

BellSouth.txt

Subject: Comments of BellSouth Corporation

Date: Mon, 16 Jun 2003 16:27:46 -0400

From: "Possner, Karen" <Karen.Possner@bellsouth.com>

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

Duplicate

> <<BellSouth FOIA Filing.PDF>>

>

>

\*\*\*\*\*

"The information transmitted is intended only for the person or entity to which it is addressed and may contain confidential, proprietary, and/or privileged material. Any review, retransmission, dissemination or other use

of, or taking of any action in reliance upon, this information by persons or

entities other than the intended recipient is prohibited. If you received this in error, please contact the sender and delete the material from all computers."

BellSouth FOIA Filing.PDF	Name: BellSouth FOIA Filing.PDF
	Type: Acrobat (application/pdf)
	Encoding: base64
	Description: BellSouth FOIA Filing.PDF

-----

**BellSouth Corporation**  
Suite 900  
1133-21st Street, NW  
Washington, DC 20036-3351

202 463 4100  
Fax 202 463 4197

www.bellsouth.com

June 16, 2003

Associate General Counsel (General Law)  
Department of Homeland Security  
Washington, D.C. 20528

*Re: Notice of Proposed Rulemaking – Procedures for Handling Critical  
Infrastructure Information, 6 CFR Part 29*

Dear Sir or Madam:

BellSouth Corporation submits these comments in response to the Department of Homeland Security (DHS) Notice of Proposed Rulemaking issued on April 15, 2003 (68 Fed. Reg. 18524-29) to implement Section 214 of the Homeland Security Act of 2002 (HSA), regarding the receipt, care and storage of critical infrastructure information (CII) voluntarily submitted to the federal government.

BellSouth is a well known and major provider of telecommunications services and, as such, owns and operates networks and systems which comprise a portion of the nation's critical infrastructure, as that term is defined and utilized in the HSA. It is well recognized that at least 80 percent of the nation's critical infrastructure is owned and operated by the private sector. BellSouth has been very supportive of federal government and private sector initiatives to mutually cooperate in national security and emergency preparedness matters. BellSouth has long advocated that appropriate incentives and protections must exist in order to foster mutual private sector and governmental efforts to protect the nation's critical infrastructure and to reduce the nation's vulnerability to acts of terrorism.

There are a number of areas where the proposed regulations either exceed the authority of DHS or require clarification with regard to the handling of CII as set forth in the HSA:

1. Proposed Section 29.1, Purpose and Scope, must be amended to comply with the requirements of the HSA. Proposed Section 29.1(a)(4) would permit the sharing of CII with foreign governments. Nowhere in the HSA is such authority granted to DHS. DHS clearly has the authority to issue notices, warnings, and advisories as recognized in proposed Section 29.1(a)(5), but its authority would appear to be limited to homeland (domestic) security and the prevention of terrorist attacks within the United States, and the sharing of CII with foreign

governments is not provided for in the statute. “Express agreements” to share CII with foreign governments, which purportedly are provided for in Section 29.1(b) also appear to be beyond the scope of DHS authority. These sections of the proposed regulations should be deleted. Should it be determined that DHS in fact has the authority to share CII with foreign governments, BellSouth suggests that the authority be exercised by the Secretary of DHS.

2. Proposed Section 29.5 purports to set forth the authority of DHS to receive CII. Subsection (b)(1) appears to provide that CII shall be protected if it is submitted directly to DHS or indirectly to DHS by submitting it to any federal agency with the express direction to forward the information to DHS. In order to avoid any question of the FOIA status of CII submitted to another entity within the federal government prior to its transmission to DHS, the regulations should clarify that CII submitted indirectly to DHS shall be transmitted immediately (or, for example, within ten (10) days) to DHS by the federal agency originally receiving it, and no copy of the CII shall be retained by the federal agency originally receiving the CII. This clarification would help eliminate any question of the FOIA status of CII submitted to another entity within the federal government, but not yet received, and acknowledged and validated as protected CII by the DHS IAIP directorate. DHS should also clarify in Subsection (d)(2) that the federal agency or DHS component receiving CII which is properly marked by its submitter may not make public such information after the information has been acknowledged and validated. The proposed regulation should make clear that such submitted information may not be made public at any time. Rather, such information may be utilized as a basis for notices and warnings, in accordance with proposed Section 29.1(a)(5) and 29.8(e), so long as the information disclosed does not include the source of the voluntarily submitted CII, information that is proprietary or business sensitive, relates specifically to the submitting person or entity, or is otherwise not appropriately in the public domain.

3. Proposed Section 29.6, should be amended to provide for the return of CII to the submitter of the information should the validation process determine that the information submitted is not protected CII or if it is determined that the information has not been submitted in “good faith.” Such an amendment is necessary in order to conform with the intent of Section 214 of HSA, which is to provide incentives to entities with direct knowledge of the security of critical infrastructure to voluntarily share such information with the expectation that such information will be protected from public disclosure. When CII is shared with the federal government with the expectation that it will be exempt from disclosure under FOIA, it is only fair and appropriate that if such information is later determined not to qualify for protection from disclosure it should be returned to the submitter. Since such information is presumed to be afforded the protection from disclosure under FOIA, a later determination that information was not submitted in “good faith” and return of the information causes no harm to the public interest and helps preserve the incentive for entities to voluntarily share CII with the federal government. Thus, it should be returned to the submitter. At a minimum, the submitter should be notified that its voluntarily shared information has been determined not to qualify as protected CII or has been determined not to have been submitted in “good faith.” Such notice will provide the opportunity for the submitter to clarify the nature of the information and resolve any misunderstanding concerning its status. Finally, a thirty (30) day period for validation should be sufficient for the review of voluntarily submitted information to verify its status as protected CII, and should be made a part of proposed Section 29.6(e). A reasonable time period is required in order to ensure

the prompt review of submitted information and to provide assurance to the submitter concerning the protected status of the information.

4. Proposed Section 29.8(b) should be reinforced to articulate the responsibilities of state and local government personnel who are provided access to protected CII pursuant to an “express agreement.” Section 214(a)(1)(E) of the HSA clearly states that CII, if provided to state or local government entities, is not subject to state or local law requiring disclosure of information or records, may not be otherwise disclosed or distributed without the written consent of the submitter, and may be used only for critical infrastructure protection, criminal investigation, or criminal prosecution purposes. These requirements of the law should be reinforced in the “express agreement” contemplated in proposed Section 29.8(b) and will, again, provide assurance to a submitter of protected CII that its information will not be disclosed improperly.

5. Proposed Section 29.8(c) should be amended to deny or severely restrict access to CII by federal contractors. Section 214(f) of the HSA and proposed Section 29.9(d) both provide for criminal penalties and administrative sanctions to officers or employees of the federal government who improperly utilize or disclose CII which is protected from disclosure by the HSA. Such penalties and administrative sanctions obviously are intended to deter unauthorized use of CII and to provide some assurance to entities that voluntarily submit CII to the federal government that such information will be protected. Under the proposed procedures, these criminal penalties and administrative sanctions do not appear to apply to federal contractors, their components and employees. Therefore, federal contractors, their components and employees should be denied access to CII unless the submitter of the CII consents in writing to permit such access. Should it be determined that such information may be provided to federal contractors, the employees of the contractors should possess security clearances which are comparable to those of the federal employees with access to the information.

6. Proposed Section 29.8(g), which concerns responses to requests made under FOIA or state/local information access laws, appears to anticipate CII being made available to contractors of state or local government agencies and entities. Such disclosure and availability does not appear to be permitted by Section 214 of the HSA. Thus, the proposed procedures should require that written permission from the submitter of the CII must be obtained prior to disclosing voluntarily submitted CII to persons or entities outside the governmental entities specifically set forth in the HSA and for the purposes stated therein.

In sum, the proposed procedures for handling critical infrastructure information should be amended or clarified as set forth above in order to protect such information from improper disclosure. Only if the HSA can demonstrate to the entities which operate the nation’s critical infrastructure that information concerning their facilities and protected systems will be reasonably protected and utilized for the protection of the nation’s critical infrastructure, will such entities voluntarily share CII with the Department of Homeland Security. Section 214 of the HSA sets forth an appropriate exemption from disclosure under the Freedom of Information Act for CII as well as provides for the written consent of the person or entity submitting such information in order for the information to be utilized for other purposes. BellSouth respectfully requests that the Department of Homeland Security adopt procedures for handling critical

infrastructure information which are consistent with Section 214 of the Homeland Security Act of 2002 and which will provide the incentives and protections necessary for CII to be voluntarily provided to the federal government.

Respectfully submitted,

A handwritten signature in blue ink, appearing to read "Karen B. Possner", with a long horizontal flourish extending to the right.

Karen B. Possner  
Vice President  
National Security and Strategic Policy