UNITED STATES
NUCLEAR REGULATORY COMMISSION

ANNOUNCEMENT NO. 179

DATE: November 20, 1986

TO: All Employees

SUBJECT: PROTECTION OF SENSITIVE UNCLASSIFIED DOCUMENTS

Reference: Manual Chapter 2301, "Systems Security," Appendix Part I, "Word Processing Security"

Recently, unauthorized access was gained to sensitive unclassified information which was created on the 5520 shared logic word processing system. Although no extensive, permanent damage resulted from this action, the consequences of unauthorized access to, and misuse of, sensitive unclassified information can be severe and far-reaching. Sensitive unclassified data must be safeguarded at all times during its preparation, communication, and use.

The purpose of this memorandum is to remind all employees of their responsibility for safeguarding sensitive unclassified information and the administrative procedures which have been developed to ensure that this responsibility is carried out.

In addition, each 5520 user has an individual responsibility for the security of material created, stored, printed, or communicated by the system. This includes operation of the system in a manner which shall protect it from unauthorized access, and shall protect its contents and products from being viewed by unauthorized persons.

Administrative procedures described in the referenced document detail the precautions which shall be taken by users of the 5520 shared logic word processing systems. The relevant pages from NRC Appendix 2301, Part I.D, are attached. Every employee should become familiar with these procedures.

If you have questions or need assistance in following these procedures, contact your 5520 System Coordinator or System Security Officer.

William G. McDonald
Deputy Executive Director
for Operations/IRM

Attachment:
As stated

h. Sensitive data will not be telecommunicated to non-NRC activities without the approval of SEC. Exceptions may be made during an emergency situation. At no time is SGI or 10 CFR Part 21 health and safety related allegations, where confidentiality is requested, to be telecommunicated between systems unless approved, in writing, by SEC.

i. Such system components as terminals, printers, and video display units will be physically located to preclude an unauthorized person from viewing the display or printed output.

j. Properly mark and prevent unauthorized viewing of the output as it comes off the printer by arranging the system so that unauthorized personnel cannot see it.

k. Back up important diskettes on a routine basis.

l. The system shall be used for official business only.

m. Confidentiality of proprietary software must be maintained. Copies of licensed software shall not be made without the prior approval of the vendor.

D. SECURITY REQUIREMENTS OF SHARED LOGIC SYSTEMS

1. Classified Data. Shared logic systems will not be used to process or store classified data without the written approval, guidance and authorization of SEC.

2. Sensitive Data.

a. The Systems Security Officer. Each Director of a Headquarters Office and each Regional Administrator must appoint a Systems Security Officer (SSO) for each shared logic system (central unit) owned/managed by their offices and notify SEC and RM/D, in writing, of said appointment. The SSO for each system shall:

(1) authorizes personnel use, assures the day-to-day security of the system, issues local addresses for shared logic systems, implements Security Operator responsibilities for IBM 5520 Systems, (see IBM publication "IBM 5520 Administrative System-System Operations Self Study") and issues, controls and changes operator passwords within the system.

(2) interfaces with the Shared Logic Systems Security Manager (see NRC Chapter 2301, Section 033.a.) and administers the appropriate security instructions contained in the User's Manual. The Systems Coordinator, required by RM/D, may serve as the SSO if desired.

b. Access Security. Only personnel authorized by the SSO will be permitted access to and use of shared logic System Display Stations, Central Processing Units (CPUs), and other components.

c. Physical Security. The shared logic system central processing unit should only be located in offices which can be secured by locks when unoccupied.

These locks shall be approved by SEC and not keyed to the building master system. Procedures to exempt offices whose systems are located in areas that cannot be easily locked will be developed on a case-by-case basis. For example, as an alternative solution, such systems should implement the optional CPU KEYLOCK feature instead of a power switch to control the power. In buildings not protected by guard service, doors will be equipped with perimeter alarms (e.g., alarms on doors or windows) approved by SEC. Magnetic storage media and shared logic system document log books and paper products containing sensitive data will be secured in approved containers, in accordance with the procedures contained in NRC Appendix 2101, Parts IV, XVI, and XVII. These media and documents will be erased, degaussed, or destroyed when obsolete, as required in paragraph d., below.

Communications equipment, including keying material and Data Encryption Standard (DES) cryptographic equipment, authorized for use in a shared logic system, shall be installed in the same room as the CPU or in a similar approved locked area. Keying material shall be stored at the same level of protection required for SGI (see NRC Appendix 2101, Part XVII).

d. Telecommunications Security. All telecommunications between NRC owned shared logic word processing system nodes, which involve communications outside the Washington metropolitan area (e.g., Headquarters to Region, Region to Headquarters, and Region to Region) will be encrypted with DES equipment approved by SEC. Once encryption capability is installed, all transmissions (except those to/from local, hard-wired Display Stations) between such systems will be encrypted. In the event of a temporary loss of the ability to establish or maintain encrypted communications due to encryption equipment failure or similar operational difficulties, communications may be reestablished for unencrypted transmission of non-sensitive information only.

Sensitive data will not be telecommunicated to non-NRC activities without the approval of SEC. Exception to these procedures may be made during an emergency situation. At no time is SGI or 10 CFR Part 21 health and safety related allegations, where confidentiality is requested, to be telecommunicated to non-NRC activities or between the NRC owned shared logic word processing system nodes described above without encryption being in effect.

Cryptographic keys will be changed at least quarterly in accordance with procedures prescribed by the Chief, Telecommunications Branch, FOS.

e. Security of Obsolete Media and Documents. When it is determined that magnetic media (e.g., diskettes) containing sensitive data are no longer needed for the storage of sensitive data, they may be reused after being sanitized by initializing or overwriting, degaussed by permanent magnets or other equipment approved by SEC. Paper documents shall be destroyed in accordance with procedures contained in NRC Appendix 2101.

Internal memory components and hard disks which contain information and must be removed from the CPU operating area shall be handled in accordance with instructions obtained from SEC.

f. Administrative Security. The following administrative controls shall be implemented, especially when processing sensitive data:

(1) Establish a diskette(s) specifically for sensitive data.

(2) Mark the storage diskette(s) with the Official Use Only (OUO), Proprietary Information, Limited Official Use (LOU), or Unclassified Safeguards Information (SGI) marking, depending on which category or type of data stored on the diskette requires the most restrictive handling and access controls.

(3) Diskettes containing sensitive data must be placed in sleeves with the wording, "This diskette contains SENSITIVE UNCLASSIFIED," printed on the outside. These sleeves, in the 8" and the 5-1/4" size, are available from the NRC Warehouse.

(4) Secure the diskette(s) containing this information in locked files, cabinets, or desks, as appropriate for the type of information involved (see NRC Appendix 2101, Parts IV, XVI and XVII), when they are not in use.

(5) Mark ribbons in accordance with the requirements for the category or type of information (as in e.(2) above) they were used to produce. Unless they are multi-strike ribbons, remove them from the machine at night. Properly store them in a key locked or combination locked cabinet. Dispose of them in a classified waste container, if available, or in accordance with procedures contained in NRC Appendix 2101.

(6) Do not leave diskettes containing sensitive data in the system upon completing processing sensitive data.

(7) Assure that such system components as terminals, printers, and video display units are physically located to preclude an unauthorized person from viewing the display or printed output.

(8) Properly mark and prevent unauthorized viewing of the printed output as it comes off the printer by arranging the system so that an unauthorized person cannot see it.

g. System Specific Security. The security requirements of specific NRC shared logic systems (i.e., IBM 5520 Word Processing Systems) follow.

(1) Personnel Security. Only personnel authorized by the SSO will be permitted access to and use of shared logic System Display Stations, CPUs, and other components by having an operator profile created for each person authorized access.

(2) Systems Security. The IBM 5520 system provides means to restrict system access and usage, as well as to protect sensitive data residing in the system. There are three types of security controls available:

- System Security controls access to the system.

- Document Security controls who can access a document.

- Operator Authority Levels control access to system menus and tasks

All three types of security controls will be implemented at each NRC IBM 5520 installation. Specifically, the following procedures will be used to implement the above controls and are required within each system:

(a) Operator Access

All operator access to the system will be restricted in two ways: operator name and password. In order to sign on to the system, every operator is required to enter an operator name which the system will use to verify the operator's authorization to use the system. In addition to the operator name, which the system requires of users, each operator will be issued a unique operator password by the SSO. Passwords shall be changed at least every six months or whenever a system compromise is reasonably suspected. The Operator profile, which includes the operator password, will be deleted from the system whenever the owner of the profile no longer needs access to the system. Passwords will be at least four characters long and may be up to eight alphanumeric characters long, will not be the same as the operator's name, and will not be initials, birthdates or any other obvious combinations of characters. Operator passwords should only be used by the persons to whom they are issued. The use of another's password to access the IBM 5520 is prohibited to both unauthorized persons and authorized persons having their own operator passwords unless permission has been granted by the password owner and/or the SSO. If, with the approval of the SSO or alternate, a password is shared for operational or emergency purposes, the password should be changed as soon as possible.

With the exception of the NRC CRESS Branch, no more than two operators, per working shift, should be identified as Lead Operator and possess system operator functions. The Lead Operators are authorized to enroll other operators in the system, create, change and delete profiles and coordinate the operations of the system on a daily basis. If so desired, this function may be restricted to the Supervisor of the Word Processing Center. The SSO shall be the individual assigned Security Operator responsibility. This gives the SSO the ability to use the Show Password menu to display the password of any enrolled operator.

The use of the Customer Engineer Operator Level will be limited by the SSO to those representatives authorized by RM/D to maintain and service the system.

(b) Node Access

Each system (node) in an IBM 5520 document distribution network shall be assigned a unique node name or node address as well as a node password.

The node name and password restrict access to the various distribution systems nodes. (Note: Node passwords are resident in the system and are not used by operators when messages are sent. The system automatically uses the password. Operators would need to know node passwords in order to look at distribution queues or to delete jobs in the queue.)

Each IBM 5520 node shall be assigned a unique security identification. An identification shall be defined within each node to indicate which nodes are authorized access to other nodes in the network via telecommunications. Unauthorized systems are automatically disconnected from the telecommunications connection and their users thereby prevented from unauthorized access. (This is a software feature which is transparent to the operator.)

(c) Document Access

Document security limits access to certain documents in storage and documents being distributed to other locations.

When a document is created, the operator can assign a security designation (Private, Shared Read, Shared Revise) to it. This designation is used by the system to limit who has access to and ownership of each document in the system. There are three classes of documents.

- Private--only the owning operator can use or change the document.
- Shared Read--any operator can read, but only the owner can change the document.
- Shared Revise--any operator can read or change the document.

An addition to the above Private, Shared Read, and Shared Revise access options to restrict access to shared documents is provided by the USER ACCESS LISTS option. User Access Lists are not associated with documents; they are associated with document owners. User Access Lists allow operators in a department or group to jointly access Shared Read and Shared Revise documents, while preventing others outside the group from having access. SEC strongly recommends that offices implement this feature, especially in situations where multiple offices share the resources of the same Central Processing Unit. When User Access Lists are not active, <u>all</u> text operators can access Shared Read and Shared Revise documents.

Whenever possible, a document containing sensitive data will be designated as a "Private" document if it is being distributed. Documents containing Unclassified Safeguards Information will always be designated as a "Private" document.

An additional distribution security feature is provided to control authorization to receive a personal document transmitted using the IBM 5520 document distribution facility. The sender of a document can specify that the receiver must enter a personal document password before a document can be delivered. The document then can only be obtained by the intended individual using the personal document password. The password must have been entered into the recipient profile prior to any intended distribution. This feature should be used when transmitting documents containing sensitive data which is intended for one particular addressee.

All passwords of all access levels are designated at least "OFFICIAL USE ONLY" and shall be protected accordingly. Passwords used in relation to the processing of Safeguards Information must be designated "Safeguards Information (SGI)."

All operator passwords shall be changed every six months.

(d) Security of Display Stations

Use of Display Stations to access the IBM 5520 system shall be authorized by the SSO only to specific authorized personnel. Display Stations located in offices not continuously occupied by NRC employees must be logged off when not in use or when unattended. No Display Station shall be left unattended overnight in a logged on condition; they shall be logged out and shut off.

(3) Security of Obsolete Media and Documents

When it is determined that magnetic media containing sensitive data are no longer needed to store sensitive data, they shall be sanitized by initializing or overwriting, degaussed by permanent magnets or other equipment approved by SEC. Paper documents shall be destroyed in accordance with authorized procedures. IBM 5520 system diskettes are to be erased by using the Diskette Initialization Procedures as described in "IBM 5520 Administrative System, System Operation Self-Study," Section 3. This procedure completely erases the diskette.

Diskettes will be stored as required in Section D.2.e. of Part I of this Appendix, and disposed of only in accordance with procedures approved for sensitive data or SGI, depending on the highest level of information which is stored on them. Diskettes can be reused for "normal" or sensitive work after they have been erased by initializing. Internal memory components and hard disks, which contain information and must be removed from CPU operating areas, shall be handled in accordance with instructions obtained from SEC.