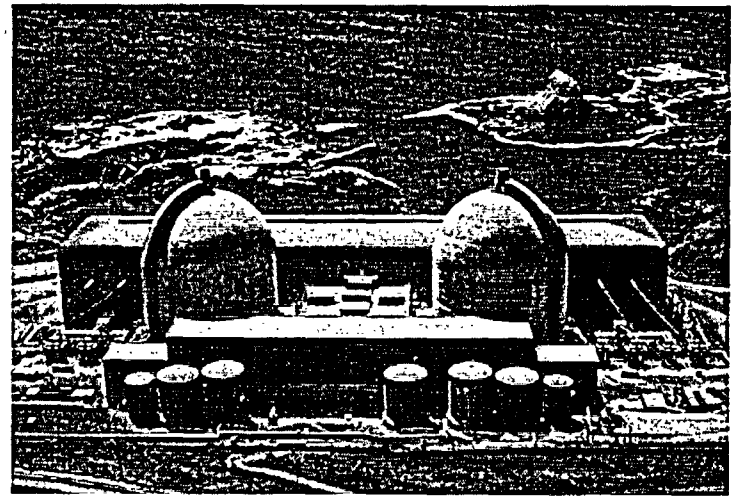
Safeguards Information



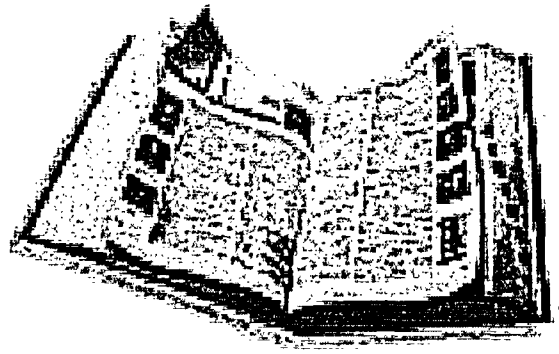
Bern Stapleton
U.S. Nuclear Regulatory Commission

C-15

Atomic Energy Act

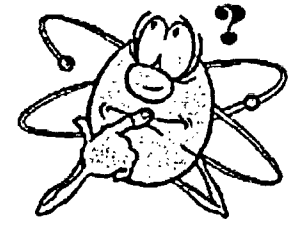
- Describes Safeguards Information as a special category of sensitive unclassified information authorized by Section 147 of the Atomic Energy Act, of 1954, as amended to be protected

Definition



- Safeguards Information specifically identifies a licensee's detailed, 1) security measures for the physical protection of special nuclear material, or 2) security measures for the physical protection and location of certain plant equipment vital to the safety of NRC licensed facilities

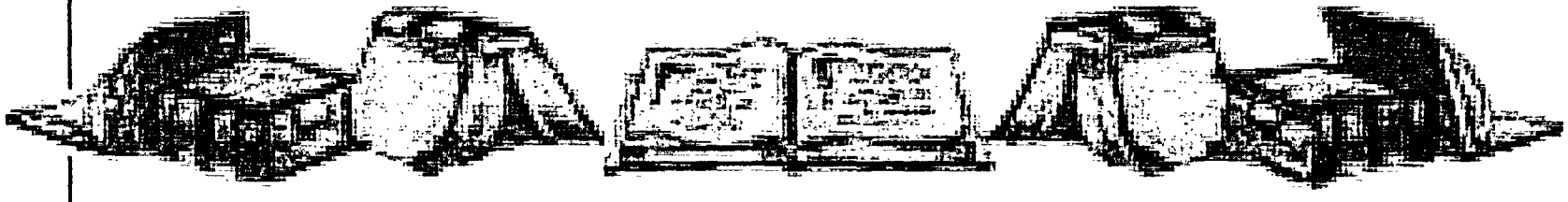
Why so Important?



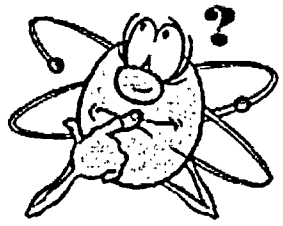
- Information the disclosure of which, could reasonably be expected to have a significant adverse effect on the health and safety of the public or the common defense and security by significantly increasing the likelihood of theft, diversion, or sabotage of materials or facilities subject to NRC jurisdiction

NRC Requirements

- The criteria for designating special nuclear material and power reactor information as Safeguards Information and associated restrictions on access to and protection of Safeguards Information are codified in Section 73.21 of Title 10 of the *Code of Federal Regulations* (10 CFR 73.21)



Who is covered by the Act?



- Any person, whether or not a licensee of the NRC, who produces, receives, or acquires Safeguards Information is subject to the requirements (and sanctions) of the Atomic Energy Act of 1954, as amended

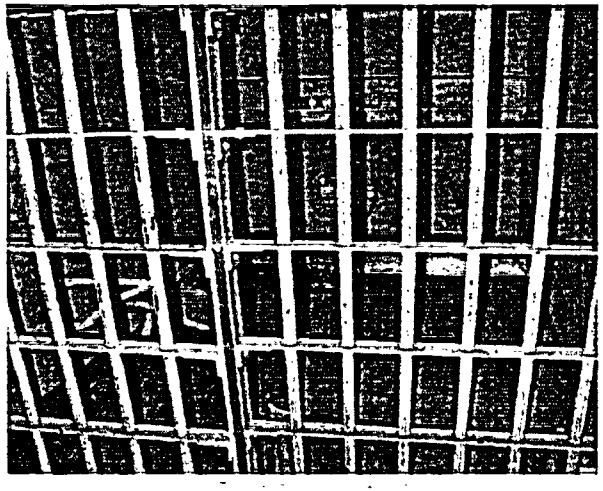
Penalties for Disclosure

- Inadequate protection of Safeguards Information, including inadvertent release or unauthorized disclosure, may result in civil and/or criminal penalties (The Act)

mvtech.com

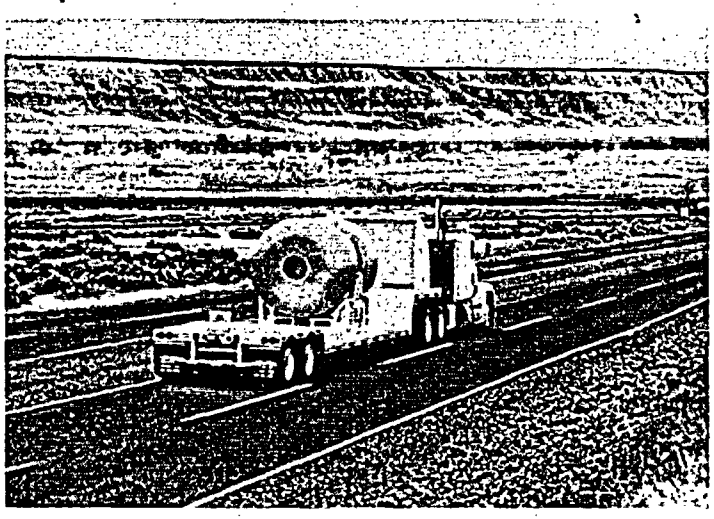
Penalties for Disclosure

- Furthermore, willful violation of any regulation or order governing Safeguards Information is a felony subject to criminal penalties in the form of fines or imprisonment, or both



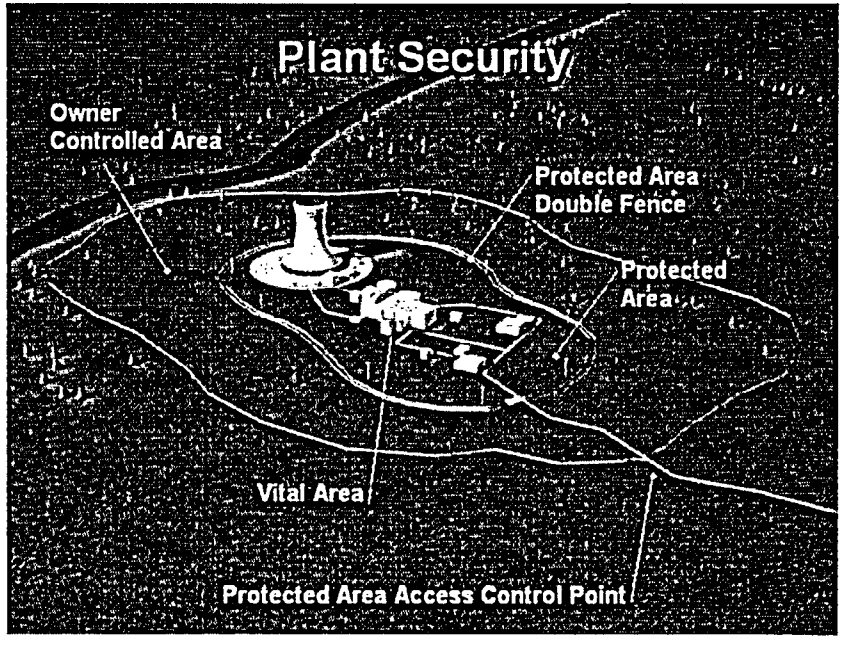
Examples of Safeguards Information

1) security measures for the physical protection of special nuclear material;



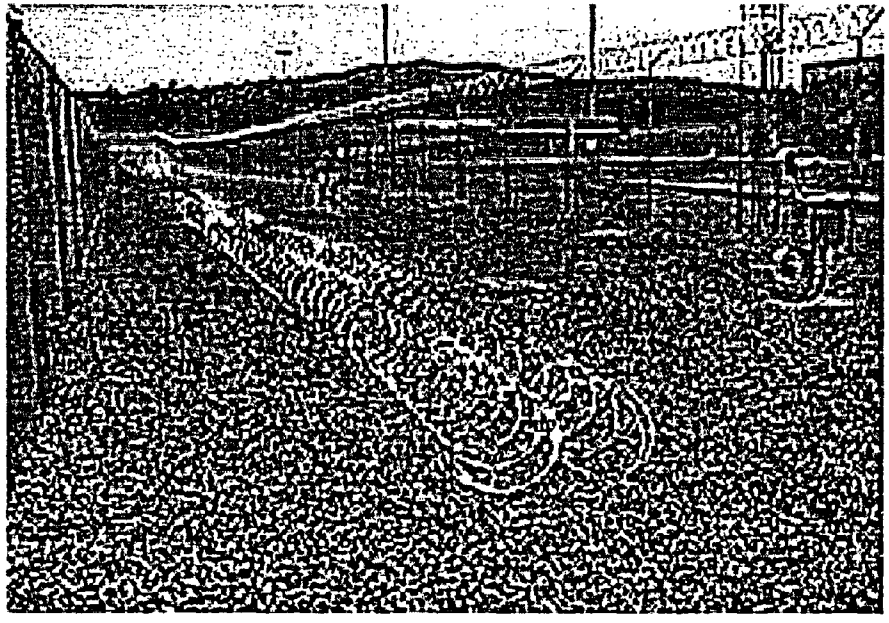
Safeguards Information

2) security measures for the physical protection and location of certain plant equipment vital to the safety of a facility possessing nuclear materials subject to NRC jurisdiction;



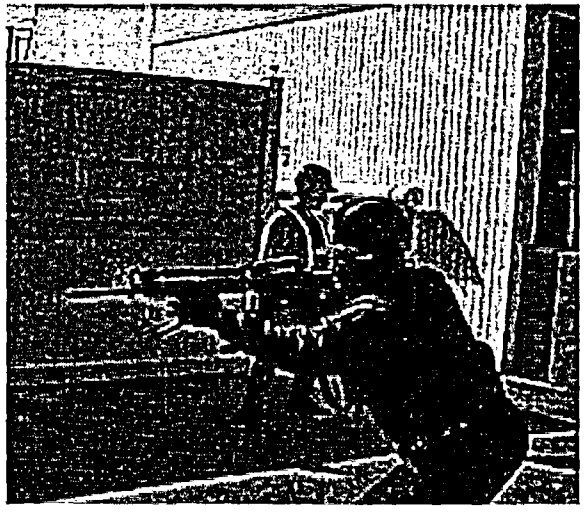
Safeguards Information

3) the design features of the physical protection system;



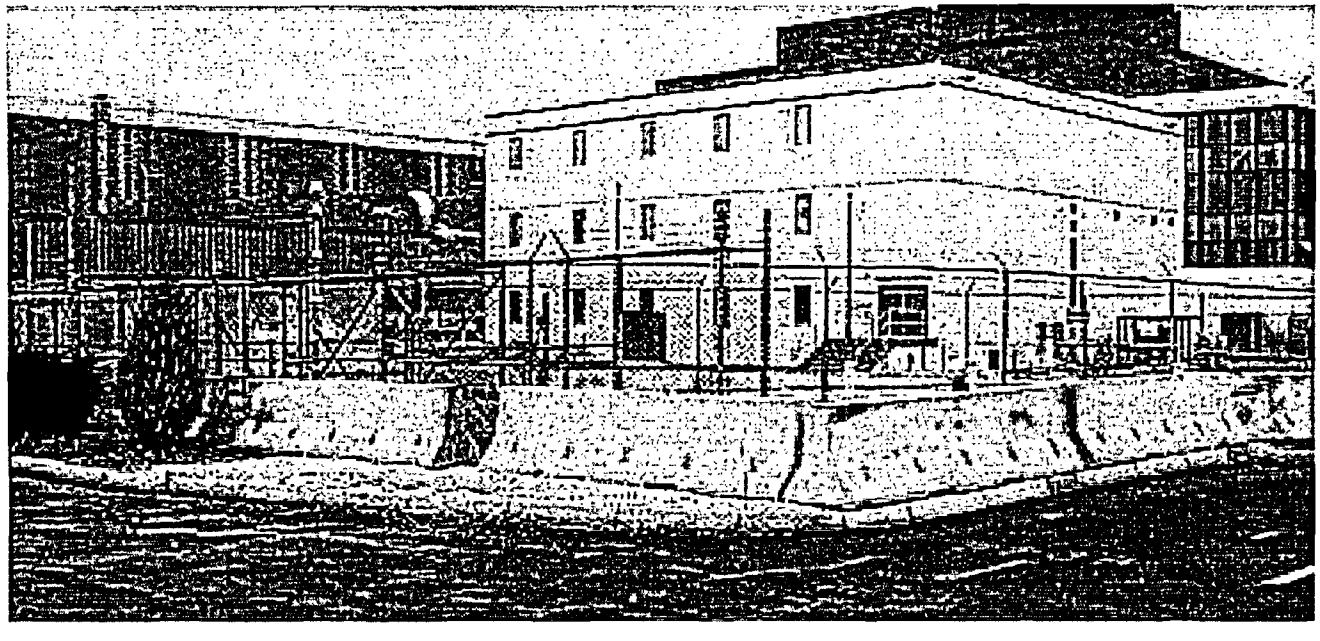
Safeguards Information

4) operational procedures for the security organization;



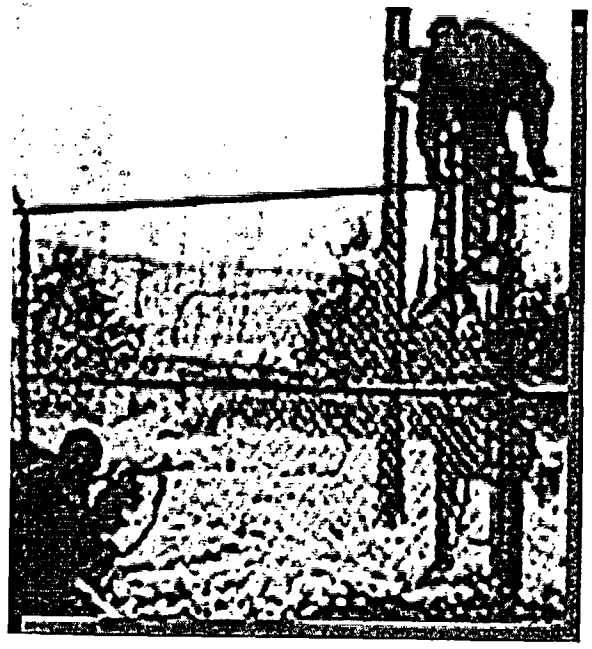
Safeguards Information

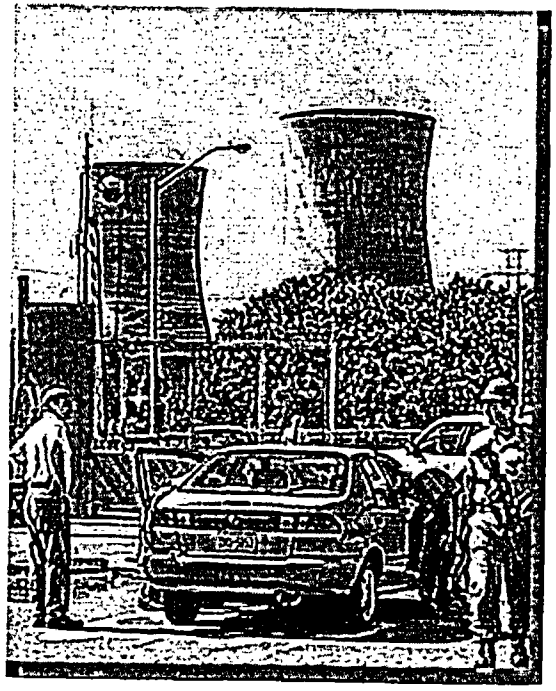
5) improvements or upgrades to the security system;



Safeguards Information

6) vulnerabilities or weaknesses not yet corrected; and





Safeguards Information

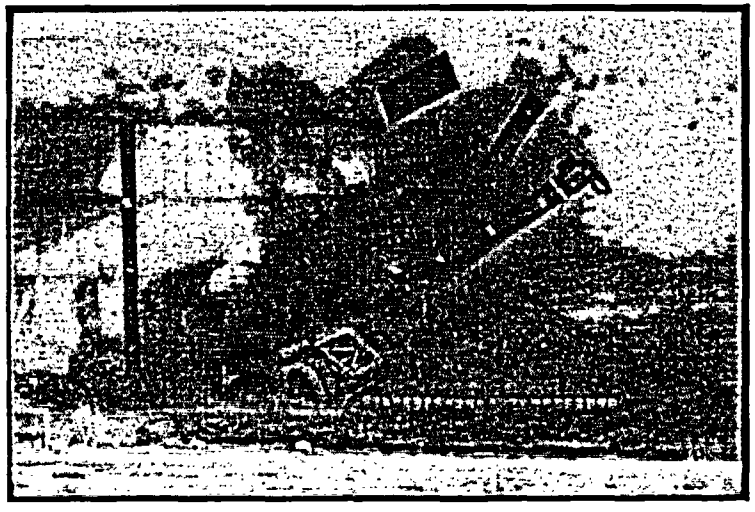
7) such other information as the Commission may designate by order

Examples Include:

Design Basis Threat;

Vulnerability Assessments

Training and Qualifications



Recent Actions

- NRC issued SGI Orders and Compensatory Measures, post 9/11, to increase security
- New SGI Orders to Irradiator licensees and Byproduct Manufacturers and Distributors
- Review of other programs

Conditions for Access

Access to SGI requires both need-to-know as well as a determination concerning the trustworthiness of individuals having access to the information. This is normally accomplished through a background check

Need-to-Know

- Determination by a person having responsibility for protecting SGI that a proposed recipient's access is necessary in the performance of official, contractual, or licensee duties of employment

No Comment Policy

Occasionally, sensitive information appears in the public domain without authorization

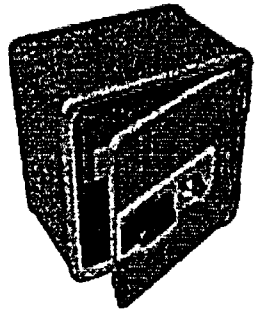
Questions raised about the accuracy, designation, technical merit of such information should be "no comment"

SGI Protection Requirements

While in Use

- Under the control of an authorized individual
- Requirement is satisfied if the SGI is attended by an authorized individual even though the information is, in fact, not constantly being used

Protection Requirements



While in Storage

- Stored in an approved security storage container
- Knowledge of lock combinations or access to keys protecting SGI limited to a minimum number of authorized personnel with "need-to-know"
- Access to lock combinations or keys strictly controlled to prevent disclosure to an unauthorized individual

Transportation of Documents and Other Matter

Outside of facility

- When transmitted outside an authorized place of use or storage-enclosed in two sealed envelopes or wrappers
- Inner envelope or wrapper contains the name and address of the intended recipient, marked both sides, top and bottom with the words "**Safeguards Information**"

Transportation of Documents and Other Matter

- Outer envelope or wrapper addressed to the intended recipient, address of the sender, not bear any markings or indication that the document contains SGI

- Transported by commercial delivery company providing nation-wide overnight service with computer tracking features, US first class, registered, express, or certified mail, or by any individual authorized access

Transportation of Documents and Other Matter

Within a facility

- Transmitted using a single opaque envelope
- May also be transmitted without single wrapping provided adequate measures are taken to protect against unauthorized disclosure

Preparation and Marking of Documents

Marked "**Safeguards Information**" in a conspicuous manner on the top and bottom of to indicate the presence of protected information

Additional pages marked in a conspicuous fashion at the top and bottom with letters denoting **"Safeguards Information"**

Preparation and Marking of Documents

Must also contain:

(i) the name, title, and organization of the individual authorized to make a SGI determination, and who determined the document contains SGI;

(ii) the date the document was originated or the determination made;

(iii) an indication that the document contains SGI; and

(iv) an indication that unauthorized disclosure subject to civil and criminal sanctions

Preparation and Marking of Documents (continued)

Transmittal letters or memoranda which do not contain SGI marked to indicate that attachments or enclosures contain SGI but transmittal does not (e.g., "When separated from SGI enclosure(s), this document is decontrolled")

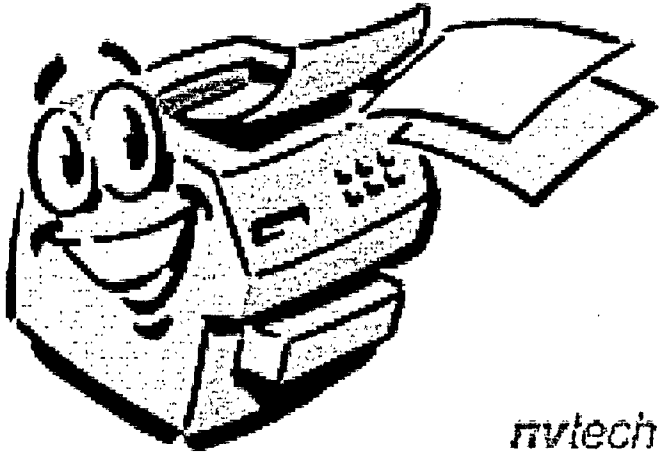
Each item of correspondence will clearly indicate which contain SGI and which do not. Portion marking is not required for physical security and safeguards contingency plans

Removal from SGI Category

- Removed from SGI category (decontrolled) only after NRC determines information no longer meets the criteria of SGI
- Licensees have authority to make determinations on specific documents they created which no longer contain SGI information
- Authority to determine document removal exercised only by, or with permission of, the individual (or office) making original determination
- Indicate name and organization of individual removing document from SGI category and date of removal
- Other persons who have the document in their possession should be notified of the downgrading

Reproduction of Matter Containing SGI

Reproduced to the minimum extent necessary consistent with need without permission of the originator



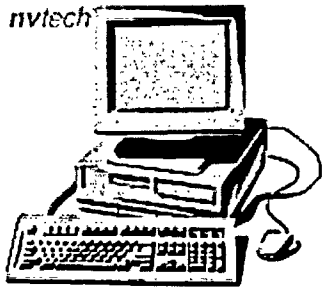
Destruction of Matter Containing SGI

Destroyed by tearing into small pieces, burning, shredding or any other method precluding reconstruction by means available to the public at large (piece sizes one half inch or smaller composed of several pages or documents and thoroughly mixed would be considered completely destroyed)

Use of Automatic Data Processing (ADP) Systems

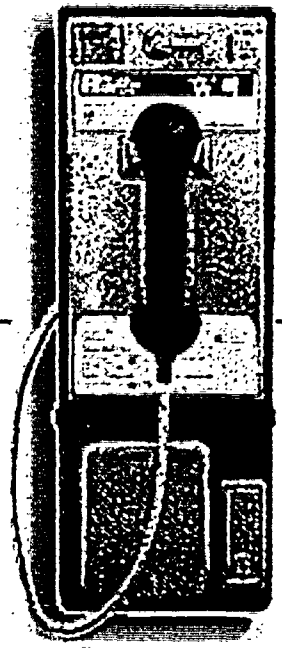
- Processed or produced on ADP system provided system is self-contained within the licensee's or contractor's facility and require use of entry code/pass word
- SGI files labeled "**Safeguards Information**" and saved to removable media stored in approved security storage container
- Specific files containing SGI password protected to preclude access by an unauthorized individual

Use of Automatic Data Processing (ADP) Systems



- If SGI is produced on a typewriter, the ribbon must be removed and stored in the same manner as other SGI information
- SGI files may be transmitted over a network if the file is encrypted
- (Federal Information Processing Standards (FIPS) 140-1 and 140-2.)

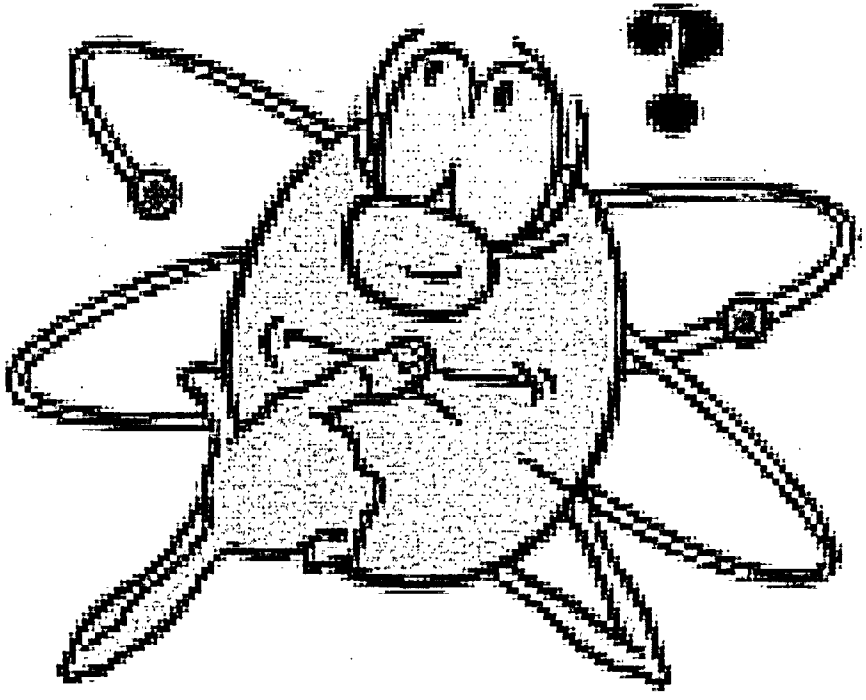
Telecommunications



- Infrequent or non-repetitive telephone conversations regarding a physical security plan or program are permitted provided discussion is general in nature
- Individuals should use care when discussing SGI at meetings or in the presence of others to insure that the conversation is not overheard by persons not authorized access
- Transcripts, tapes or minutes of meetings or hearings that contain SGI should be marked and protected in accordance with these requirements

NRC Intent

- Strike a balance between the public's right to information so they can meaningfully participate in regulatory processes and the need to protect sensitive security information from inadvertent release or unauthorized disclosure

- Continue to evaluate its requirements, policies and guidance concerning the protection and unauthorized disclosure of Safeguards Information

Questions?