

Subject: Comments of Lockheed Martin Corporation
Date: Mon, 16 Jun 2003 14:47:34 -0400
From: "Miller, Barry" <BMiller@wbklaw.com>
To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Attached are comments submitted on behalf of Lockheed Martin Corporation in response to the Notice of Proposed Rulemaking issued by the Department of Homeland Security (DHS) on April 15, 2003 (68 FR 18524) seeking comments on a proposed rule for the receipt, care, and storage of voluntarily submitted Critical Infrastructure Information.

Barry P. Miller
Wilkinson Barker Knauer, LLP
2300 N Street, NW
Suite 700
Washington, DC 20037-1128
202-383-3411 (phone)
202-783-5851 (fax)
bmiller@wbklaw.com
www.wbklaw.com

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

³ Section 10(b)(1)(B) of the Homeland Security Act.

damage from potential attacks.⁴ Critical to the success of these missions is improved coordination and information sharing among previously separate government agencies brought together in the newly established DHS in order to protect our nation.⁵ Useful information relating to Critical Infrastructure,⁶ which is frequently maintained by private entities rather than government agencies, will only be given by private entities to DHS if the proposed rule, modified and clarified as discussed herein, is implemented. Adoption of this rule will enable DHS to have ready access to information to assist in preventing terrorism, protecting lives and property, and promoting economic stability.

Some commenters will no doubt assert, as they have in the past, that protecting voluntarily submitted CII would deprive third parties of a perceived “right” to access that CII. The concerns underlying such assertions are legitimate—rooted as they are in a desire to maintain the public’s ability to oversee the actions of its government. However, objections to the proposed rule based on a “public right of access” are misplaced. Private sector CII will not be voluntarily submitted to DHS absent appropriate safeguards relating to its use and releasability. Simply put, if the protections in the proposed rule are not implemented, there will likely be CII to have access to. As a consequence, DHS will be denied information critical to successful performance of its mission; and, those persons objecting to the proposed rule on the basis of a public interest in securing access to CII will, in fact, only ensure that the public’s important interest in having a well-informed DHS will be thwarted. Even if, however unlikely, CII is voluntarily submitted without protections against its potential misuse, the real beneficiaries will be those who would use the information to perpetrate acts of terrorism – not the public.

Although Lockheed Martin is very supportive of the proposed rule and its purposes, there are several proposed sections that, if clarified and/or slightly modified, would make the proposed rule even more effective. Those items that Lockheed Martin believes need clarification and/or modification are set forth below.

II. ISSUES FOR ADDITIONAL CLARIFICATION OR MODIFICATION

Definition of Critical Infrastructure Information. The proposed rule defines “Critical Infrastructure Information” (CII) to include “records or information” concerning certain defined categories of information.⁷ Lockheed Martin strongly supports defining CII to include both records and information. Any argument that information should be excluded is not warranted under current law. Specifically, S.609 (the Restoration of Freedom of Information Act of 2003), which has been introduced, seeks to amend the current Act to remove coverage of information not contained in “records.” Lockheed Martin notes, however, that FOIA applies only to records. Thus, information known to a government agency but not contained in a document or record is not discoverable via a

⁴ Section 10(b)(1)(C) of the Homeland Security Act. See, Statement of DHS at <http://www.dhs.gov/dhspublic/faq.jsp>.

⁵ See, Statement of DHS at http://www.dhs.gov/dhspublic/theme_home1.jsp that the president decided that the 22 previously disparate domestic agencies needed to be coordinated into one department to protect the nation against threats to the homeland.

⁶ Critical Infrastructure Information is defined as “information not customarily in the public domain and related to the security of critical infrastructure or protected systems... concerning [certain defined categories].” NPRM at 18525, Proposed Rule at Section 29.2(b), 6 CFR 29.2(b). As discussed below, certain revisions to this definition may be warranted.

⁷ NPRM at 18525, Proposed Rule at Section 29.2(b), 6 CFR 29.2(b).

FOIA request. Any comment or other argument made in this proceeding that “information” should not be protected under the CII Act in order that it can be released under FOIA, fails to recognize that FOIA does not provide for its release. Regardless, if “information” not contained in records is to be removed from the purview of the CII Act, it cannot be eliminated in a rulemaking.

The proposed rule defines “protected critical infrastructure information” as “CII... that is voluntarily submitted to DHS.”⁸ The proposed rule requires that the submitter expressly request that the submitted information be forwarded to DHS’s IAIP Directorate. Lockheed Martin notes that this specific request for forwarding may not always be made, especially in time-sensitive situations. Moreover, Section 29.5(c) provides that information that is not forwarded to the CII Program Manager⁹ will not qualify for protection.¹⁰ As a result, information submitted in good faith reliance on the Rule might fail to be protected under the Rule solely because the submitter failed to request that the information be forwarded to the CII Program Manager. Lockheed Martin supports the position in the proposed rule that information submitted with any reasonable indication that the submitter expects it to qualify as Protected CII should qualify as Protected CII until and unless it has been deemed otherwise. Further, such information should either be maintained with the submitter’s consent or be disposed of in accordance with the Federal Records Act, pursuant to Section 29.6(i) of the proposed rule.

Lockheed Martin believes that the Final Rule should provide that facilities or other assets that support the development of national defense systems constitute “Critical Infrastructure” so that information regarding the same clearly qualifies as “Protected CII.” Although the definition of “Critical Infrastructure” in proposed Section 29.2(a)¹¹ includes “systems or assets... so vital... that [their] incapacity or destruction would have a debilitating impact on security..., national public health or safety, or any combination thereof,” clarification of the term’s applicability to defense systems would remove any doubt and would further encourage potential submissions of valuable CII.

With regard to the disposition of information deemed not to be Protected CII, Lockheed Martin supports the suggestion in Section 29.6(i) that when a submitter requests it, information be “disposed of in accordance with the Federal Records Act” to the extent that this contemplates destruction. It must be noted however, that the Federal Records Act provides a general mandate that records be maintained, not destroyed. Thus, the language in Section 29.6(i) of the proposed rule regarding disposition under the Federal Records Act may in fact be insufficient to authorize agencies to destroy records containing CII once a submitter has requested destruction. Lockheed Martin suggests that the Rule as promulgated state the specific authority, under the Federal Records Act or otherwise, pursuant to which records containing CII may be destroyed when the submitter has requested destruction.

The proposed rule defines “voluntarily” submitted to exclude information which DHS has the legal authority to obtain, as well as any information submitted or relied upon as a basis for making determinations on licenses or permits, information submitted during regulatory proceedings, and information submitted pursuant to other legal requirements.¹² It is unclear under the current language

⁸ NPRM at 18525, Proposed Rule at Section 29.2(f), 6 CFR 29.2(f), and at Section 29.2(i), 6 CFR 29.2(f).

⁹ Appointed by the Undersecretary pursuant to Section 29.4(b)(1).

¹⁰ NPRM at 18527, Proposed Rule at Section 29.5(c), 6 CFR 29.5(c).

¹¹ NPRM at 18525, Proposed Rule at Section 29.2(a), 6 CFR 29.2(a).

¹² NPRM at 18526, Proposed Rule at Section 29.2(j), 6 CFR 29.2(j) and at Section 29.3(a), 6 CFR 29.3(a).

whether a private contractor that is already contractually obligated to provide certain types of information to DHS (or one of its components) might be deemed to submit CII other than voluntarily to assist in anti-terrorism efforts. Lockheed Martin believes the language should be clarified to encourage submissions under such circumstances by stating that information submitted under such circumstances will not cease to qualify as “voluntarily” submitted because of the existence of a contractual relationship between the submitter and DHS (or one of its components).

Protections Under Proposed Rule. Under Section 29.5(d)(1)(ii) of the proposed rule, the submitted information will not be protected against disclosure until “... the CII Program Manager acknowledges and validates the information as ‘Protected CII’ and authorizes the agency or component to mark the information as ‘Protected CII.’”¹³ This provision leaves a question concerning how the information is to be treated prior to its official acceptance and designation as “Protected.” This ambiguous status raises potential issues regarding, for example, the availability of the FOIA exemption and a CII recipient’s protection against civil suit. The availability of these protections under the Rule—a FOIA exemption and indemnity from suit—during internal government processing of information and during the procedures for validation of the request for Protected CII status should be clearly stated.

Lockheed Martin notes that the proposed rule may be seeking to address the issue of protection pending a determination on eligibility for protection by providing a separate mandate under Section 29.5(d)(2) that “[t]he Federal agency or DHS component forwarding the information to the CII Program Manager may not disseminate, distribute, or make public the information until the CII Program Manager has notified the agency or component that the Program Manager has acknowledged and validated the information,”¹⁴ but if the agency or DHS component does not forward the information, this provision appears not to apply. The ambiguity on protection of information pending validation of its protected CII status also appears to be partially addressed by the presumption of protection under Section 29.6(b).¹⁵ Nevertheless, given the lack of uniformity among the various relevant provisions, it would appear that Section 29.5(c) either should be revised or omitted and that the availability of protection under the proposed rule during internal processing and the procedures for validation should be explicitly stated.

Section 29.3(e) of the proposed rule specifies that it creates no private right of action for any person or entity.¹⁶ Similarly, Section 29.8(i) of the proposed rule provides that Protected CII cannot be used in any civil action arising under Federal or State law, if such information is submitted in good

¹³ Making the CII Program Manager the point of contact for initial CII submissions reflects that DHS intends to have a single point of contact serve as the CII Program Manager. NPRM at 18527, Proposed Rule at Section 29.5(d)(1)(ii), 6 CFR 29.5(d)(1)(ii).

¹⁴ NPRM at 18527, Proposed Rule at Section 29.5(d)(2), 6 CFR 29.5(d)(2).

¹⁵ NPRM at 18527, Proposed Rule at Section 29.6(b), 6 CFR 29.6(b), providing:

(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.

¹⁶ NPRM at 18526, Proposed Rule at Section 29.3(e), 6 CFR 29.3(e). Section 215 of the Homeland Security Act provides, “Nothing in this subtitle may be construed to create a private right of action for enforcement of any provision of this Act.”

faith for homeland security purposes.¹⁷ Together, these rule sections afford submitters of CII certain protections against adverse action resulting from the submission of CII. This will encourage submissions to DHS; however, these protections do not appear to be available if the submitted information fails to qualify as “Protected CII,” even if the submitter fully expected the information would qualify as CII and submitted it in reliance on that assumption. This result would be inconsistent with the Act, which provides that “critical infrastructure information ... that is voluntarily submitted to a covered Federal agency ... shall not, without the written consent of the person or entity submitting such information, be used directly by such agency, any other Federal, State, or local authority, or any third party, in any civil action arising under Federal or State law if such information is submitted in good faith.”¹⁸ By narrowing the scope of Section 214 of the Act, the proposed rule may have the unintended consequences of deterring some from voluntarily submitting information that the Act is otherwise trying to encourage.

Under Section 29.7 of the proposed rule s,¹⁹ all persons, including Federal contractors, granted access to Protected CII are responsible for safeguarding all such information in their possession or control. Section 29.7(c) allows documents or material containing Protected CII to be reproduced only “to the minimum extent necessary consistent *[sic]* with the need to carry out official duties...” The term “official duties,” as used in this section, is not defined. Lockheed Martin believes the term “official duties” should be defined as including the actions of Federal contractors taken in furtherance of their contracts with the Federal government. This would be consistent with the language in proposed Section 29.8(c), which refers to a Federal contractor that is “performing services in support of the purposes of DHS.”

Section 29.7 sets forth standards for the use and storage of Protected CII, referring to storage “in a secure container, such as a locked desk or file cabinet, or in a facility where Government or Government-contact security is provided.”²⁰ The standards for the safeguarding of protected CII in section 29.7 should specify that Protected CII in all media—whether in print or electronic form—should be subjected to appropriate measures for protection.

Sharing of CII. Section 29.8 of the proposed rule s provides that the CII Program Manager can share Protected CII with employees of the Federal Government, or a State or local government, for “purposes of securing the critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or for another informational purposes related to homeland security.”²¹ No similar provision authorizes a Federal contractor, acting on behalf of the Federal government, to share Protected CII with employees of the Federal Government, or a State or local government. Lockheed Martin believes that the goal of the proposed rule—the sharing of information to reduce vulnerability to attacks—requires that Federal contractors be allowed to share CII with other federal agencies, state, and local governments. Lockheed Martin suggests, however, that Federal contractors be required to obtain the approval of the CII Program Manager or his designee on a case-by-case basis before sharing Protected CII with any third party, including any State or local government. Approval from the CII Program Manager or his designee would serve as confirmation

¹⁷ NPRM at 18529, Proposed Rule at Section 29.8(i), 6 CFR 29.8(i).

¹⁸ H.R. 5710, section 214(a)(1)(c). NPRM at 18529, Proposed Rule at Section 29.8(i), 6 CFR 29.8(i).

¹⁹ NPRM at 18527, Proposed Rule at Section 29.7, 6 CFR 29.7.

²⁰ NPRM at 18527, Proposed Rule at Section 29.7(b), 6 CFR 29.7(b).

²¹ NPRM at 18528, Proposed Rule at Section 29.8(b), 6 CFR 29.8(b).

that such sharing of Protected CII is for authorized purposes. Case-by-case approval should not, however, be required where blanket authority for further distribution is given by the submitter of the CII.

The final rule should be specific in terms of whom within a state or local governmental entity is authorized to receive information from a CII Program Manager. Lockheed Martin suggests that there be a designated official at the state and local government levels (*e.g.*, an HLS Officer) to whom Protected CII should be transmitted, as appropriate.

Section 29.8(c) of the proposed rule provides that Protected CII can be shared with a Federal contractor “after a CII Officer certifies that the contractor is performing services in support of the purposes of DHS.” It is not clear from the language of the proposed rule whether, when the CII Officer certifies that a contractor is performing services in support of the purposes of DHS, the contractor is thereby authorized to receive all manner of Protected CII from DHS or whether the CII Officer must make a certification with respect to specific CII on a case-by-case basis. Lockheed Martin suggests that the CII Officer must make a certification with respect to specific CII on a case-by-case basis.

Section 29.8(c) of the proposed rule also prohibits a contractor from sharing information with any of its “components,” employees, or other contractors or subcontractors (but not governments) without prior written approval of a CII Officer or prior written authorization from the submitter. An inability to share CII with one’s employees would be unworkable insofar as corporate contractors exist only through their various individual employees.

Lockheed Martin seeks clarification regarding whether the proposed rule contemplates that CII Officers must authorize specific employees to use CII or whether groups or types of employees can be authorized. Lockheed Martin also seeks clarification on what type of language will constitute authorization from the submitter. Clarification on this issue would be aided if the final Rule were to specify whether contractor personnel can be appointed as a “CII Officer” pursuant to Section 29.4(c), whether such a CII Officer can grant approval under Section 29.8(c), and whether—as a result—contractors can share Protected CII with their employees.

It is unclear under Section 29.8(d) whether State and local governments will be authorized to share Protected CII with Federal contractors acting on behalf of the Federal government without the submitter authorizing the State and local governments in writing. Section 29.8(d)(1) provides that States and local governments cannot disclose Protected CII to “any other party” without written consent from the submitter²² and Section 29.8(d)(2) provides that the CII Program Manager may not authorize States or local governments to further disclose or distribute Protected CII without written consent from the submitter;²³ however, Section 29.8(d)(3) authorizes State and local governments to use Protected CII “for the purpose of protecting critical infrastructure or protected systems....” Section 29.8(e) of the proposed rule authorizes the IAIP Directorate (but not specifically state and local governments) to “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.”

²² NPRM at 18528, Proposed Rule at Section 29.8(d)(1).

²³ NPRM at 18528, Proposed Rule at Section 29.8(d)(2)

Thus, some provisions suggest, and may require, the sharing of information with third parties, but the proposed rule also contains fairly clear mandates prohibiting the sharing of Protected CII by States and local governments, possibly even with Federal contractors that are managing/maintaining critical infrastructure assets and/or performing services in support of the Federal government within a given State. The Rule should be clarified to indicate that State and local governments may share Protected CII with Federal contractors that are managing/maintaining critical infrastructure assets and/or performing services in support of the Federal government.

Notification Provisions/Procedures. The proposed rule at Section 29.6(f) indicates that when the CII Program Manager determines that information has not been submitted in good faith, the Program Manager is not required to notify the submitter that the information will not qualify as “Protected CII.”²⁴ Lockheed Martin believes it is equally as appropriate to provide notification to the submitter under these circumstances as it is to provide it under Section 29.6(e) of the proposed rule. This would afford the submitter thirty (30) days to provide evidence of good faith, provide for review of that evidence by the CII Program Manager, and give the submitter the option to request either continued retention of the information by DHS or disposition under the Federal Records Act. Moreover, for risk management purposes, Lockheed Martin believes that Federal contractors receiving or given access to CII, which a submitter claims to have submitted in good faith under the final Rule, should be informed that the information was submitted by a party seeking the protections of the Rule even though the CII Program Manager determined that the information was not submitted in good faith.

Lockheed Martin believes that parties that have submitted information that the CII Program Manager subsequently deems to not qualify as protected CII,²⁵ and who are notified of this determination in accordance with the Rule,²⁶ should be given a defined period of time in which to require the return and/or destruction of all such information/material.

Lockheed Martin further supports a procedure by which a party submitting information or materials with an expectation of protection under the Rule, may request, within a stated period of time and for any reason whatsoever, the return and/or destruction of all such information/material.

Federal contractors also have a need to know when the CII Program Manager or his designee changes the status of Protected CII to non-Protected CII and removes its Protected CII markings.²⁷ The Rule should set forth the circumstances under which such a change in status can be made (*e.g.*, the submitter notifies DHS that a change is allowable). The Rule should also clarify that the “designee” of the CII Program Manager which is authorized under the Section 29.6(f) to change the status of

²⁴ NPRM at 18527, Proposed Rule at Section 29.6(f), 6 CFR 29.6(f), providing:

(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.

²⁵ NPRM at 18527, Proposed Rule at Section 29.6(e), 6 CFR 29.6(e).

²⁶ NPRM at 18527, Proposed Rule at Section 29.6(e)(i), 6 CFR 29.6(e)(i).

²⁷ NPRM at 18527, Proposed Rule at Section 29.6(g), 6 CFR 29.6(g), providing:

(g) Changing the status of CII to Non-CII. Only the CII Program Manager or the Program Manager’s designee may change the status of Protected CII to non-Protected CII and remove its Protected CII markings.

Protected CII must be a person within the IAIP Directorate. Whenever such a change is to occur, notice should be given to all contractors, and other parties with whom the CII has been shared, so that such parties will know that the information need no longer be treated as Protected CII.

Notice of the prospective change should also be given to the submitter if the status is not being changed at the submitter's request. The process for notifying the submitter should be modeled after the process set forth in Section 29.6(e) of the proposed rule, allowing the submitter thirty (30) days to provide further support for continuing protection, providing for review of that further support by the CII Program Manager, and giving the submitter the option to request either continued retention by DHS of the information after the status is changed or disposition of the information under the Federal Records Act.²⁸

Lastly, insofar as The Department of Homeland Security Advisory Council is comprised of private sector entities, some of which have competitors who may submit CII to DHS, it is important that the final Rule expressly provide that CII submitted under the Rule will not be revealed to private sector council members unless expressly authorized in writing by the submitter.

III. CONCLUSION

Lockheed Martin supports the proposed rule concerning the receipt, care, and storage of voluntarily submitted CII and asks DHS to consider clarifying the various points that have been raised above.

Respectfully submitted,

By: _____/s/ Gerald Musarra_____

Gerald Musarra, Vice President
Trade & Regulatory Affairs, Washington Operations
Lockheed Martin Corporation
1725 Jefferson Davis Highway
Crystal Square 2, Suite 403
Arlington, VA 22202
(703) 413-5970

June 16, 2003

²⁸ See the comments above regarding the need to clarify the authority for destruction under the Federal Records Act.