www.progressiveregulation.org

FACT SHEET

Department of Homeland Security
Procedures for Handling Critical Infrastructure Information;
Proposed Rule – published in 68 Fed. Reg. 18525

COMMENTS DUE ON JUNE 16, 2003

What the Rule Does Not Do:
No Workable Procedures for Review of Industry CII Claims

While the proposed rule contains several questionable provisions, discussed in detail below, its primary flaw is what it does not do. It does not set up a workable system for reviewing CII claims and ensuring that the law is not subject to abuse.

Amazingly enough, the Department of Homeland Security (DHS) makes a commitment in the proposed rule to review ***every*** piece of "critical infrastructure information" (CII) in order to determine whether the submission is, in fact, CII under the law. The proposed regulation states that this review will take place ***when DHS first receives the information***. If the DHS "CII Program Manager" determines that the information is ***not*** CII, the submitter will be notified and given an opportunity to lobby for a reversal of this adverse decision. See 68 Fed. Reg. 18527, 6 C.F.R. §29.6(e).

We must await the next budget cycle to determine the resources DHS will commit to this potentially onerous and overwhelming task. However, it is likely that if companies take full advantage of the law's broad definitions, the flood of submissions will force DHS to convert this upfront process into a superficial, cursory review.

Most troubling, the proposed regulation does not provide any opportunity to review this initial determination as more facts come to light. Nor do they allow people requesting the information to challenge the CII claim and have DHS make a decision that the claim is invalid on the basis of information provided by the requester, as is typically done in the context of Freedom of Information Act requests.

A crucial test of the validity of a CII claim is whether the information is "customarily in the public domain." See 68 Fed. Reg. 18325, 6 C.F.R. §29.2(b) (defining CII in conformance with the Homeland Security Act). Since the status of information in this regard can change over time, it is especially important that DHS provide for a revisiting of its initial determination. To omit this crucial component of a workable rule is to ensure that a morass of litigation will be necessary to resolve these questions.

Recommendation: DHS must revise the proposed regulation to provide for ongoing review of the legitimacy of CII claims. The final rule must provide an opportunity for requesters to provide evidence challenging such claims and bind DHS to consider it.

Using Other Agencies as Conduits for Unrestricted CII Claims

The implications of DHS's failure to establish a workable review procedure are compounded by its misguided and arguably illegal decision to encourage companies to use other agencies as conduits for CII, rather than requiring that all such information be submitted directly to DHS. See 68 Fed. Reg. 18525, 6 C.F.R. §29.2(i). Not only must agencies and departments act as conduits, they must establish procedures for protecting CII when it is given to them, presumably in response to the submitter's claim that it is CII, as opposed to any independent verification they might wish to conduct. 68 Fed. Reg. 18527, 6 C.F.R. §29(7).

The CII provisions enacted as part of the Homeland Security Act limit the opportunity to submit CII, and the authority to protect CII, to the "covered federal agency," in turn defined solely as DHS. See Section 214(a), Title II, Subtitle B, of the Homeland Security Act of 2002, P.L. 107-296. Advocates of the legislation made an unsuccessful attempt to extend this opportunity and authority to all federal agencies and departments, but the amendment was soundly defeated on the House floor. Congressional Record, H5850-53, H5869-70 (July 26, 2002). For DHS to decide to use federal agencies and departments as conduits for CII violates the clear intent of the law.

DHS will defend this provision by arguing that it does not give agencies and departments authority to "acknowledge and validate the receipt of Protected CII." See 68 Fed. Reg. 18526, 6 C.F.R. §29.5(a). Rather, DHS will say, other agencies are merely instructed to forward CII to DHS when explicitly directed to do so by the submitter. Or, in other words, acting as a conduit for information does not violate the intent of the law because it does not confer authority to accept and protect CII, which was the purpose of the amendment rejected on the House floor.

Nevertheless, the provision allowing other agencies and departments to receive and forward CII compounds the problems with the confused and ineffective process for reviewing such information. With protected information seeping into files government-wide, it is very difficult to imagine how DHS will keep up with its review, much less track its dispersal. In the free-for-all that follows, the lodging of CII claims will inevitably inhibit the daily operations of government, especially because there are

criminal penalties for disclosing it improperly, but there are no penalties for making blatantly unsupported CII claims. See 68 Fed. Reg. 18529, 6 C.F.R. §29.9(d).

Indeed, it is tempting to conclude that the conduit provision was a deliberate attempt by supporters of the Act to chill use of a wide range of information for any purpose other than the protection of CII by DHS. This effort flouts the clear intent of the Act, which explicitly preserves the normal use of information that ***is*** "customarily in the public domain." While the proposed regulation acknowledges these provisions, it sets up circumstances that, as a practical matter, are very likely to result in their routine violation. See 68 Fed. Reg. 18525, 6 C.F.R. §29.2(b) (acknowledging that CII does not include information customarily in public domain), 6 C.F.R. §29(j) (defining which types of information cannot be deemed CII).

At his confirmation hearing before the Senate Committee on Governmental Affairs, Tom Ridge promised to establish a "tag and track" system to ensure that CII claims sent to DHS would be labeled and processed correctly. See Pre-hearing Questionnaire for the Nomination of Tom Ridge, Nominee for Secretary, Department of Homeland Security at 37-38 (answer to question 67 posed by the Committee). Such a system is vital to ensure that false claims are not spread throughout government without any opportunity to question and refute them, potentially paralyzing routine functions. Instead of establishing such a system, DHS has done the opposite, ensuring that it will never be able to keep up with false claims and that its fellow agencies and departments will challenge them under the threat of committing criminal violations.

Recommendation: The proposed rule must eliminate provisions allowing other agencies and departments to act as conduits for CII. It must instead establish a "tag and track" procedure for monitoring the dispersal of CII and continuously reviewing the validity of such claims.

Meaning of "Voluntarily" Submitted

To qualify for confidential treatment, CII must be submitted to DHS "voluntarily," a term the Act defines to mean "submittal thereof in the absence of such [covered] agency's exercise of legal authority to compel access to or submission of such information." See Section 212(7), Title II, Subtitle B, of the Homeland Security Act of 2002, P.L. 107-296. Following this provision to the letter, DHS's proposed regulation states that to qualify for protection, the CII must be submitted "***in the absence of DHS's exercise of legal authority*** to compel access to or submission of such information." See 68 Fed. Reg. 18526-7, 6 C.F.R. §29(j) (emphasis added).

This approach reflects a considerably more conservative, even crabbed, interpretation of the law than the liberal, arguably illegal interpretation that permits agencies and departments throughout the government to act as conduits for CII. When combined with the conduit provision, the definition of voluntary in the proposed regulation means that agencies and departments receiving CII claims cannot dissolve such claims by simply exercising their own authority to obtain it independently. Rather,

they must forward the claims to DHS, which may or may not have authority to obtain the information independently, and may or may not review the legality of the claims.

If companies engage in widespread gaming of this distorted system, labeling as CII the information they formerly provided to agencies and departments to demonstrate compliance with applicable regulatory requirements, regulators will be hard-pressed to loosen the restrictions on this data unless and until DHS assists them. This daunting hurdle will place the entire burden of refuting CII claims on the question whether the information was customarily in the public domain.

To its credit, DHS has included a provision instructing companies ***not to claim*** CII treatment for information that "***is required to be submitted*** to a Federal agency to satisfy a provision of law." 68 Fed. Reg. 18526, 6 C.F.R. §29.3(a). This provision correctly reflects the legislative intent not to cover information that was already available to the government. Unfortunately, however, since there is no enforcement mechanism available to agencies and departments or requesters wishing to invoke this prohibition, and the process for asserting CII claims through those same agencies and departments is so open and confusing, the prohibition may well prove meaningless as a practical matter.

Recommendation: DHS must rewrite its proposed regulation to state that information formerly provided to other agencies and departments throughout government is "customarily in the public domain" unless it is covered by other, existing Freedom of Information Act exemptions (e.g., protection of confidential business information). The final regulation should provide that submitters mislabeling information in violation of the rule's requirements will lose CII status for that information and will have all future claims scrutinized more carefully.

For more information, please contact Rena Steinzor at (410) 706-0564, rstein@law.umaryland.edu.