

Subject: [FR Doc: 03-09126];[Page 18523-18529]; Critical InfrastructureInformation;  
handling procedures

Date: Mon, 16 Jun 2003 10:32:07 -0400

From: "Mike Littlejohn" <MLittlejohn@wickwire.com>

To: "RegComments, CII" <CII.RegComments@HQ.DHS.GOV>

Attached please find the comments of Kaba Mas Corporation of Lexington, KY  
on the above-captioned proposed regulations for the Department of Homeland  
Security.

Thank you,

J. Michael Littlejohn

J. Michael Littlejohn  
Senior Counsel  
Wickwire Gavin, P.C.  
8100 Boone Blvd., Suite 700  
Vienna, VA 22182-7732

email: [mlittlejohn@wickwire.com](mailto:mlittlejohn@wickwire.com)

website: [www.wickwire.com](http://www.wickwire.com)

Phone: 703-790-8750

Fax: 703-448-1801

NOTICE: This communication may contain privileged or other confidential  
information. If you are not the intended recipient, or believe that you  
have received this communication in error, please do not print, copy,  
retransmit, disseminate, or otherwise use the information. Also, please  
indicate to the sender that you have received this email in error, and  
delete the copy you received. Thank you.

cii-comments.pdf            Name: cii-comments.pdf  
                              Type: Acrobat (application/pdf)  
                              Encoding: base64  
                              Description: cii-comments.pdf



June 16, 2003

Associate General Counsel  
General Law  
Department of Homeland Security  
Washington, DC 20528

Dear Sir or Madam:

We appreciate the opportunity to comment on the proposed rules to establish procedures for handling Critical Infrastructure Information (CII) (6 CFR Part 29). 68 Fed. Reg. 18524-18529 (April 15, 2003). Kaba Mas is an industry leading producer of safe locks. We manufacture and sell electronic locks for storage of classified material for the federal government and its contractors. In addition, we also have developed several lines of safe locks for industry, including electronic locks with audit capabilities, safe locks for retail establishments, and Automatic Teller Machine (ATM) locks. Accordingly, we hope that our expertise in security will benefit the DHS. We note that our proposed suggestions do not necessarily implicate our products, although some suggestions may.

Our overall concern is that the proposed rules for storage of CII in Section 29.7 fall well short of any industry or government standards for information of this type of sensitivity. Indeed, the regulations propose unclear and inadequate standards that will



749 W. Short Street  
Lexington KY 40508  
(859) 253-4744  
(888) 950-4715  
fax (859) 253-0310  
[www.kaba-mas.com](http://www.kaba-mas.com)

only increase the risk of inappropriate disclosure and increase DHS's cost of oversight. Thus, our recommendations are generally twofold. First, there should be a mechanism for DHS to review and characterize Protected CII for the varied levels of sensitivity that might apply. Secondly, the storage requirements proposed in Section 29.7 need to be improved and clarified so that they state clear, objective, and adequate standards for storage of Protected CII at different levels of sensitivity.

DHS Should Establish a Classification System for Protected CII To Account for Varied Levels of Sensitivity.

The CII Act and the regulations define CII as information "so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof." § 29.2(a). Within that definition, we believe that there could be varied levels of sensitivity. The DHS may decide that some of the information involves the highest levels of national security, the disclosure of which could result in real and immediate danger to the protection of the United States. In those cases, it would probably be appropriate for the DHS to classify the information at the Secret or Top Secret levels and require appropriate storage. Other information may be highly sensitive because it would involve national security and it would also be business confidential, so that the disclosure could harm the business submitter and the nation. Businesses would be concerned for their information to be protected adequately.

Likewise, Protected CII may be less sensitive. In some cases, the information may not



749 W. Short Street  
Lexington KY 40508  
(859) 253-4744  
(888) 950-4715  
fax (859) 253-0310  
[www.kaba-mas.com](http://www.kaba-mas.com)

involve confidential business information and the danger to national security may be less. In those cases, different types of security might be appropriate.

Under the proposed rule, however, there is no indication that the DHS will review Protected CII to determine and classify its level of sensitivity. Without guidance as to the nature of the sensitivity, it may be difficult for DHS handlers and state and local recipients of the Protected CII to understand how they should handle and use the information. As described below, a classification system would allow varied levels of sensitive information to be stored differently, which could reduce some costs of protection. More importantly, the classification system would ensure that highly sensitive information would be stored properly and effectively protected.

DHS Should Amend § 29.7 To Increase the Minimum Storage Requirements and to Provide for Enhanced Security for Higher Levels of Sensitivity

As we understand the purpose of the CII Act and the regulations, one of the main goals is to encourage companies to share information with the DHS that the company might otherwise not share with its competitors or the Government because it considers the information highly confidential, a trade secret, or so sensitive that its release could result in economic hardship to the company. Many companies that we deal with keep tight control over that type of information, and they usually require the limited number of employees who might have access to the information to use enhanced security products to protect it, especially after working hours. Those companies would very rarely trust the protection of that information to a typical desk drawer or file cabinet, as suggested by



749 W. Short Street  
Lexington KY 40508  
(859) 253-4744  
(888) 950-4715  
fax (859) 253-0310  
[www.kaba-mas.com](http://www.kaba-mas.com)

Section 29.7 of the regulations. Accordingly, we would expect that companies would be more willing to provide such information to the DHS if they understood that it would be protected at the same or higher level than it is protected within its own organization.

Appropriately, we would suggest that the agency require, at the least, that all confidential business information which qualifies as Protected CII be controlled by an access control product with a non-duplicable token and audit features. There are several security companies that provide these types of products, and they are relatively affordable.

We realize that there may be some information which qualifies as Protected CII which will not be as sensitive from a business perspective, even though it would have an impact on infrastructure security concerns. While we would still not recommend that this less sensitive type of information be kept in a typical file cabinet or desk drawer, we would at least recommend some enhancements to that type of storage. Indeed, a desk drawer lock is usually not as robust as other locking mechanisms. If the DHS decides, however, to allow individuals to store low-level sensitivity Protected CII in a desk drawer, the DHS should, at the least, require the desk lock to be a patented key control device that would prevent the unauthorized duplication of the keys to the desk drawer. There are several companies that manufacture such products and the cost is relatively reasonable.

Additionally, we would also recommend against allowing Protected CII, even of the lowest level of sensitivity, to be stored in a typical file cabinet. A "file cabinet" could have several meanings, and they are usually not appropriate for storing sensitive material



749 W. Short Street  
Lexington KY 40508  
(859) 253-4744  
(888) 950-4715  
fax (859) 253-0310  
[www.kaba-mas.com](http://www.kaba-mas.com)

unless they have been properly inspected and are secured with enhanced locking mechanisms. For instance, in 1992, the U.S. Army SECOM Intelligence Material Management Command discovered that file cabinets that were being used by the government and contractors to store classified (Confidential, Secret, and TopSecret) material suffered from serious vulnerabilities and neglect which jeopardized security. The Army concluded that none of the file cabinets (which were secured with a bar lock) complied with requirements to prevent surreptitious and covert entry. In tests on several file cabinets, the Army was able to "fish" documents out of the file cabinets in less than a minute without leaving a trace of evidence that the safe had been compromised. In one case, the testers "fished" a document out in 15 seconds. Furthermore, in every case, the testers were able to covertly open the file cabinets in less than 30 minutes. (*Test Report No. 40, Lock Bar Cabinets*, U.S. Army Intelligence Materiel Activity, Fort Meade, Maryland). The Army found that a large numbers of the file cabinets were missing backs or bottoms, and some had broken welds, bent locking bars, exposed screw heads, and unfastened metal keepers which could allow intruders to remove sensitive documents surreptitiously or use other methods to easily compromise the file cabinet. It stands to reason that if the Army found these issues with file cabinets that were in use by the Government and its contractors for classified information, then it is likely that the same or worse may be true of file cabinets used by states, localities and others who may be entrusted with Protected CII from the DHS. Accordingly, DHS should take steps to ensure that file cabinets, if used, are only used for the least sensitive CII, and, even then,



749 W. Short Street  
Lexington KY 40508  
(859) 253-4744  
(888) 950-4715  
fax (859) 253-0310  
[www.kaba-mas.com](http://www.kaba-mas.com)

the file cabinet should meet certain standards. The Government has set federal standards through the General Services Administration (GSA) for file cabinets which we would recommend the DHS adopt for low-level CII information.

We can also envision situations where the DHS will consider some Protected CII to be so sensitive from a national security point-of-view that it will be necessary to deem the information as classified at the Secret or TopSecret level. There is no provision in the proposed regulations that addresses the storage requirements for that type of classified information, but this issue must be addressed by DHS. In this regard, for the maximum amount of security and the least amount of oversight by DHS, the DHS should require that all classified information (Confidential, Secret, and TopSecret) must be stored in a GSA-approved security container or approved vault that is secured with a locking device meeting FF-L-2740A. (There are two companies that build the GSA-approved security container. Currently, Kaba Mas is the only company that meets the federally developed specification for the locking device.)

The GSA adopted these standards in the early 1990's for storage of classified material to replace the use of traditional mechanical combination locks and bar-lock file cabinets, both of which are highly susceptible to surreptitious attack. Laptop and handheld computer technology makes it easy to crack any mechanical lock in 15-20 minutes without detection. Accordingly, federal government security specialists developed the requirements for an electronic combination lock that prevents surreptitious entry and which is now required on GSA-approved containers. "Lock bars" cabinets are



749 W. Short Street  
Lexington KY 40508  
(859) 253-4744  
(888) 950-4715  
fax (859) 253-0310  
[www.kaba-mas.com](http://www.kaba-mas.com)

even more susceptible. A lock-bar container is nothing more than a standard file cabinet secured by a steel rod and a padlock. The lock-bars can be cracked in seconds, and, as noted above, federal government security audits have discovered that many regular file cabinets were easily compromised.

Finally, we would caution against allowing any level of Protected CII to be left in the "open" where "Government or government contract security is provided" as suggested by the proposed regulations at Section 29.7(b). First, the regulations do not clearly define the term "government contract security." Does this term mean a hired guard service? Does the term require the "security" to make regular checks of areas where Protected CII will be stored? We would recommend that DHS define this term more specifically in the final regulations. Second, however, we caution against relying solely on the "government contractor security" for protecting the information. As we have stated above, all Protected CII should be protected by an access control system with a non-duplicable token and audit features, at the least. This is a less costly and more effective approach than relying on guards and other supplemental security measures.

Again, we appreciate the chance to comment on the proposed regulations. If you have any questions regarding our comments, please do not hesitate to contact me.

Best Regards,



Carl Sideranko  
General Manager



749 W. Short Street  
Lexington KY 40508  
(859) 253-4744  
(888) 950-4715  
fax (859) 253-0310  
[www.kaba-mas.com](http://www.kaba-mas.com)