Classifying National Security Information

Agency for International Development
Office of Security
Washington, D.C. 20523

Classifying National Security Information

Agency for International Development
Office of Security
Washington, D.C. 20523


UNITED STATES OF AMERICA

Contents

Introduction

This pamphlet, "Classifying National Security Information", has been developed as a guide for classifying, declassifying, and safeguarding National Security Information in all forms. It is intended for use by persons who originally or derivatively classify National Security Information or participate in its preparation. Further specific guidance and instructions can be obtained from the Uniform Security Regulations (5 FAM 900).

This pamphlet is applicable to both A.I.D./Washington and all A.I.D. missions abroad.

Any questions concerning the handling of administratively controlled or National Security material should be referred to your A.I.D. Unit Security Officer or the Office of Security on (703) 875-4050.

Corbett M. Flannery
Assistant Inspector General for Security

Classifying National Security Information

What is national security information? National security information is official information that relates to our national defense or foreign relations. The Government must own, have a proprietary interest in, or otherwise control the information. Control pertains to the government's ability to regulate access to the information.

National security information may be classifed at one of the following three levels:

TOP SECRET is applied only to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security.

SECRET is applied only to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

CONFIDENTIAL is applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security.

Except as provided by statute, we cannot use terms such as SENSITIVE, AGENCY, BUSINESS, ADMINISTRATIVELY, etc., in conjunction with any of the three classification levels defined above.

Why is information classified? Since World War II, we have recognized the need to protect official information. This need is related to maintaining an advantage in the security of our nation. If classified information were compromised, our national advantage would or could be damaged, minimized, or lost, thereby adversely affecting the national security. Security classification is therefore applied only to protect the national security.

Classification cannot be used to conceal violations of law, inefficiency, or administrative error; to prevent embarrassment to a person, organization, or agency; to restrain competition; or to prevent or delay the release of information that does not require protection in the interest of national security.

Basic scientific research information not clearly related to the national security may not be classified.

How is national security information classified? Official information is protected through a series of Executive Orders. Except as provided in the Atomic Energy Act of 1954, Executive Order 12356 prescribes a uniform system for classifying, declassifying, and safeguarding national security information. Information may be classified in one of two ways—originally or derivatively.

Original classification is an initial determination that information requires protection against unauthorized disclosure in the interest of national security. Derivative classification is just as its name implies, classification derived from another source. It is the act of incorporating, paraphrasing, restating or generating in new form information that is already classified, and marking the newly developed material consistent with the markings of the source information.

Information may be classified after receipt of a request for it under the Freedom of Information Act of 1974 or the mandatory review provisions of E.O. 12356, if its classification is consistent with E.O. 12356 and is authorized personally on a document-by-document basis by the Administrator as set forth in the Uniform State/A.I.D./USIA Security Regulations.

Classification may be restored by the Administrator to documents already declassified and disclosed if a determination is made in writing that the information requires protection in the interest of national security and it may reasonably be recovered. The following factors must be considered:

- the elapsed time following disclosure;
- the nature and extent of disclosure;
- the ability to bring the fact of reclassification to the attention of personnel to whom the information was disclosed;
- the ability to prevent further disclosure; and
- the ability to retrieve the information voluntarily from persons not authorized access in its reclassified state.

Who may classify information originally? Information may be classified originally up to the Secret level by the Administrator or by officials delegated that authority by the Administrator. No official of A.I.D. is authorized to originally classify information at Top Secret. Classification authority delegated by the Administrator cannot be redelegated but may be exercised by persons designated in writing to act in the absence of the classifying authority. No one has a right to classify information solely by virtue of rank or position.

How is information classified originally? To make an original classification determination, first the official making the determination must have original classification authority. Second, identify exactly each item of information that may require protection. Third, determine that the information falls within one or more of the classification categories listed below. Fourth, and most importantly, the original classifier must determine that unauthorized disclosure of the information reasonably could be expected to cause damage to the national security.

When in doubt about the need to classify, safeguard the information as Confidential national security information until a final determination is made by an authorized classifier as to its classification. The final determination must be made within thirty days.

When in doubt as to the appropriate level of classification, safeguard the information at the higher level until a final determination is made by an authorized classifier. The final determination must be made within thirty days.

What criteria are used to classify information? Information may be considered for classification if it concerns:

- foreign relations or foreign activities of the United States;
- foreign government information;
- scientific, technological, or economic matters relating to the national security;
- intelligence activities (including special activities) or intelligence sources or methods;
- military plans, weapons, or operations;
- the vulnerability or capabilities of systems, installations, projects, or plans relating to the national security;

- United States government programs for safeguarding nuclear materials or facilities;
- cryptology.
- a confidential source; or
- other categories of information that are related to the national security and that require protection against unauthorized disclosure as Determined by the President, the A.I.D. Administrator, or by other officials who have been delegated original classification authority by the President.

A compilation of unclassified items of information may be classified if the compilation provides an added factor which warrants classification under the criteria listed above. Information associated with other unclassified or classified information may also warrant classification. Classification on this basis must be supported by a written explanation that is maintained with the file copy or referenced on the record copy of the information.

Unauthorized disclosure of foreign government information, the identity of a confidential foreign source, or intelligence sources or methods is presumed to cause damage to the national security.

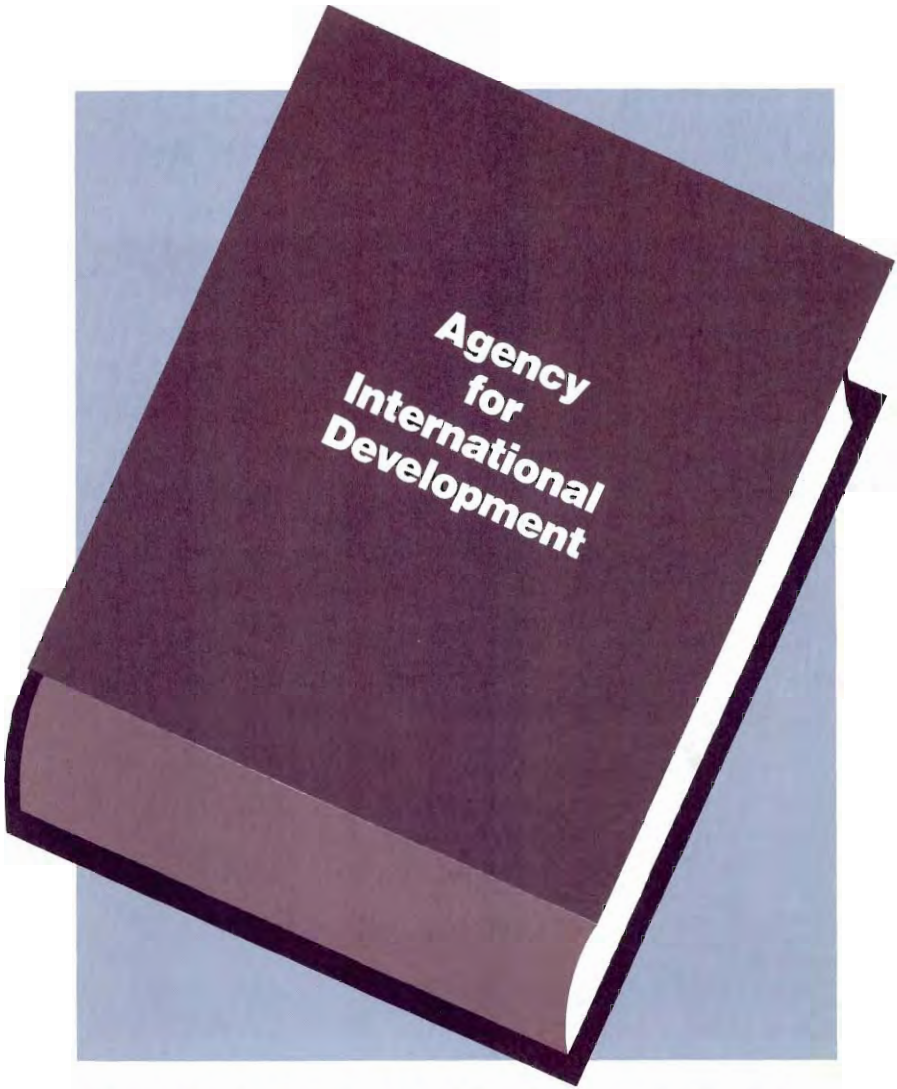
Foreign government information need not fall within any other classification criteria to be classified.

Classified information must not be declassified automatically as a result of any unofficial publication or inadvertent or unauthorized disclosure in the United States or abroad of identical or similar information.

How long may information remain classified? Information shall remain classified as long as its unauthorized disclosure would result in damage to the national security. When it can be determined, a specific date or event for declassification must be set by the original classification authority at the time the information is originally classified.

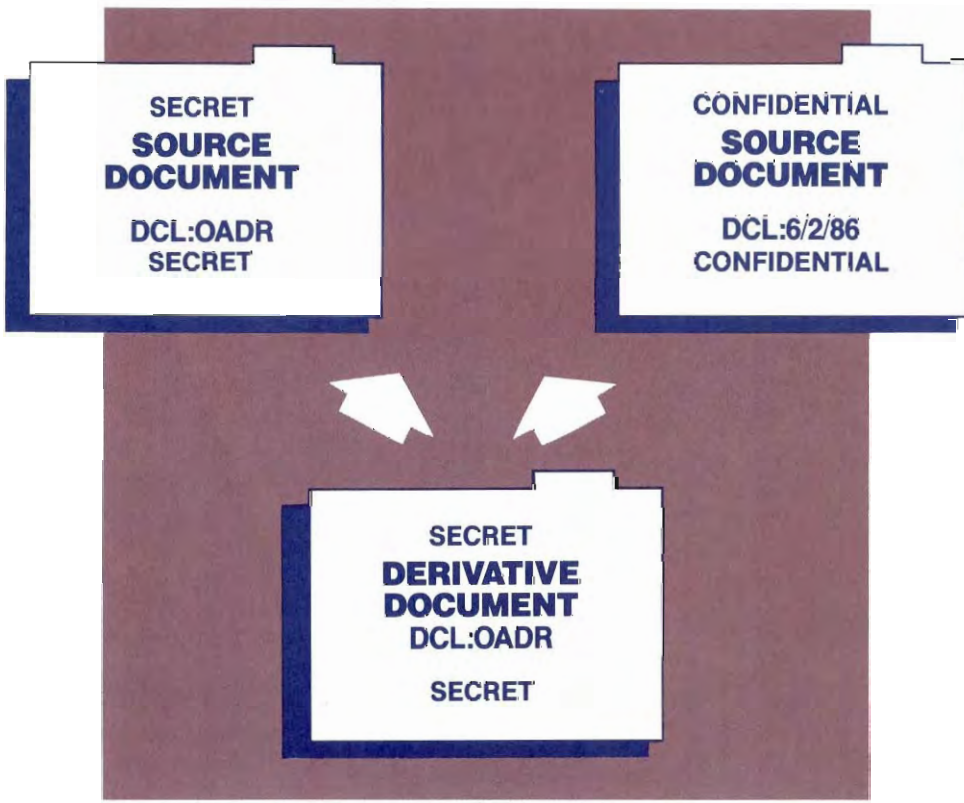
Automatic declassification markings applied under predecessor executive orders will remain valid unless the classification is extended by an authorized declassification authority. The extensions may be by individual documents or categories of information. The declassification authority must notify holders of any such extensions.

Information classified under E.O. 12356 and other predecessor orders and marked for declassification review must remain classified until reviewed for declassification.



How can tentative classification be applied? If a person originates or develops information which is believed to require original classification and the person does not possess original classification authority, that person must safeguard the information in the manner prescribed for the intended classification and forward it to an appropriate original classification authority for decision. A classification determination must be made within thirty (30) days. Information intended to be classified at the TOP SECRET level must be forwarded to the agency having primary interest or to the Information Security Oversight Office for final classification. Upon decision by the classifying authority, the appropriate classification marking will be applied.

Who may classify information derivatively? Those employees with the appropriate security clearance, who are required by their work to restate classified source information, may classify derivatively.

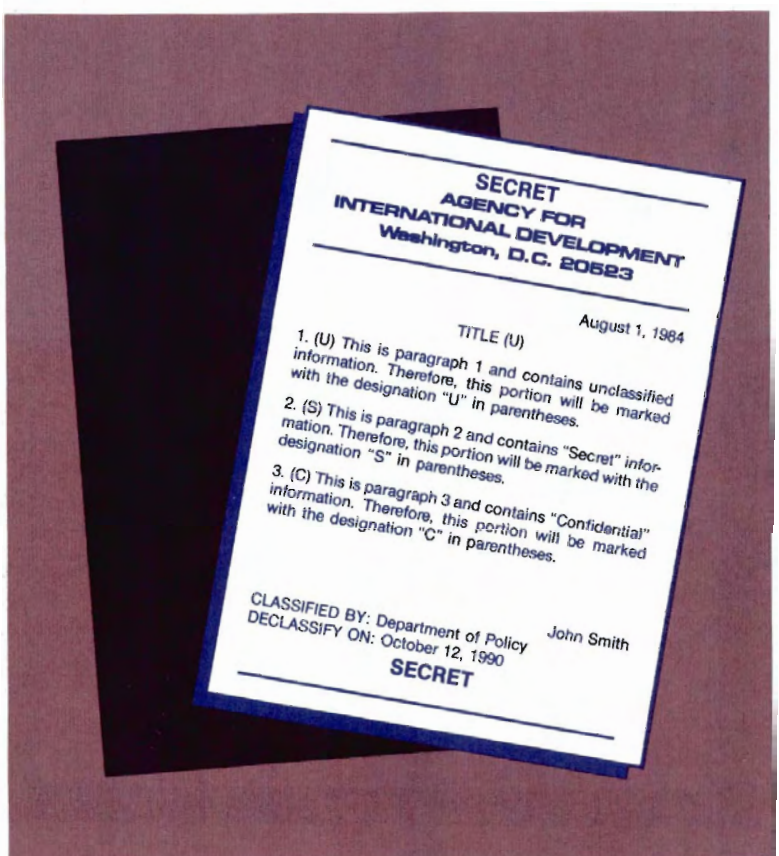


How is information classified derivatively? Derivative classification is usually accomplished by referring to information contained in a previously classified source document. However, this type of classification still requires that judgments be made, such as whether the new document actually contains specific information which the original classification authority considered to be classified. It is essential that officials preparing new material related to a classified source document respect and comply with the classification decisions reflected in the source document. Using the classification markings of portions, it may be possible to selectively extract information from a source document which may be incorporated in a new document at a lower level of classification.

The overall classification markings and portion markings of the source documents should apply adequate classification guidance to the person making the extraction. If portion markings or classification guidance are not found in the source, guidance must be obtained from the originator of the source document. In the absence of such markings or guidance the extracted information will be classified according to the overall classification of the source document.

What markings are placed on classified documents?

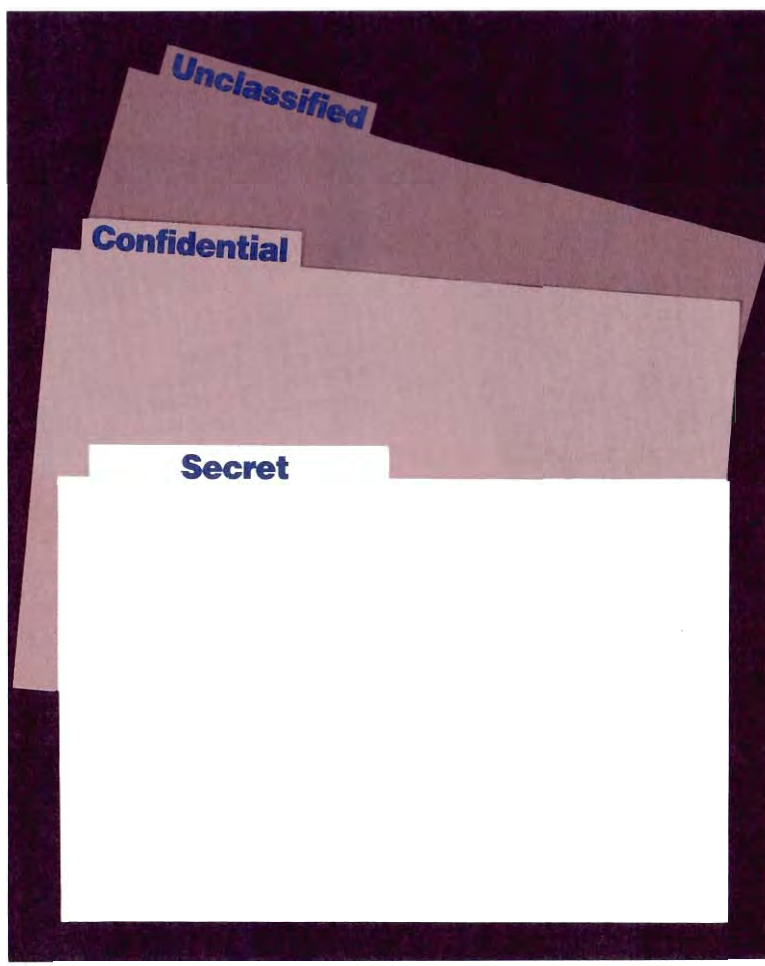
Classified information is marked to place recipients on alert about its sensitivity. At a minimum, classified documents must indicate (1) the highest classification level of the information, (2) the identity of the original classification authority,



(3) the agency or office of origin, and (4) a date or event for declassification, or the notation, "Originating Agency's Determination Required," abbreviated "OADR." This marking denotes that at the time of original classification, the classifier is unable to determine a date or event for declassification.

Mark all portions, including subjects and titles, of a classified document to indicate the level of classification. This is done by placing a parenthetical designation immediately preceding the text to which it applies.

Who may declassify information? Information may be declassified or downgraded by the official who authorized the original classification, if that official is still serving in the same



position; by a successor; by a supervisory official of either; or by an official specifically delegated such authority in writing by the Administrator.

When is information declassified? National security information over which the Agency for International Development exercises final classification jurisdiction must be declassified or downgraded as soon as national security considerations permit. There are four actions that may result in the declassification of information. First, information marked with a specific declassification date or event is declassified on that date or upon occurrence of that event. Second, an agency or citizen may request information be reviewed under the mandatory review provision of E.O. 12356. Third, an agency or citizen may request information under the Freedom of Information Act. Fourth, the Archivist of the United States systematically reviews for declassification the permanently valuable records in the National Archives.

If the Director of the Information Security Oversight Office determines that information is classified in violation of E.O. 12356, the Director may require the agency that originally classified the information to declassify it. Any such decision by the Director may be appealed to the National Security Council. The information will remain classified until the appeal is decided.

How is information declassified? Information is declassified by removing the security classification restrictions and markings. Then, the information may be further protected from disclosure pursuant to an applicable statute or released as public information.

To declassify information, line through the overall classification marking and place a statement on the cover or first page to indicate the declassification authority, by name and title, and the date of declassification. If practicable, the classification markings on each page should be cancelled; otherwise, the statement on the cover or first page must indicate that the declassification applies to the entire document.

Be aware that when information is determined to be no longer damaging to national security, it may continue to be exempt from public disclosure by law. If so, when the information is declassified, the declassification authority must indicate that all or portions of the information become LIMITED OFFICIAL USE and cite the authority which permits non-disclosure.

What notification is made when information is declassified? When classified information has been properly marked with a specific date or event for declassification it is not necessary to issue notices of declassification to any holders. However, when declassification action is taken earlier than originally scheduled, or the duration of classification is extended, the authority making such changes must promptly notify all holders to whom the information was originally transmitted. This notification shall include the marking action to be taken, the authority for the change (name and title), and the effective date of the change.

Who can have access to classified information? An employee or contractor is eligible for access to classified information provided the employee or contractor has been determined to be trustworthy and access is essential to the accomplishment of lawful and authorized Government purposes. A national security clearance is an indication that a trustworthiness decision has been made. No one has a right to have access to classified information solely by virtue of title, position, or level of security clearance. The fact that an individual is a Federal employee does not mean that he or she has been cleared for access to classified information.

Before granting access to classified information, you must verify the identity, the security clearance, and the need to know of the recipient. You are ultimately responsible for determining whether an individual requires access to classified information.

A.I.D. issues the following types of color-coded identification badges:

1. Picture badges with AGENCY FOR INTERNATIONAL DEVELOPMENT written in *Green* with a blue background identify the holder as possessing a TOP SECRET clearance.
2. Picture badges with AGENCY FOR INTERNATIONAL DEVELOPMENT written in *Red* with a blue background identify the holder as possessing a security clearance, level unspecified.
3. Picture badges with AGENCY FOR INTERNATIONAL DEVELOPMENT written in *Red* with a yellow background identify the holder as possessing no security clearance.
4. Picture badges with AGENCY FOR INTERNATIONAL DEVELOPMENT written in *Red* with a green background identify the holder as possibly having a security clearance.

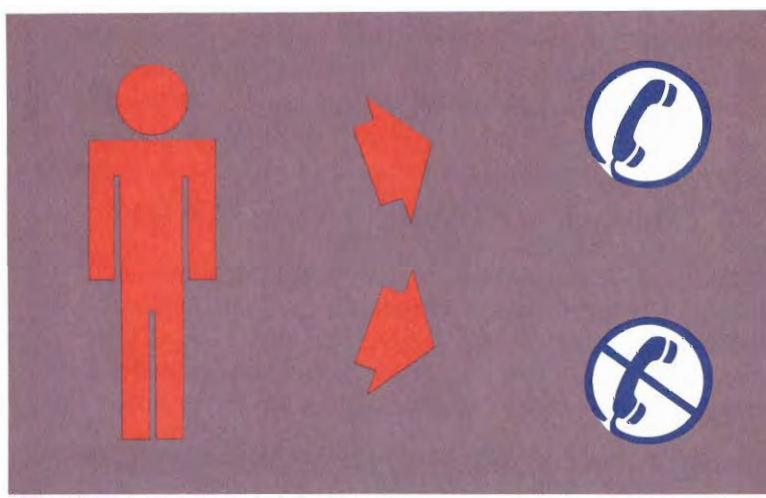
Whenever any doubt exists, you can verify a security clearance by calling the Office of Security (IG/SEC) on 875-4050. If you are overseas, you can contact the Unit Security Officer, the Post Security Officer, the Regional Security Officer or cable IG/SEC.

When you disclose classified information, you should advise the recipient of the classification level of the information.

What restrictions are placed on the dissemination of classified information? Some classified documents may be marked with caveats restricting their dissemination. As a general rule, however, classified information originated in another agency may be disseminated outside of A.I.D. only with the consent of the originator. Such consent must be maintained in writing as a matter of record. This restriction does not apply to additional distribution within A.I.D. or to distribution to contractors who require the information in performance of contracted services for A.I.D.

How should classified information be safeguarded? You can protect classified information in many ways. These ways involve the use, storage, reproduction, transmission, and destruction of classified information under conditions that provide protection and prevent access by unauthorized persons.

- First, never perform classified work or hold classified discussions in a non-secure area such as a home, restaurant, hotel, car pool, or plane.



- Never discuss classified information on the telephone unless you are using an approved security communications system. While most people recognize the dangers of using the telephone for this purpose, some believe that by using code words, acronyms, or double talk, they somehow render a classified conversation harmless. Don't be misled. Telephone conversations are extremely vulnerable to interception.

- Most leaks of classified information result from conversations or interviews, not from the compromise of documents. Be especially cautious when dealing with persons who are not authorized to have access to classified information.

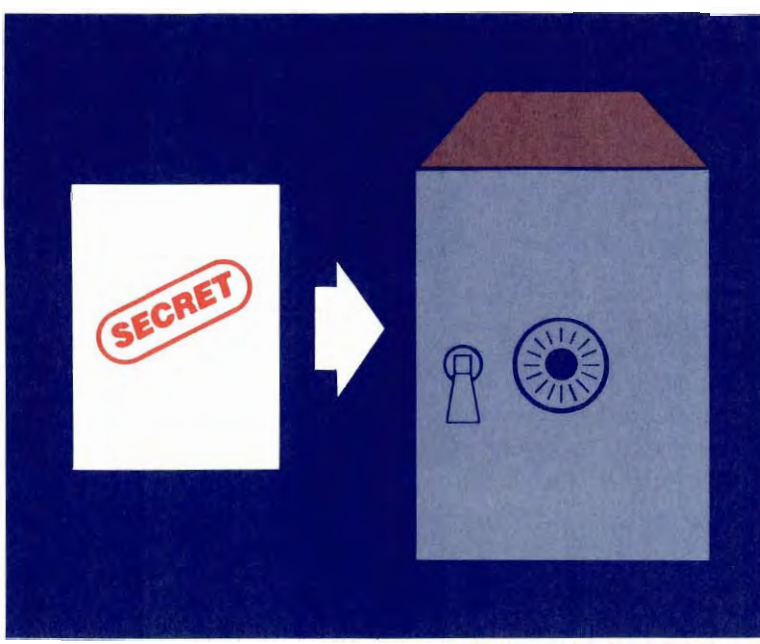
- When you are not working with classified documents, lock them up in an approved container. Memorize your safe combinations. Never write them on calendars, store them in your desk, or carry them in your wallet or purse.

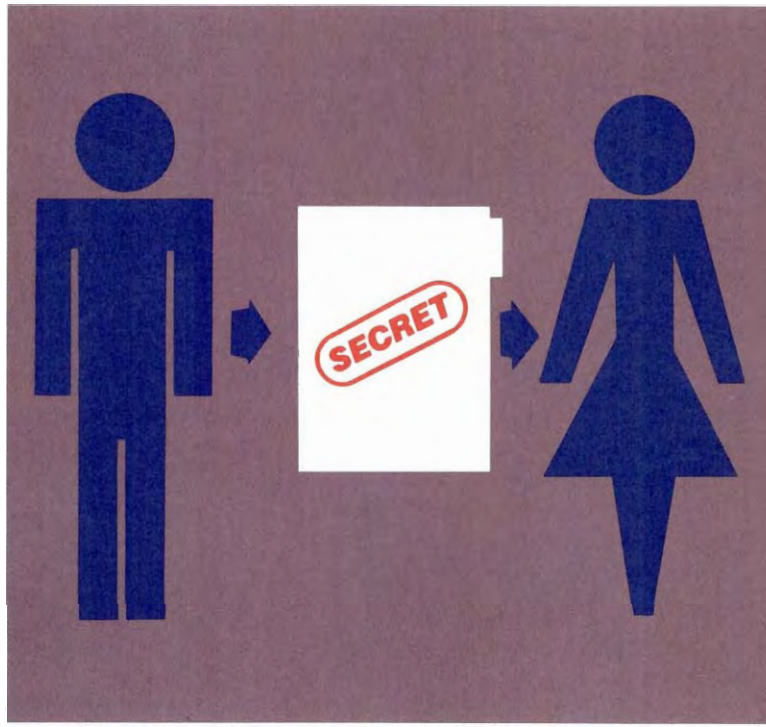
- If you no longer require classified information for operational or record purposes, destroy it using one of the many approved methods. Be sure the destruction of your classified information is recorded.

Is classified information personal property? Classified information is not personal property. Upon transfer or separation, you must return all classified information for which you are responsible to your supervisor or security office.

What can I do to prevent the compromise of classified information. You can prevent the compromise of classified information by being conscious of its sensitivity and by following the rules and precautions for safeguarding it. Remember, you expose yourself to serious penalties if you purposely or even negligently compromise classified information.

Immediately report any actual or suspected unauthorized compromise or disclosure of classified information to your security office. Also, don't hesitate to report incidents for which you may be partially or fully responsible. Your failure to report them is far more likely to result in serious consequences.





Need help?

In A.I.D./Washington, contact:

Office of Security
Agency for International Development
Room 415
1621 North Kent Street (State Annex 16)
Washington, D.C. 20523
(AC 703) 235-2920

Overseas personnel contact:

Unit Security Officer
Post Security Officer
Regional Security Officer
Cable IG/SEC, A.I.D./W

Processing "Limited Official Use" Material on Word Processing and Office Information Systems Equipment in A.I.D./Washington

In A.I.D./Washington the employees are permitted to process LOU material on word processing or office information systems equipment, providing the following conditions are met:

- All LOU documents processed on word processing or office information systems equipment must be protected by a password. If the word processor or office information systems does not have the capability of placing a password on LOU documents, it may NOT be used for processing LOU material.
- All tapes, magnetic cards, and floppy diskettes which are used for the storage of LOU material shall be secured at the close of each working day, in accordance with provisions of paragraph 958.1 of the Uniform Security Regulation (5 FAM 900).

CLASSIFIED MATERIAL (CONFIDENTIAL, SECRET, TOP SECRET) SHALL NOT BE PREPARED, PROCESSED, OR STORED ON WORD PROCESSING AND OFFICE INFORMATION SYSTEMS EQUIPMENT.

THIS NOTICE DOES NOT AUTHORIZE A.I.D. MISSIONS TO PROCESS CLASSIFIED OR LOU MATERIAL ON WORD PROCESSING AND/OR OFFICE INFORMATION SYSTEMS EQUIPMENT.