

149787

**GAO**

United States  
General Accounting Office  
Washington, D.C. 20548

Accounting and Information  
Management Division

B-233809



149787

July 19, 1993

The Honorable Gary A. Condit  
Chairman, Information, Justice,  
Transportation and Agriculture  
Subcommittee  
Committee on Government Operations  
House of Representatives

Dear Mr. Chairman:

This letter responds to the October 30, 1992, request of the former Chairman that we review Federal Information Resources Management Regulation (FIRMR) Bulletin C-22, which provides guidance to federal agencies on the security and privacy protection of federal computer resources. Specifically, we were asked to determine whether (1) the bulletin's procedures on the disposition of sensitive automated information are adequate to prevent such incidents as the one in which a U.S. Attorney's Office in Lexington, Kentucky, sold surplus computer equipment later found to contain highly sensitive information; and (2) the General Services Administration (GSA) sought input from staff who worked on the investigation of the Kentucky matter while developing the bulletin. In a discussion with your office, staff expressed your interest in obtaining the results of our review.

To address our objectives, we reviewed Bulletin C-22 and interviewed GSA officials responsible for issuing this guidance. We also interviewed officials from the National Institute of Standards and Technology (NIST) who developed the sections of the bulletin on the disposition of sensitive information, and reviewed other NIST guidance and information on this subject. We also reviewed National Security Agency (NSA) guidance on the disposition of sensitive and classified automated information.

RESTRICTED--Not to be released outside the  
General Accounting Office unless specifically  
approved by the Office of Congressional  
Relations.

**RELEASED**

GAO/AIMD-93-7R, GSA's Computer Security Guidance

557651

RESULTS IN BRIEF

GSA's Bulletin C-22 is not adequate to address the problems that gave rise to the incident in Lexington, Kentucky. This guidance is intended for general use by federal agencies and does not consider the types of sensitive information--for example, the names of federal agents--disclosure of which could jeopardize lives or have other serious effects. As a result, the guidance does not adequately address all methods available for removing highly sensitive information from computers. While drafting the bulletin, a GSA official involved in developing the guidance obtained information from Justice and GAO personnel knowledgeable about the Kentucky incident. GSA, however, did not share drafts of the bulletin with Justice and GAO staff for comment because, according to GSA officials, it is not their normal procedure to coordinate with other agencies.

BACKGROUND

The proper disposition of sensitive automated information is often overlooked. Even when a computer file is deleted or erased, the data remain on the computer's hard disk drive, floppy disk, or memory until overwritten. It is a simple matter to restore a deleted or erased file; in fact, many software utility programs have been designed for just this purpose. As a result, it is important to properly remove such information from the computer before releasing any such equipment for reuse, sale, or maintenance.

The importance of this issue was demonstrated in 1990 when the U.S. Attorney's Office in Lexington, Kentucky, sold surplus computer equipment that was later found to contain sensitive information, such as the names of federal agents and witnesses. Although Justice officials recognized the need to remove this information, they did not use proper methods to do so. As a result of this incident, as well as several congressional and GAO inquiries into computer security at the Department of Justice, the Office of Management and Budget (OMB) requested that GSA and NIST develop guidance to address this issue governmentwide. In September 1992 GSA, with help from NIST, issued Bulletin C-22.

GUIDANCE DOES NOT ADDRESS  
HIGHLY SENSITIVE INFORMATION

Bulletin C-22 does not recognize the many types of sensitive information in existence, ranging from the less threatening (individuals' social security numbers) to the life-threatening (names of federal agents). According to NIST officials who developed the guidance, GSA instructed them to write the policy for general use in the government.

However, NIST's own advisory material to agencies contains a much more extensive discussion of sensitive information.<sup>1</sup> This material advises agencies to take a risk-based approach to protecting information by analyzing both (1) what harm may result if information is inadequately protected and (2) the cost of protective measures. NIST officials said its material was more explicit than the GSA bulletin because NIST wrote the bulletin for information having low sensitivity, which they perceive as the majority of sensitive data residing in federal government systems. Further, the NIST advisory material was written after the bulletin and was intended to provide an in-depth discussion of sensitive information.

GUIDANCE DOES NOT DESCRIBE  
ALL AVAILABLE DISPOSITION  
ALTERNATIVES

Bulletin C-22 also fails to adequately address the various methods of disposition that may be appropriate, depending on the sensitivity of the information. For example, while the bulletin recommends overwriting sensitive data with non-sensitive data, it only describes a simplistic process in which a series of "0s" are used to overwrite the data. The bulletin does not discuss other overwriting methods, such as using a pattern of "0s" and "1s," then its opposite, and finally another pattern, which make retrieval of sensitive data from data remanence more difficult.<sup>2</sup> Such a sophisticated method

---

<sup>1</sup> CSL (Computer Systems Laboratory) Bulletin, November 1992.

<sup>2</sup> Data remanence is the residual physical representation of data that can remain on storage media even after the data have been erased. Such residual representation can allow the data to be reconstructed.

may be more appropriate for some highly sensitive data. Further, while the bulletin mentions degaussing (demagnetizing magnetic storage media, such as tapes and disks, to erase them) using approved equipment, it does not describe circumstances in which degaussing is recommended, define approved equipment, discuss how to use it, specify what training is required, or describe how to test to determine whether the procedure was effective. Finally, the guidance does not identify destruction of the magnetic media as an alternative.

The NIST advisory material, as well as NSA guidance on the secure handling of sensitive or classified automated information, provides more of this information on disposition alternatives.<sup>3</sup> The NSA guidance, which is referenced in the NIST material, provides even more extensive information on the alternatives for disposition, including those recommended for different storage media and the risks associated with using different alternatives.

A GSA official involved in developing the bulletin explained that while it was being drafted, he obtained information from Justice and GAO staff familiar with the Kentucky incident. GSA officials stated, however, that they did not share a draft of the bulletin with these agencies for comment because it is not their normal procedure to do so.

#### CONCLUSIONS AND RECOMMENDATIONS

While C-22 may address the disposition of most sensitive federal information, this guidance is not adequate to prevent the type of incident that occurred in Lexington, Kentucky. As a result, the government is subject to the risk of other such occurrences and the potential compromise of sensitive data--some of which, if disclosed, could jeopardize lives. While Bulletin C-22 represents a good first step, more complete information is needed.

---

<sup>3</sup> CSL (Computer Systems Laboratory) Bulletin, October 1992; and National Computer Security Center, A Guide to Understanding Data Remanence in Automated Information Systems, NCSC-TG-025, Version 2; September 1991.

B-233809

Therefore, we recommend that the Administrator of General Services and the Secretary of Commerce revise Bulletin C-22 by

- incorporating into it information already published in NIST advisory material concerning the sensitivity of information and various appropriate methods of disposition, and
- clearly stating that NSA guidance on the secure handling of sensitive or classified information provides disposition alternatives that may be appropriate, depending on the sensitivity of the data involved.

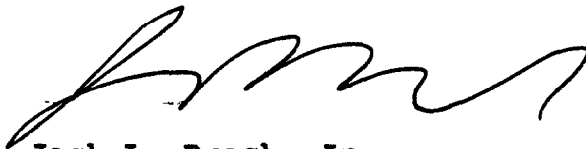
- - - - -

In accordance with your wishes, we did not obtain written agency comments on a draft of this letter. However, we discussed its contents with GSA and NIST officials, who generally agreed with the facts as presented. Further, these officials agreed to make the necessary revisions to the bulletin or develop separate guidance to address our recommendations. We have incorporated their other comments where appropriate. We conducted our work from December 1992 through July 1993, in accordance with generally accepted government auditing standards.

As agreed with your office, unless you publicly announce the contents of this letter earlier, we plan no further distribution until 30 days from the date of this letter. We will then give copies to other interested parties. Copies will also be made available to others upon request.

Please contact me at (202) 512-6406 or Linda D. Koontz, Assistant Director, at (202) 512-7487, if you have any questions about this report.

Sincerely yours,



Jack L. Brock, Jr.  
Director, Information Resources  
Management Core Group

(510913)