

National Security Archive.txt

---

Subject: Comments on Proposed Procedures For Handling Critical Infrastructure Information

Date: Mon, 16 Jun 2003 17:28:53 -0400

From: "Meredith Fuchs" <mfuchs@gwu.edu>

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

Attached please find the comments of the National Security Archive on the Department of Homeland Security Proposed Procedures for Handling Critical Infrastructure Information.

A hard copy is following by regular mail. Please let me know if you have any trouble opening this WORD document.

Meredith Fuchs, General Counsel

National Security Archive

George Washington University

Gelman Library Suite 701

2130 H Street, NW

Washington, DC 20037

Tel: 202-994-7000

Fax: 202-994-7005

E-mail: mfuchs@gwu.edu

Visit our website at: [www.NSArchive.org](http://www.NSArchive.org)

FINAL COMMENTS ON DHS CII PROCEDURES.doc

Name: FINAL COMMENTS ON DHS  
CII PROCEDURES.doc  
Type: WINWORD File  
(application/msword)  
Encoding: base64  
Description: FINAL COMMENTS ON DHS  
CII PROCEDURES.doc

---

# The National Security Archive

The George Washington University  
Gelman Library, Suite 701  
2130 H Street, N.W.  
Washington, D.C. 20037

Phone: 202/994-7000  
Fax: 202/994-7005  
nsarchive@gwu.edu  
www.nsarchive.org

TO: Associate General Counsel (General Law)  
Department of Homeland Security  
Washington, DC 20528

DATE: June 16, 2003

RE: Comments of the National Security Archive on the Department of Homeland Security's  
Proposed Procedures for Handling Critical Infrastructure Information

---

## INTRODUCTION

The National Security Archive (the "Archive") submits these comments regarding the Department of Homeland Security's ("DHS" or "Department") "Proposed Procedures for Handling Critical Infrastructure Information," 68 Fed. Reg. 18,523 (April 15, 2003) ("Proposed CII Rule").

The Critical Infrastructure Information Act (the "CII Act"), a section of the Homeland Security Act, 6 U.S.C. § 631, creates a new Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, exemption (b)(3) statute for critical infrastructure information ("CII"). The new exemption restricts public access to important information about the activities and operations of the DHS and to important information held by private businesses about the security of critical infrastructure. The free flow of government information to the public has been a critical part of the democratic process. An open government allows the public to ensure that their government is adequately securing the infrastructure, wisely spending tax dollars, and acting legally or in good faith. Access to information about private industry has allowed the public to use natural market forces to demand improved business, health, and safety practices, particularly when the government is unable to respond to every threat to the public wellbeing. While Congress determined through the CII Act that cutting off access to a small amount of information held by the Federal government would encourage private business to share with the government information that it ordinarily would not provide and enhance national security, DHS's Proposed Rule unnecessarily expands the Act's restrictions on information flow without assuring comparable gains in security.

In implementing the Homeland Security Act, DHS must consider the important functions of other Federal agencies in protecting the public welfare. Whether it relates to protection of the economy, trade, the environment, public health, education, or employment opportunities, the mission of each of these other Federal agencies should be respected. A safe and secure homeland is one in which all of these important issues are balanced to ensure the overall welfare of the public. DHS's Proposed Rule unnecessarily trumps the vital role of other Federal agencies, including their role in fighting terrorism.

Moreover, to help protect national security and provide for improved homeland defense, the materials received under a CII label must be susceptible of being processed and disseminated by DHS. Here, however, instead of developing a workable program for receiving and safeguarding CII, DHS has created the incentive for private businesses to swamp the agency with information. DHS's Proposed Rule

**An Independent non-governmental research institute and library located at the George Washington University, the Archive collects and publishes declassified documents obtained through the Freedom of Information Act. Publication royalties and tax deductible contributions through The National Security Archive Fund, Inc. underwrite the Archive's Budget.**

unnecessarily defers to submitters of claimed CII as to what information will be treated as CII and provides no means of stemming bad faith by submitters.

### **INTEREST OF THE NATIONAL SECURITY ARCHIVE**

The National Security Archive is an independent, non-governmental research institute and library located at the George Washington University that collects and publishes declassified documents obtained through the FOIA concerning United States foreign policy and national security matters. The Archive also serves as a repository of declassified and released documents on a wide range of topics pertaining to the national security, foreign intelligence, and international economic policies of the United States.

As part of its mission to broaden access to the historical record, the Archive is a leading user of the FOIA. In its 18-year history, the Archive has made over 24,000 FOIA requests to over 40 government agencies. Thus, the Archive has extensive experience as an FOIA requester with agencies' implementation of the FOIA. We submit these comments to ensure that the DHS's CII procedures do not hinder the FOIA process or interfere with Congress's intent of opening government records to public scrutiny. As explained in detail below, the Department should make the following changes in its Proposed CII Rule: (1) Establish precise criteria that clearly delineate what is and is not CII, including narrowing the definition for "voluntarily submitted," adding a definition for "customarily in the public domain, and including in the definition of CII those categories of information that cannot qualify for or be submitted under the label of CII; (2) Provide for review of claimed CII and Protected CII when a FOIA request is made for those materials; and (3) narrow the proposed rule to permit the submission of claimed CII only to the DHS and not to other Federal agencies.

### **COMMENTS**

The American people look to the federal government for protection from harm beyond that threatened by terrorism – e.g., health, public safety, fraud – and the FOIA has helped advance such significant public interests.<sup>1</sup> As with the other Federal agencies, protecting the core democratic values that distinguish our society must be an essential part of the mission of the Department. The confidence of the people in their government and security will be strengthened by minimizing secrecy and enhancing the transparency of the Department's actions. As Secretary Ridge has stated:

[A]s long as we have a transparent democracy ... and a rule of law and a system of checks and balances and press that constantly probes and inquires and citizens that probe and inquire we can meet the goal of enhancing security and at the same time preserving our way of life ....

[A]t the heart of all that is preserving our rule of law that governs our activity and our relationships.<sup>2</sup>

---

<sup>1</sup> The congressional findings accompanying the 1996 Amendments to the FOIA recognize that the FOIA has "led to the disclosure of waste, fraud, abuse and wrongdoing in the Federal government" and has "led to the identification of unsafe consumer products, harmful drugs, and serious health hazards." Electronic Freedom of Information Act Amendments of 1996, Pub. L. No. 104-231, § 2(a)(1), 110 Stat. 3048 (1996) (Findings).

<sup>2</sup> Online Chat Between Secretary Ridge and MSNBC viewed on February 21, 2003 at <<http://www.dhs.gov/dhspublic/display?theme=42&content=80>>.

The Archive encourages the Department to establish its CII Procedures with these core democratic values firmly in place.

**1. The Proposed CII Rule Should Establish Precise Criteria That Clearly Delineate What Materials May Be Considered CII And Require The Submitter To Certify That It Has Been Labeled As CII In Good Faith.**

The proposed rule fails to establish clear and precise criteria to ensure that only true CII will be protected from FOIA disclosure. The proposed definition of “Critical Infrastructure Information or CII” includes “information not customarily in the public domain and related to the security of critical infrastructure or protected systems.” Proposed (Prop.) Rule 29.2(b). Substantively, CII concerns any possible attack, defense of, or risk management and recovery solutions relating to critical infrastructure. *Id.* In order to be “Protected CII,” the information must be submitted to DHS for DHS’s own use and accompanied by an express statement that it is being voluntarily submitted in expectation of Protected CII status. Prop. Rule 29.2(f). There is no provision defining what is not CII.

Rather than set forth clearly defined criteria, the proposed rule delegates responsibility to the private sector at the same time as it removes any accountability to the private sector to submit only actual CII. The proposed rules’ excessive deference to submitters – which “relies upon the discretion of the submitter,” 69 Fed. Reg. at 18524 (Background), in determining what is CII – and the absence of any penalty for mislabeling materials as CII – even when done in bad faith<sup>3</sup> – increases the risk that the vague definition of CII will be exploited by private business seeking to gain the benefits associated with labeling information CII.<sup>4</sup> It also invites arbitrary and inconsistent decision-making by the CII Program Manager who must devise criteria to determine what is and is not CII.

The Proposed CII Rule should be revised to include specific limitations on what information may and may not be labeled as CII, and to require that an officer of the private business submitting the material sign a certification that the material is submitted in good faith as CII.

**a. The Term “Voluntarily Submitted” Is Defined Too Broadly To Exclude Only Information That Is Submitted In The Exercise Of DHS’s Legal Authority.**

As noted above, the purpose of the CII Act is to encourage new submission of information to DHS that would not otherwise occur. As such, it is clear that Congress did not intend for voluntary submission to include submission of information that takes place as a result of a non-DHS agency exercising its legal authority to compel access to or submission of information, or information that otherwise is required to be submitted to a Federal agency or to satisfy a provision of law. Yet the proposed rule defines “voluntarily submitted” information as limited to information that is submitted “in the absence of DHS’s exercise of

---

<sup>3</sup> Prop. Rule § 29.6(f) affords that “[i]n 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.” Prop. Rule § 29.8(i) provides that “[p]rotected CII shall not... 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.” These sections are the Proposed CII Rules’ only disincentive to the mislabeling of information as CII.

<sup>4</sup> These benefits include the civil immunity described in Prop. Rule § 29.8(i) for information contained in Protected CII.

legal authority to compel access or submission of such information.” Prop. Rule § 29(j). While this is consistent with the statutory definition of voluntary, it conflicts with congressional intent. It also conflicts with the provision of the CII Act that purports to protect the ability of non-DHS Federal agencies to obtain CII through means other than the CII Act. Under the Rule, any CII material that may be obtained by another Federal agency under separate authority would be defined as “voluntarily submitted” and potentially fall subject to the use limitations of the CII Act. This result would undo the efforts of all non-DHS agencies to carry out their own statutory missions. DHS does not have the authority to interfere with the activities of other Federal agencies.

**b. The Lack Of Any Definition For The Term “Not Customarily In The Public Domain” Permits Too Much Discretion To The Submitters Of Claimed CII And The CII Program Manager.**

The term “not customarily in the public domain” is not defined in the proposed rules. Without a detailed explanation of what does and does not qualify as “customarily in the public domain,” the CII Program Manager can apply the clause far too arbitrarily. The Proposed CII Rule must define the phrase and/or establish clear evaluation procedures. Because Congress enacted the CII Act to encourage voluntary submissions to government of information that would not otherwise be made available to a government agency, the only reasonable interpretation of the phrase is that information not customarily in the public domain is information that the submitter would not submit to any agency or make available to the public under any circumstances unless compelled by legal authority.

**c. The Proposed Rule Should Define Certain Categories Of Information As Excluded From The Definition Of CII Under All Circumstances.**

The definition of CII should explicitly exclude a number of types of information, many of which already are described in other sections of the proposed regulation. By specifically delineating these types of information in the definition of CII, DHS will make it easier for the CII Program Manager to quickly make initial determinations of CII ineligibility in the first instance. These categories include, among others:

- Information submitted to any agency with the authority to compel access to or submission of such information;
- Information relied on by or as a basis for making licensing or permitting determinations, or during regulatory proceedings, or to obtain any benefit from the federal government;
- Information required to be submitted to any federal agency to satisfy a provision of law; or
- Any other information that any federal agency could obtain under any law, regulation or other authority.

**d. There Is No Rationale For DHS To Maintain Open-Ended Definitions Of CII And To Lodge Such Excessive Discretion In Submitters Of Claimed CII.**

DHS would disclose nothing of use to terrorists or of harm to privately competing enterprises by outlining clearer guidelines for designating CII and requiring that an officer of any private business that submits claimed CII certify that the material is submitted as CII in good faith. Rather, doing so increases public awareness of the agency’s actions and submitters’ conceptions of what is and what is not

appropriate material for submission as CII. Increased public awareness strengthens agency accountability and ensures an efficient, effective government. Increased submitter understanding allows them to submit more information with greater confidence that it will be protected and reduces the agency's workload of information wrongly marked CII that it must review and reject.

The absence of specific criteria for determining CII raises practical concerns that could be alleviated by more specific definition. A great influx of information, all of which the CII Program Manager must evaluate upon receipt, will require vast resources to process. Not only would more specific guidance on what is and what is not CII reduce the expenditure of time and money on this pursuit, but it would make the careful evaluation of each item more likely. Requiring that an officer of the private business submitting claimed CII certify that the information is submitted in good faith as CII would also provide an incentive for the private business to be selective in determining what submissions merit the CII label.

## **2. The CII Procedures Should Provide Review Of Claimed CII and Protected CII When A FOIA Request Is Made For The Materials.**

The Proposed CII Rule indicates that information submitted with the appropriate CII label "will be presumed to be treated as Protected CII from the time the information is received by a Federal agency or DHS component ... unless and until the CII Program Manager renders a final decision that the information is not Protected CII." Prop. Rule § 29.6(b). Moreover, the Proposed Rule appears to provide for one-time review of information marked CII that will take place when the material is first received by the DHS. Prop. Rule § 29.6(f). The only re-review that appears contemplated by the Proposed CII Rule is in response to a submitter's request that it be permitted to explain why materials were labeled as CII. There are no provisions that explicitly provide for subsequent review of purported CII in response to an FOIA request for the material. These provisions will create two problems: (1) delay that will cause agencies to fail to meet their FOIA obligation to respond to a FOIA request within 20 business days, see 5 U.S.C. § 552(a)(6); and (2) likelihood of refusal to search under FOIA for materials that no longer merit a CII label and should be releasable under FOIA.

### **a. The Proposed Rule Conflicts With The Statutorily Mandated Time For Agency Responses To FOIA Requests.**

Congress adopted a time limit provision in the FOIA "in order to contribute to the fuller and faster release of information, which is the basic objective of the Act." H.R. Rep. No. 876 (1974), reprinted in, 1974 U.S.C.C.A.N. 6285, 6289. One of Congress's key concerns in enacting the 1996 Amendments to the FOIA was addressing extensive delays in responding to FOIA requests. Congress amended the FOIA to include a twenty-day time limit for an agency to respond to FOIA requests "[i]n order to help Federal agencies in reducing their backlog of FOIA requests ...." H.R. Rep. No. 104-795 (1996) at 26. An agency's failure within the statutory time period to provide a response that addresses: (1) the agency's determination of whether or not to comply with the request; (2) the reasons for its decision; and (3) notice of the right of the requester to appeal to the head of the agency if the initial agency decision is adverse, is a constructive denial of the request. See Oglesby v U. S. Dep't of Army, 920 F.2d 57, 65 (D.C. Cir. 1990) (citing 5 U.S.C. § 552(a)(6)(A)(i)) (additional citations omitted). Congress provided that an FOIA requester may be deemed to have constructively exhausted administrative remedies, and entitled to file a lawsuit against the agency, if the 20-day period has passed without a substantive response to the request

or a notice advising of a one-time ten day extension of time for “unusual circumstances” from the agency. 5 U.S.C. § 552(a)(6)(C)(i); 5 U.S.C. § 552(a)(6)(B).

DHS cannot by regulation undo the statutory mandate that an agency respond to an FOIA request within 20 days of the request. See Prop. Rule 29.3(a) (the CII Act of 2002 and these procedures do not apply to or affect any requirement . . . pertaining to the obligation of any Federal agency to disclose such information under the Freedom of Information Act.”) Thus the proposed rule should provide that any materials marked CII will be reviewed pursuant to an FOIA request even if the CII Program Manager would not yet have reviewed the materials under the ordinary course of the CII Procedures.

**b. The Proposed Rule Excludes Materials That Should Be Subject to Search, Review, and Disclosure Under the FOIA.**

As to improper FOIA denial, these rules are problematic because the character of information as CII potentially changes over time. For instance, CII is limited to “information that is not customarily in the public domain.” Prop. Rule § 29.2. A number of circumstances may change over time that affects what is customarily in the public domain. Another federal agency may begin to require the submission of the same information through changes in statutory and regulatory disclosure requirements. Accordingly, DHS should make provisions for re-review of materials at appropriate times.

In particular, CII should be re-reviewed if there is a FOIA request for the records. FOIA permits disclosure of information that would not be releasable under the FOIA but for the fact that the information actually is in the public domain. See Cottone v. Reno, 193 F.3d 550, 554-55 (D.C. Cir. 1999); Afshar v. Dep’t of State, 702 F.2d 1125, 1129-31 (D.C. Cir. 1983). Similarly, FOIA requesters are granted the legal right to dispute an agency’s conclusion that a FOIA exemption applies to permit withholding of a record. See 5 U.S.C. Sec. 552(a)(6)(A)(i) (administrative appeal) and (ii) (judicial review). As written the Proposed CII Rule provides no opportunity for a FOIA requester to present the argument that information should not be granted Protected CII status, such as providing proof that it is information submitted to a non-DHS agency with the authority to compel access to such information, or information relied on in making licensing or permitting determinations, or during regulatory proceedings, or that it is information in the public domain. Moreover, the Proposed Rule applies a broad brush in protecting the entire contents of materials submitted under a CII label. Under the FOIA, by contrast, protection from release is only available to the segregable parts of a record that merit protection from disclosure.

Accordingly, DHS should, at the very least, require re-review of CII whenever an FOIA request is made for such materials, should permit an FOIA requester to present information concerning why the material does not qualify as Protected CII, and should permit release of portions of records that do not qualify as Protected CII.

**3. The Homeland Security Act Does Not Permit The DHS To Insulate From FOIA Information Provided Directly to Another Federal Agency.**

The proposed rule provides that submission of CII to DHS includes submission “via another Federal agency, which, upon receipt of the CII, will forward it to DHS.” Prop. Rule § 29.2(i); see also 29.1(b), 29.5(b)(1), 29.5(c), 29.5(d), 29.6(b). This provision is not authorized by statute and thus must be deleted in its entirety and replaced with a provision that indicates that CII protection is available only for materials submitted directly to the DHS.

**a. The Homeland Security Act Does Not Authorize The Expansion of The CII Act to Materials Submitted to a Non-DHS Agency.**

The Homeland Security Act provides:

critical infrastructure information (including the identity of the submitting person or entity) that is voluntarily submitted to a covered Federal agency for use by that agency regarding the security of critical infrastructure and protected systems, analysis, warning, interdependency study, recovery, reconstitution, or other informational purpose, when accompanied by an express statement specified in paragraph (2)--(A) shall be exempt from disclosure under section 552 of title 5, United States Code (commonly referred to as the Freedom of Information Act)

6 U.S.C. § 133.

First, the term “covered Federal Agency” is defined in the CII Act solely as “the Department of Homeland Security.” 6 U.S.C. § 131(2). Moreover, the CII Act repeatedly refers to submission solely in terms of submission to the DHS. *Id.* at § 131(3); 131(7); 133.

Second, the CII Act applies only to information that is not “customarily in the public domain.” 6 U.S.C. § 133. The rationale for this limitation is that the CII protection was granted to encourage new sharing of information with the government that would not otherwise take place without a FOIA exception. *Id.* The Proposed rules echo this purpose. 68 Fed. Reg. at 18,524 (“The Department[’s]... receipt of [critical infrastructure] information... is best encouraged through the assurance that such information... will not be disseminated to the general public). The only intent of Congress that can be inferred from the Act, therefore, is that information customarily provided to non-DHS federal agencies that is not protected from FOIA disclosure by some other pre-existing statutory limit on disclosure is non-protected information that “customarily is in the public domain.”

**b. Expanding The Homeland Security Act to Protect From FOIA Information Submitted to a non-DHS Federal Agency Undermines the Purpose of the Homeland Security Act and Conflicts With Section 133(a) of the Act.**

The Homeland Security Act specifically provides that “[n]othing in [the CII Act] shall be construed to limit or otherwise affect the ability of a State, local, or Federal Government entity, agency, or authority, or any third party, under applicable law, to obtain critical infrastructure information in a manner not covered by [6 U.S.C. § 133(a)], including any information lawfully and properly disclosed generally or broadly to the public and to use such information in any manner permitted by law.” 6 U.S.C. § 133(c). This provision prohibits the CII Procedures from interfering with the efforts of other federal agencies to obtain CII directly from private business or through other channels. Expanding the scope of the CII program to require other federal agencies to accept materials marked as CII and forward them to the DHS, will grossly interfere with the regulatory functions of the other federal agencies and render this provision ineffective.

As drafted, the proposed rules will require the CII Program Manager to manage a complex program of receiving, reviewing, and then, potentially responding to each agency with a record marked CII. In light of the challenges that will be faced by the CII Program Manager in simply identifying what

is genuine CII, this added administrative burden could threaten to swamp the office. These genuine practical and logistical challenges will be significantly amplified by expansion of the program for CII submission to non-DHS federal agencies. First, all information with CII markings will have to be reviewed by the DHS “CII Program Manager.” Thus, all materials will have to be forwarded to DHS to await review before any action can be taken. With DHS’s separate procedures requiring all mail to be analyzed and centrally reviewed, this will build in an extensive delay in the use of the records. The CII program presumes any matters a submitter marks “CII” to indeed be CII and protects these records from agency disclosure or use until the CII Program Manager says otherwise. Because the agencies are not allowed to review this information and extract any non-CII information, they are forced to sit on their hands until the Program Manager has time to review it before they can use any of it. The rules’ complete lack of time limits or deadlines for the Program Manager in rendering such a decision could endlessly prolong these delays, and a similarly unbounded submitter appeal process could render valuable information useless to agencies for periods of months or years. The rules do not allow FOIA officers to expedite review for information subject to FOIA requests or clearly marked incorrectly as CII by the submitter, and so the agencies must wait regardless of pressing circumstances. A presumption that falsely marked CII is destroyed unless the submitter objects further keeps this information out of the agencies’ hands and hinders effective regulation. Thus, empowering agencies to receive but not review CII submissions needlessly complicates the processing of CII and elongates the process of other important regulatory functions.

Moreover, in the absence of any penalty, any private business submitting CII to a non-DHS agency would label such information under the CII Act in order to ensure the maximum protection from disclosure possible. That non-DHS agency would then be constrained by the CII Procedures in its handling of the information, leading potentially to significant delay, limitations on use of the information, and, ultimately interference with its own regulatory mission. Thus, the protection afforded by Section 133(c) of the CII Act to the non-DHS agency would be ineffective.

It is a standard canon of statutory construction that every provision enacted by Congress has a purpose and that there is no language that will be treated as mere surplusage. See Duncan v. Walker, 533 U.S. 167, 174 (2001) (“If it can be prevented, no clause, sentence, or word shall be superfluous, void, or insignificant”) (quoting Market Co. v. Hoffman, 101 U.S. 112, 115 (1879)); Dunn v. Commodity Futures Trading Comm’n, 519 U.S. 465, 472 (1997) (“legislative enactments should not be construed to render their provisions “mere surplusage”). Moreover, this clearly would be inconsistent with the purpose of the CII Act, i.e. to encourage new sharing of CII that could not or would not otherwise take place without protection from disclosure.

**c. The DHS is Prohibited By Law From Expanding the Scope of the CII Act.**

Finally, the CII Act authorizes DHS to engage in only limited and strictly confined rulemaking. These limitations do not permit the expansion of the CII Act to information provided to non-DHS Federal agencies. The CII Act provides that the elements of this rulemaking specifically concern the “acknowledgment,” “maintenance,” “care and storage,” and “protection and maintenance of the confidentiality” of CII. 6 U.S.C. § 633(e)(2). They do not concern the scope of the CII program, which DHS has taken upon itself to expand. An agency has only the power that Congress grants it. DHS has exceeded its statutory powers by changing an element the Act did not permit it to change. It has altered the scope of the CII program in a way that does not rationally relate to the statute’s purpose of preserving freedom of information while securing our nation’s infrastructure. Because the expansion of the CII Act

protection to information submitted by entities to non-DHS Federal agencies is not permitted by law, it must be deleted in its entirety and replaced with a provision that indicates that CII protection is available only for materials submitted directly to the DHS.

### **CONCLUSION**

For the reasons stated above, the National Security Archive urges the Department of Homeland Security to incorporate the following changes into its Proposed CII Rule: (1) Establish precise criteria that clearly delineate what is and is not CII, including narrowing the definition for “voluntarily submitted,” adding a definition for “customarily in the public domain, and including in the definition of CII those categories of information that cannot qualify for or be submitted under the label of CII; (2) Provide for review of claimed CII when a FOIA request is made for those materials; and (3) narrow the proposed rule to permit the submission of claimed CII only to the DHS and not to other Federal agencies.

Respectfully submitted,

Meredith Fuchs, General Counsel  
The National Security Archive  
George Washington University  
Gelman Library Suite 701  
2130 H Street, NW  
Washington, DC 20037  
202-994-7000

DATED: June 16, 2003