its desired goal.

There is No Legal Basis for Extending the Protections of the Critical Infrastructure Act of 2002 to Information Submitted to Agencies Other than the Department of Homeland Security.

The Proposed Rules exert a naked grab of power in direct contravention of the authority delegated to DHS by Congress. Proposed Rule 29.1(b) states, “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 is reinforced by Proposed Rule 29.2(i), which states, “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 CII will forward it to DHS.” Thus, the rules clearly contemplate that CII will be protected regardless of the agency to which the information is first submitted.

This expansive collection authority is in direct contravention of the Critical Infrastructure Act of 2002, in which Congress explicitly rejected protection of CII that is submitted to and approved by an agency other than the DHS. Section 214 of the Homeland Security Act, as enacted, only applies to a “covered federal agency”. Section 212 of the Homeland Security Act states that the only “covered federal agency” is the DHS. The breadth of federal agencies to whom the term “covered federal agency” would be applied was debated during the legislative process.² In rejecting the broader range of agencies to whom CII could be submitted, Congress’ desire to have the protections of this law apply to information submitted only to the DHS could not have been more explicit.³

The Proposed Rules Must Allow for Multiple Department of Homeland Security Employees to Review and Validate Submitted Information.

Proposed Rule 29.6(a) states that “Only the Program Manager or the Program Manager’s designee, is authorized to acknowledge and validate the receipt of information as Protected

² On July 26, 2002, the House of Representatives voted on House Amendment 598, introduced by Rep. Tom Davis (R-VA). House Amendment 598 sought to define the term “covered Federal agency,” as the Department of Homeland Security and agencies with which the Department shares critical infrastructure information. It was rejected by a vote of 195-233, with 5 Representatives not voting.

³ Perhaps recognizing the burden that will be imposed upon other federal agencies, Proposed Rule 29.4(c) requires any other agency that handles CII to create a position called known as the “CII Officer”, who will manage and oversee implementation of this law. Thus, the Proposed Rules actually increase the personnel required by agencies other than DHS. The federal government has not funded these agencies to allow them to accomplish this goal; the DHS cannot mandate that these agencies add additional personnel, and foot the cost for doing so, without receiving some benefit in return.

CII.”⁴ It is unclear from this language whether the “Program Manager’s designee” is envisioned as just one person within DHS who must act as the Program Manager’s proxy or whether the Program Manager can designate a limitless number of DHS employees to assist in processing submitted CII. The DHS should clarify this distinction in its final rules in a manner that allows the maximum number of DHS employees to engage CII review and validation. Only through the use of multiple employees will the DHS be able to prevent the backlogs that will invariably result from the review and validation of thousands of documents on a yearly basis. A single CII Program Manager cannot fully evaluate the highly specialized aspects of each portion of our nation’s critical infrastructure.

Though They Should Not Collect Critical Infrastructure Information, Other Agencies Should be Allowed to Take an Active Role in the Review and Processing of this Information.

Rather than granting protection to all information submitted to any federal agency and forwarded to DHS, the Final Rules should allow those other agencies to use their expertise to determine whether that information truly qualifies for protection, but only after these agencies receive the information from DHS. Unfortunately, the non-DHS “CII Officer” that is created by the Proposed Rules is merely an administrative position, a “traffic cop” who will simply funnel paperwork through his or her agency to the DHS. The Proposed Rules only vest with the DHS’ own CII Program Manager the authority to declare CII as “protected” under these rules.

The DHS is charged with protecting homeland security but that does not mean that it will have the ability to unilaterally accomplish that task. DHS cannot seriously claim to be better qualified than the Nuclear Regulatory Commission to determine whether the alleged deficiencies

⁴ Proposed Rule 29.4(a) vests all authority for administering the CII Program with the Under Secretary of the Information. This official must appoint a “CII Program Manager” to direct and administer the CII Program. Proposed Rule 29.4(b)(1).

at the physical borders of a nuclear power plant would actually allow a terrorist to attack that plant; nor can it claim superior knowledge in the area of airline security when regulatory oversight of that industry is charged to the Department of Transportation. These are just two examples of how DHS could benefit from outside consultation.

ASNE does not advocate that the DHS abdicate its role in reviewing CII submissions to these agencies, it simply suggests that the excessive overbreadth of the Homeland Security Act of 2002 caused by allowing private companies to submit CII through any federal agency – as well as the attendant burdens on those agencies finances and manpower – could be significantly reduced by allowing experts to scrutinize these submission to ensure they are truly related to homeland security and not just an abusive filing. Proposed Rule 29.6(b) must be amended to allow for consultation with the other agencies that will process these requests.

Enforceable Processing Deadlines Must be Created to Ensure that Significant Information Does Not Languish on the CII Program Manager's Desk.

Proposed Rule 29.6 also contains one glaring omission from the acknowledgment, receipt and validation process: there is no time limit within which the CII Program Manager (or his or her designee) must make a determination as to whether the submitted information qualifies as Protected CII. The federal FOIA, and every state Freedom of Information or Right to Know Act, contains a time limit for compliance with a filed request for information.⁵ This a requirement ensures that the requestor receives an answer While the need for that information is still ripe. Nowhere is this more necessary than in the highly sensitive arena of infrastructure vulnerability. A mandated period in which the agency must act benefits the public interest because it ensures that DHS will engage in timely review of sensitive issues. ASNE has already made this

⁵ The Federal FOIA states that an agency has 20 days to respond to a FOIA request with an indication as to whether it will comply with or deny the request. 5 U.S.C. § 552(a)(6)(A)(i).

argument in comments before the DHS, when it sought an additional basis for expedited processing of FOIA requests in the DHS proceeding entitled In the Matter of Freedom of Information Act and Privacy Act procedures, 6 C.F.R. Chapter I and Part 5:

The United States District Court for the District of Columbia only recently granted expedited access to records held by the Department of Energy which were relevant to a special “energy task force” created by President Bush. Its decision noted the secrecy in which the task force had cloaked itself and the immense public concern in the issues under its jurisdiction, particularly those which were intertwined with the events of September 11. Natural Resources Defense Council v. Department of Energy, 191 F.Supp.2d 41 (D.D.C. 2002); Judicial Watch, Inc. v. Department of Energy, 191 F. Supp.2d 138 (D.D.C. 2002). Many of the DHS’s records will cover similar topics. The maximum invocation of expedited processing procedures for these records of recognized public importance is imperative to allow the public, and the press as its surrogate, to ensure that a thriving democracy, based on informed and timely public participation in government, provides the bedrock of homeland security.

Comments of the American Society of Newspaper Editors at pages 2-3.

The ability of an agency to process information in a timely manner without regulatory compulsion is most certainly the exception, not the rule, where handling of government information is concerned. The record of federal agencies in processing submissions and requests for information is woefully subpar. In August 2002 the United States General Accounting Office released a report entitled Information Management: Update on Implementation of the 1996 Electronic Freedom of Information Act Amendments. That report studied 25 executive branch agencies, analyzing their progress in processing FOIA requests. It found that the number of requests received and processed appeared to peak in fiscal year 2000 and decline in fiscal year 2001 while “the agency backlogs of pending requests are substantial and growing governmentwide.” Id. at 2. When one looks at agency processing times, it is clear that rapid response is not within the government’s standard operating procedures. Estimated response times for FOIA requests in 2001 for key agencies were:

- Department of Energy:
 - 211 days for a “Simple Track Request”
 - 1,788 days for a “Complex Track Request”
- Department of Justice:
 - 137 days for a “Simple Track Request”
 - 1,311 days for a “Complex Track Request”
- Department of Treasury:
 - 20 days for a “Simple Track Request”
 - 232 days for a “Complex Track Request”
- Environmental Protection Agency:
 - 36 days for a “Simple Track Request”
 - 333 days for a “Complex Track Request”

Id. at 13-14. These processing times, if applied to the review and analysis required of a CII Program Manager, will result in documents remaining unlabeled for several months or even years. By this time one would expect the remedial process, not the review process, to be completed. The presence of a mandatory processing deadline is necessary to ensure some opportunity for enforcement. It is only this form of compulsion that will truly ensure the system functions as intended.

DHS alone has been charged with implementing the Critical Infrastructure Information Act of 2002. It is the second largest federal executive branch agency and, presumably, will be provided with the funding required to ensure that this law is implemented. Submission of CII must be limited to DHS with that agency receiving the manpower necessary to perform its job unless Congress is willing to fund the resources and personnel necessary for every federal agency to handle the massive increase in paperwork and review that will result from this questionable interpretation of law.

The Proposed Rules Stifle Effective Emergency Response Efforts by Offering Too Much Control and Protection to Submitters.

The Proposed Rules allow a submitting entity to retain excessive and unnecessary control over information it has willingly given to the government. When submitting information to the government with a claim that the information is related to our national infrastructure and the protection thereof, an entity should be required to trade some measure of control in exchange for the assistance it receives in remedying a security vulnerability. Allowing the submitter to exert sole control over that information defeats the purpose of enlisting government assistance. The final rules must allocate greater discretion to the government, and its employees, to use that information to prevent and respond to emergencies; the rules must also define “good faith” so as to provide some check on the ability of private industry to abuse these procedures.

Submitters Retain Too Much Control Over Use of their Information by the Government in Preventing or Responding to Emergency Situations.

Proposed Rules 29.8(c)-(d) allow a submitter to veto the use of information to prevent or respond to an emergency.⁶ The Proposed Rules create, with one fell swoop, thousands of informal non-disclosure agreements between submitters and the federal government, each of which binds third parties without their input or consent. It is these third parties – state and local government officials – who, in the event of an actual or impending emergency situation, will be the ones who are called upon to respond, not the DHS CII Program Manager. Forcing them to contact the CII Program Manager in the event of an emergency, who must then contact each

⁶ Proposed Rule 29.8(c) states, “[Federal] contractors shall not further disclose Protected CII to any of their components, employees, or other contractors (or other subcontractors) without the prior written approval of a CII Officer unless such disclosure is expressly authorized in writing by the submitter.” Proposed Rule 29.8(d) states, “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.”

submitter and receive written permission to use that submitter's information, is guaranteed to result in catastrophe.

Disclosure of CII, even that which contains sensitive details, to non-governmental entities is a necessary and regular function of responding to an emergency. ASNE is acutely aware of this fact because newspapers are often among the first non-governmental entities contacted in an emergency situation. Newspapers and other media are asked not only to notify the public of the existence of an emergency, but also to instruct the public as to how to best protect themselves from harm. This often requires the disclosure of information that could be considered "Protected CII". For instance, the identity of chemicals held at a chemical plant and the possible result of their mixture could be labeled "Protected CII". The same is true for the identification of the most efficient ingress and egress to that chemical plant. Yet, in the event of an accidental, or even terrorist-related, chemical explosion at that plant, the first information that the public would want is the worst case scenario in the event that a potential dangerous compound is created. The second, in the event of this compound's release into the local atmosphere or ground water, would be how to quickly flee from the immediate vicinity of the plant. Announcement of an emergency situation, without any indication of the extent of that emergency or how the public can protect itself, will create a panic-driven response which would pose even more danger to the population.⁷

The Proposed Rules will also damage relationships between the press and government officials that have been cultivated over time. In communities throughout the United States, the local government and press have learned to work together in order to provide safety to the

⁷ The federal government actually requires, through the use of the Emergency Alert System ("EAS"), all broadcast media to be able to broadcast such emergency or disaster information to the public at a moment's notice. Under the Proposed Rules, the EAS system would be activated, but crucial follow up details could not be broadcast.

citizenry. Proposed Rules 29.8(c)-(d) will prevent these collaborations from working effectively in a time of emergency. Worse yet, they will destroy the sense of trust that has grown as both sides have shared information and come to understand the other's needs and roles in emergency management. There must be some exemption that allows state or local government officials to release Protected CII to the public upon a reasonable belief that disclosure benefits the public interest in averting a specific danger to public health or safety.

Proposed Rule 29.8(f) creates the same danger when it limits the instances in which an officer or employee can disclose Protected CII with the knowledge that he or she will not be prosecuted. The rule only allows disclosures by a government employee, with prior approval, to Congress or the United States Comptroller General, or in furtherance of the investigation or prosecution of a criminal act. In order to disclose Protected CII without such prior approval the employee must evidence: (1) an employee's or agency's conduct in violation of criminal law or other law, rule or regulation affecting the critical infrastructure, or (2) mismanagement, a gross waste of funds, an abuse of authority or a substantial and specific danger to public healthy or safety affecting the critical infrastructure. However, that employee will be prosecuted if he or she wrongly asserts the existence one of these bases for disclosing information, even if the disclosure is made with the best of intentions. The determination of whether the employee is correctly gauging whether mismanagement, gross waste of funds, abuse of authority, a "specific danger to public healthy or safety" or whether the information actually relates to the protection of critical infrastructure, is a difficult one to make, as no definite standards exist to guide that determination.

Whistleblowers perform a crucial safety function in our society. These government employees are willing to risk their jobs and reputations in order to make our nation safer. Their

work often involves CII that will remain secret under these Proposed Rules; yet case studies compiled by the Government Accountability Project make clear that disclosure of this type of information often makes us safer than if the information were suppressed:

- Despite repeated claims by the Department of Transportation that our nation's airports are now safer than they were before September 11, 2001, former FAA Security Expert Bogdan Dzakovic argued, based upon his personal visits to major United States and foreign airports, that the Federal Aviation Administration was covering up certain findings that would have denigrated the airline industry. His findings were upheld by the United States Office of Special Counsel.⁸
- Mick Anderson was a senior advisor for policy planning in the Criminal Division of the United States Department of Justice. His work related to the training of foreign law enforcement officials. In 1997, Anderson noted to the Department of Justice Security Chief that there were numerous leaks of classified information from within the Criminal Division. His report resulted in a security sweep by that division and a three year investigation by the Office of the Inspector General, which confirmed all of his allegations. In 2001, Mr. Andersen won the U.S. Office of Special Counsel Public Service Award.
- Mark Graf was a seventeen year veteran at the Department of Energy's Rocky Flats Environmental Technology Site when, in 1995, after a private security agency took over the site, there were numerous security vulnerabilities, including elimination of a key bomb detecting unit, relaxation of emergency drills, and negligence in inventory of highly unstable elements. Although repeated attempts to bring these vulnerabilities to light were rebuffed, Mr. Graf's continued efforts resulted in legislation in the 1998 Defense Authorization bill that requires an annual review of the Department of Energy's entire Safeguard and Security Program.⁹

The chilling effect of Proposed Rule 29.8(f) threatens the ability of whistleblowers to act as another layer of protection against accidental or intentional damage to our infrastructure. The Final Rule should allow a whistleblower to remain free from prosecution upon demonstration of a reasonable belief of the existence of one or more justifications for disclosure. It should also

⁸ Despite his vindication, Mr. Dzakovic was transferred to a clerk-type position immediately after his disclosure, where he remains, thereby lending credence that the government will utilize the fullest prosecutorial tools available to it in order to retaliate against whistleblowers.

⁹ Before he was proven correct, Mr. Graf had been placed on administrative leave by his superiors.

contain an exemption allowing a government employee to disclose Protected CII in the event of an actual emergency or the proven pendency of an emergency.

The Term “Good Faith” is a Key Element of these Proposed Rules, Yet it Remains Undefined.

The lack of any definition of “good faith”, which appears twice in the Proposed Rules, is a glaring and dangerous omission. Without any definition of that term, the DHS is deprived of an integral method of reviewing CII submissions for possible abuse or unintentional overbreadth.

Proposed Rule 29.6(f) provides the only instance in which a CII Program Manager can unilaterally adjudge that information is not “Protected CII”:

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.

In all other instances, the submitter gets a second chance to meet the low threshold required for information to be labeled “Protected CII.” There is never any public participation in the CII process; the submitter will have repeated, unopposed, attempts to prove its case that the information qualifies for protection with only the undefined term “good faith” – and its interpretation by an already-overwhelmed CII Program Manager – acting as a check against possible abuse by companies seeking to hide their negligent or willful acts from the public.

The effect of this provision is especially important in light of Proposed Rule 29.6(e)(1)(i)(d), which determines the fate of submitted information in the event of the denial of full protection under these rules. This Proposed Rule allows a submitter to state in the event that 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.” Thus, the

submitter gets a “do-over” whereby a mistake in its judgment that submitted information qualifies as Protected CII is forgiven. No other entity is offered such favorable treatment. A submitter is not the governor, nor should it act in that capacity. By requiring every submitter to consider the repercussions in the event of its misjudgment, another layer of review is instituted that ensures the final rules apply only to information that is truly related to the protection of the critical infrastructure. Without some teeth in the definition of “good faith”, every submitter will push the limits of that term, secure in the knowledge that should its information (somehow) not qualify as Protected CII, there will be no negative ramifications.

The term rears its head again in Proposed Rule 29.8, which states:

Protected CII shall not, without the written consent of the person or entity submitting such information, be used by any Federal, State or local authority, or by any third party, in any civil action arising under Federal or State law if such information is submitted in good faith for homeland security purposes.

This is the crux of ASNE’s longstanding argument against the Critical Infrastructure Act of 2002 – that a private company will be able to avoid any punishment or liability for negligent or willful behavior by labeling any evidence thereof as “Protected CII”. Any large corporation will be able to hide any form of corporate malfeasance under the guise that to reveal even financial data would result in a potential breach of security. The company’s stockholders likely would be unable to recoup their financial investments if the submission is adjudged to be in good faith. And that determination is left to just one person.

The term “good faith” is the lynchpin of two key protections guaranteed to CII submitters: (1) the right receive full protection of its information with little to no opposition and (2) the right to remain virtually free of any civil liability. Yet, the application of that term is likely to be arbitrary. DHS should allow some public participation in the determination of whether a submission is made in good faith, even if it only takes the indirect form of defining

how that term will be applied. Including a definition of “good faith” in Proposed Rule 29.2 after opportunity for public comment will achieve this.

There Should be a Second Review as to Whether Information Qualifies as “Protected CII” Upon the Filing of a Freedom of Information Request Incorporating These Documents.

The Proposed Rules grant sole power to the submitter and the CII Program Manager to determine whether submitted information is Protected CII. At time these determinations will be made, there is little reason that either the submitter or CII Program Manager will believe the information is unworthy of such protection. If the final rule provides for an additional review of protected CII status, upon the filing of a FOIA request for that information, there will be an additional safeguard that this information is related to the protection of the critical infrastructure.

There are several reasons the addition of a second, delayed, layer of review is beneficial. The passage of time might result in the correction or extinction of the vulnerability. Rather than serving as a positive example of how a company was able to detect, correct, and learn from its mistakes, the failure to disclose the prior existence of any problem will remain hidden even though there would be no harm resulting from its disclosure. Instead of resting safe in the knowledge that, while vulnerabilities may exist, they can be rectified, the public will remain ignorant of the extent of any danger, and will likely assume the worst anytime a vulnerability does become public. While it could serve as a model for the correction of similarly situated vulnerabilities, submitted CII will serve no useful purpose.

The framing of a FOIA request may spur reconsideration by the submitter as to the positive uses of this information. In the same way that the existence of a controversy is necessary to make a lawsuit ripe for consideration, so too will the filing of a FOIA request frame the analysis as to whether the requested protection for submitted CII remains necessary.

Allowing review of Protected CII upon the filing of a FOIA request engages citizenry and industry in working together to ensure homeland security. It will promote dialogue which, even if unresolved, will serve to enhance public trust of both government and industry.

Information that Does Not Qualify as “Protected CII” Must be Made Available to Freedom of Information Act Requestors, Subject to the Redaction of “Protected CII.”

Proposed Rule 29.8 must also allow for redaction of information that qualifies as Protected CII while disclosing information that poses no threat to the nation’s critical infrastructure. By incorporating a redaction requirement, the DHS will ensure that only information which is absolutely necessary to the protection of the critical infrastructure will remain hidden from public view. It will also force submitters to closely consider the scope of the alleged vulnerability, as they will be required to determine the precise nature of that vulnerability in order to receive the full protection of these rules.

Conclusion

The Proposed Rules are, in places, a functional nightmare. They allow CII submitters to act as surrogate governors and withhold information even when disclosure is absolutely necessary to avoid disaster. DHS has ill-equipped itself to handle the resulting number of documents it will receive by vesting all responsibility and authority in just one DHS official who will have neither the time, resources nor expertise to skillfully perform his or her duties.

Once this information resides within the DHS storage facilities, it will be of little to no use in protecting the public. Even if a submitter consents to disclosure of Protected CII to state and local government officials and members of the public involved in response efforts, achieving any disclosure will be a logistical impossibility when the task of effectuating consent will fall to that single, overwhelmed, DHS CII Program Manager. Any employees who are able to

preemptively avoid a potential emergency by revealing serious safety concerns face criminal prosecution if, even with the best of intentions, they incorrectly gauge that their actions are protected by law.

The defining characteristic of these Proposed Rules is that they allow a private entity to control the ultimate response to any emergency on a federal, state or local level – even after that entity has submitted information to the federal government as an admission that it is ill-equipped to deal with the emergency. If a private company recognizes a security problem that is so pervasive and dangerous that it requires the assistance of the government in order to be corrected, then the government should be given the ability to assist and correct the problem, and the public should at least be given the right to know that the problem exists. The Proposed Rules allow neither.

Respectfully Submitted,

A handwritten signature in black ink, appearing to read 'P. Bhatia', with a stylized, cursive script.

Peter Bhatia
President

June 16, 2003