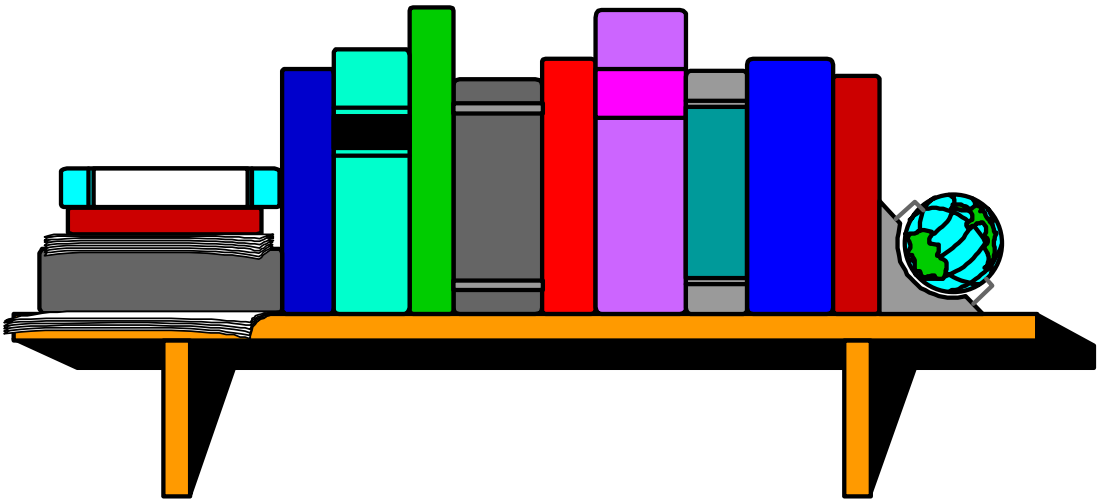
USDA UNITED STATES DEPARTMENT OF AGRICULTURE

Information Security Desktop Reference



FORWARD

This booklet was developed to assist United States Department of Agriculture employees and contractor personnel to properly classify information and procedures in handling classified information. The President awarded Original Classification Authority (OCA), for information up to the SECRET level, to the Secretary of Agriculture on September 26, 2002.

Federal Agencies receive their classification guidance from the President of the United States through an Executive Order. The Executive Order for National Security Information is EO 12958, dated April 17, 1995, and was signed by Former President William Clinton. During his administration, the EO was amended twice, EO 12972, dated September 18, 1995, and EO 13142, dated November 19, 1999.

On March 25, 2003, President Bush further amended EO 12958 with EO 13292. This amendment is the largest change in classification and declassification since 1995. This booklet covers EO 12958, as amended. The term "agency" is used throughout the EO and the booklet. For the purpose of this booklet, consider the term "**Agency**" equal to the term "**Department**" as used in "Department of Agriculture".

Information Security Staff
Personnel and Document Security Division
Office of Procurement and Property Management
August 2004

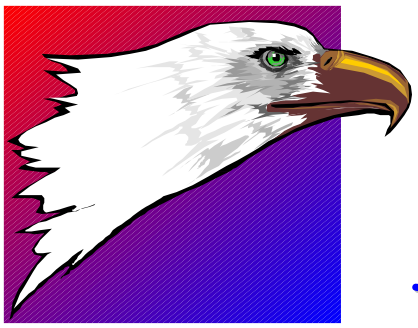


TABLE OF CONTENTS

WHAT CAN BE ORIGINALLY CLASSIFIED?

Authority: EO 12958 and implementing directives.

Requirements: Information may be originally classified if all the following conditions are met:

a. an OCA is classifying the information;

b. the information is owned by, produced by or for, or is under the control of the U.S. government;

c. the information falls within one or more of the categories of information listed below;

d. the OCA determines that unauthorized disclosure of the information reasonably could be expected to result in damage to national security, which includes defense against transnational terrorism, and the OCA is able to identify or describe the damage.

Classification Categories: (EO 12958 as amended, Section 1.4) Information shall not be considered for classification unless it concerns **(recommended USDA categories in purple)**:

a. military plans, weapons systems, or operations;

b. foreign government information;

c. intelligence activities (including special activities), intelligence sources or methods, or cryptology;

d. foreign relations or foreign activities of the U.S., including confidential sources;

e. scientific, technology, or economic matters relating to the national security, which includes defense against transnational terrorism;

f. U.S. government programs for safeguarding nuclear material or facilities;

g. vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism; or

h. weapons of mass destruction.

COMPILATION OR AGGREGATION OF INFORMATION

Placing two or more pieces of unclassified information together can create information that may fall into one of these categories. It's important to USDA that we quickly identify and appropriately classify this information when it occurs!

WHAT'S PROHIBITED FROM CLASSIFICATION?

There are prohibitions and limitations to what can be classified. Our democratic principles require that the American people be informed of the activities of their Government and our Nation's progress depends on the free flow of information. Note:

a. In no case shall information be classified in order to:

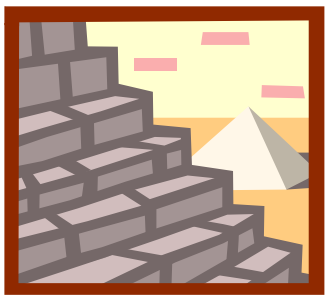
1) Conceal violations of law, inefficiency, or administrative error;

2) Prevent embarrassment to a person, organization, or agency;

3) Restrain competition; or

4) Prevent or delay the release of information that does not require protection in the interest of national security.

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



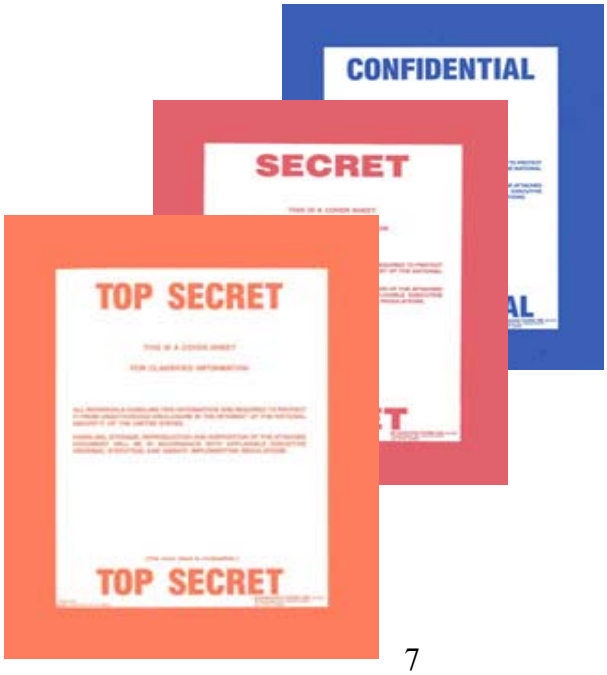
CLASSIFICATION LEVELS

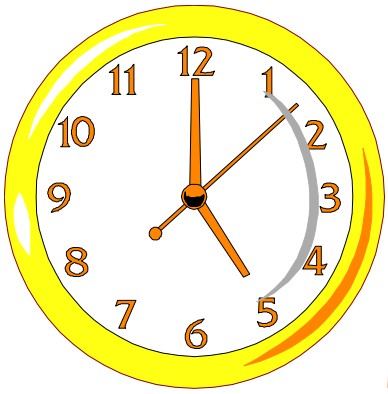
Classification Levels: There are only three levels of classification:

a. "**TOP SECRET**" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **EXCEPTIONALLY GRAVE DAMAGE** to the national security that the original classification authority is able to identify and describe.

b. "**SECRET**" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **SERIOUS DAMAGE** to the national security that which the original classification authority is able to identify and describe.

c. "**CONFIDENTIAL**" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause **DAMAGE** to the national security that which the original classification authority is able to identify and describe.





HOW LONG TO CLASSIFY?

Duration of Classification: At the time of original classification, the OCA shall attempt to:

a. establish a specific date or event (i.e. a field test, or upon completion of the Olympics) for declassification based upon the duration of the national security sensitivity of the information;

b. if a date or event cannot be determined, the OCA can select a timeframe up to ten years for declassification of the information;

c. if the information is considered to have permanent historical value (Presidential documentation or a file series or record is identified by USDA and approved by the U.S. Archivist), a date up to 25 years from it's original classification can be selected; or

d. if the information is expected to do one of the items below, the OCA can exempt (see below) the information from declassification (beyond 25 years provided a 25 year review is conducted):

1) reveal the identify of a confidential human source, or a human intelligence source, or reveal information about the application of an intelligence source or method;

2) reveal information that would assist in the development or use of weapons of mass destruction;

3) reveal information that would impair U.S. cryptologic systems or activities;

4) reveal information that would impair the application of state of the art technology within the U.S. weapon system;

5) reveal actual U.S. military war plans that remain in effect;

6) reveal information, including foreign government information, that would seriously and demonstrably impair relations between the U.S. and foreign government, or seriously and demonstrably undermine ongoing diplomatic activities in the U.S.;

7) reveal information that would clearly and demonstrably impair the current ability of U.S. government officials to protect the President, Vice President, and other protectees for whom protection services, in the interest of national security, are authorized;

8) reveal information that would seriously and demonstrably impair current national security emergency preparedness plans or reveal current vulnerabilities of systems, installations, infrastructures, or projects relating to the national security; or

9) violate a statute, treaty, or international agreement.

If the OCA chooses to exempt information from declassification for +25 years, they must notify the President through the Assistant to the President for National Security Affairs with the specific file series of records for which a review or assessment has determined that the information requires continued classification. The format for this notification is described in the EO 12958.

Derivative Classification

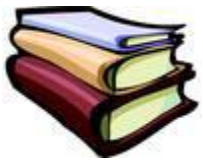
What is Derivative Classification? Incorporating, paraphrasing, restating, or generating in new form that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. Derivative classification includes the classification of information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

Who can do Derivative Classification?

Anyone who is authorized to use classified source documents and is required to paraphrase, extract, or summarize classified information from the source documents into a new document or media.

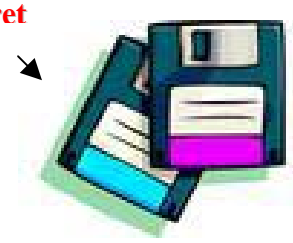
Classified Food Reports

Secret



New Classified Presentation

Secret

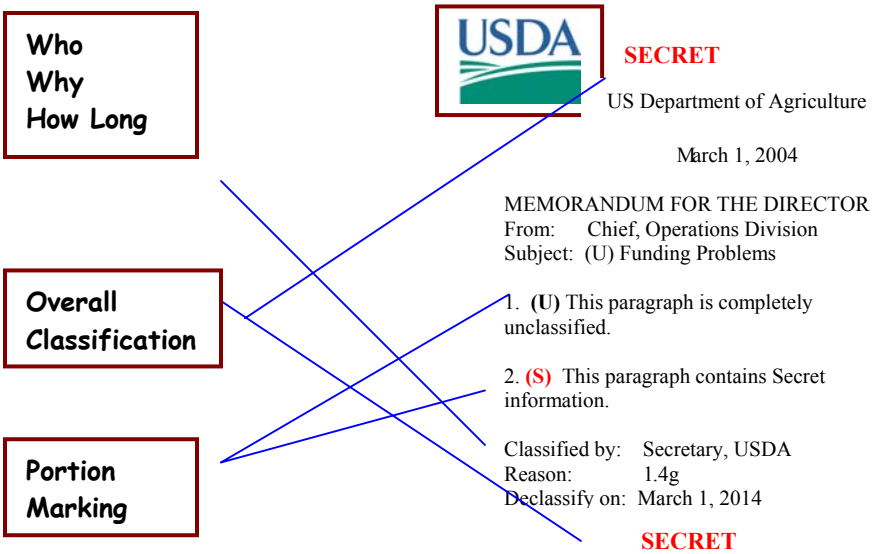


THE NEW MEDIA MUST BE MARKED WITH THE HIGHEST CLASSIFICATION OF THE SOURCE DOCUMENTS.

MARKING DOCUMENTS

Example of a Document Originally Classified by the Secretary of USDA

This is an example of a document that an original classifier has determined requires protection under E.O. 12958, as amended. It contains the essential markings required under the Order including portion marking, overall classification, identifies who it's classified by, the reason for classifying, and how long it can be classified:



Example of a Document Derivatively Classified by USDA

This is an example of a document that is derivatively classified. It contains the essential markings required under the Order including portion marking, overall classification, identifies the source document of classification, and how long it can be classified:

Source Document When do you Declassify

Overall Classification

Portion Marking

USDA

SECRET

US Department of Agriculture

March 1, 2004

MEMORANDUM FOR THE DIRECTOR
From: Chief, Operations Division
Subject: (U) Funding Problems

1. **(U)** This paragraph is completely unclassified.

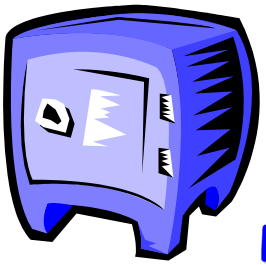
2. **(S)** This paragraph contains Secret information.

Derived From: USDA Security Classification Guide
Declassify on: March 1, 2014

SECRET

All media that has classified information stored on it must be labeled to identify the highest classification of the information stored within.

Labels for Marking Diskettes and Videos



PROPER SAFEGUARDING!

Authority – 32 CFR Part 2004, Safeguarding Classified National Security Information

General – This booklet provides only the basic safeguarding standards. It's important to note that when processing classified information on a computer, or safeguarding information higher than Top Secret (i.e. Sensitive Compartmented Information (SCI)) that the physical and procedural security requirements increase. All authorized holders of classified information are required to properly safeguard classified information. This includes Intellectual Property, which requires you to only discuss classified information with an individual who has the appropriate clearance, need-to-know, and the area is cleared for classified discussions.

CONFIDENTIAL Documents can only be stored in a **GSA approved security container.**

SECRET Documents can only be stored in a **GSA approved security container.**

TOP SECRET Documents must be stored in a **GSA approved security container** with one of the following supplemental controls:

a. Continuous protection by cleared guard or duty personnel;
b. Inspection of the security container every two hours by cleared guard or duty personnel;
c. An Intrusion Detection System (IDS) with the personnel responding to the alarm arriving within 15 minutes of the alarm annunciation; or
d. Security-in-Depth conditions, provided the GSA approved container is equipped with a lock meeting Federal Specifications.

DESTRUCTION OF CLASSIFIED INFORMATION

All classified information must be destroyed by using a shredder or coordinating with a central repository for burning the material. USDA can coordinate burn runs for large amounts of classified material. The preferred method is to use an approved **High Security Cross-Cut Shredder** that is NSA approved. CONFIDENTIAL and SECRET level documents can be destroyed without a witness or documentation. TOP SECRET information must be destroyed by two individuals cleared people for TS and the destruction is documented.

Diskettes, CDs, and removeable hard drives must be destroyed by NSA. Coordination for the destruction of these items can be done through the Personnel and Document Security Division.

http://www.nsa.gov/ia/government/MDG/EPL_02_01_J_July_2004.pdf

The Link to the NSA Approved Shredders!

TRANSMISSION OF CLASSIFIED INFORMATION!

Authority - 32 CFR Part 2004, Safeguarding Classified National Security Information

General – Persons transmitting classified information are responsible for ensuring that intended recipients are authorized persons with the capability to store classified information. A receipt system must be used. All classified information physically transmitted outside facilities shall be enclosed in two layers, both of which provide reasonable evidence of tampering and which conceal the contents. The outer layer does not show the level of classification inside or the recipient's name. The inner layer reflects those markings. The address on the outer envelope must be approved for receiving classified information. Detailed guidance on the transmission of classified information can be found in the Departmental Regulation 3440-01, Classification, Declassification, and Safeguarding Classified Information.

WITHIN THE U.S., DISTRICT OF COLUMBIA, PUERTO RICO, OR U.S. POSSESSION OR TRUST TERRITORY:

Hand-carrying – When classified information is hand-carried outside a facility, a locked briefcase may serve as the outer enclosure. The package must remain under continuous and constant protection while enroute. Routes must be kept point-to-point. Refer to DR 3440-01 for additional guidance.

CONFIDENTIAL – U.S. Postal Certified Mail or U.S. First Class Mail to a US government facility. Outer envelope must be marked "Do Not Forward, Return to Sender". Do not use street-side mail collection boxes. Can transmit same as SECRET information.

SECRET – US. Postal Service Express Mail or U.S. Postal Service Registered Mail. Do not use street-side mail collection boxes. Can transmit same as TOP SECRET information.

TOP SECRET – Preferred method is person to person. If not possible, use the Defense Courier Service or an authorized government agency courier service, a designated courier or escort with Top Secret clearance, or electronic means over approved communications systems. The U.S. Postal system is not authorized for Top Secret information.

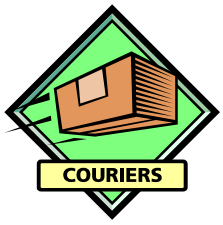
MAILING TO AREAS OUTSIDE THE U.S.

If outside the 50 United States, the District of Columbia, the Commonwealth of Puerto Rico, or a U.S. possession or trust territory, you must use one of the following methods for transmission:

a. Same as Top Secret;

b. U.S. register mail through Military Postal Service facilities may be used to transmit Secret and Confidential information provided that the information does not at any time pass out of U.S. citizen control nor pass through a foreign postal system.

HANDCARRYING CLASSIFIED INFORMATION



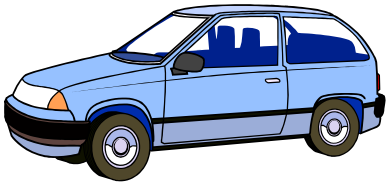
Regardless of your mode of transportation, you must have a **courier letter** or card issued to you by the USDA Security Office. Your responsibilities include:

Arranging for storage of the classified material at the destination site.

Properly wrapping and labeling your package.

Notifying the airlines in advance so they are expecting you with the package. This precludes you from having to open the package.

You must keep the package with you at all times. You must go directly to your destination. Do not stop to visit, shop, etc. If you must take stop for a break, take the package with you. Under no circumstances are you to leave the package in a hotel, automobile, plane, or taxi unattended.



The Hotel Safe is NOT proper storage for classified information!

WHO CAN ACCESS CLASSIFIED INFORMATION?

Only those individuals who have a Security Clearance equal to the level of the information you wish to share and they must have a need-to-know.

Hosting a Classified Meeting? You must:

a. Schedule the meeting in a room approved for the classification level of the meeting.

b. Inform all invitees that they must have a US government security clearance equivalent or higher than the classification of the meeting.

c. Visitors must request their security office to forward their security clearances to a USDA security office through a visit request. A visit request cannot be handcarried to a meeting because it can be tampered with or fake.

d. Contractors must have their company send their personnel security clearances and they should have a contract number and proof that they have a need-to-know for the information. In some cases, proof can be a DD 254 (Contract Security Classification Specifications) of a contract identifying the mission and type of classified information within the performance of their contract.

SANCTIONS

ISOO – Responsibility of having OCA is a privilege and not to be considered a right. As a result, ISOO oversees agency actions to ensure compliance with the EO and it's implementing directives. If ISOO finds a violation of the EO and it's implementing directives, the violation is reported to the head of that agency or senior agency official to take corrective actions.

SANCTIONS:

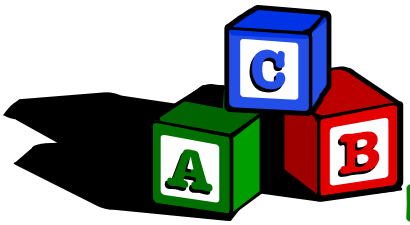
Reprimand
Suspension without Pay
Loss or Denial of Access to Classified Information
Other Sanctions as defined by USDA or Law

RESPONSIBILITY: The agency head, senior agency official, or supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards. Appropriate, prompt action must be taken when a security violation or infraction occurs. Report to ISOO when classified information is disclosed to unauthorized persons, when classifying information has been inappropriately classified, or when an agency or individual fails to declassify information at the appropriate time.

WHAT ARE THE LIMITATIONS?

Reclassification: Information that was previously declassified and released to the public can now be reclassified. An agency head must determine in writing that the reclassification of information is necessary in the interest of national security. If considering reclassification you need to ask yourself if the information can be reasonably recovered. If the information can be recovered, will the reclassification create a heightened attention to the information? The Information Security Oversight Office must be notified.

Information that has never been previously disclosed to the public under proper authority may be classified or reclassified after an agency has received a request for it under the Freedom of Information Act or Privacy Act, or a mandatory review is required. This can be done on a document-by-document basis and in accordance with EO 12958.



DEFINITIONS

Automatic Declassification – the declassification of information based solely upon:

a. the occurrence of a specific date or event as determined by the OCA.

b. the expiration of a maximum time frame for duration of classification established under EO 12958.

Classification Guidance – any instruction or source that prescribes the classification of specific information.

Classification Guide – a documentary form of classification guidance issued by an OCA that identifies the elements of information regarding a specific subject that must be classified and establishes the level and duration of classification for each such element.

Damage to National Security – harm to the national defense or foreign relations of the United States from the unauthorized disclosure of information, taking into consideration such aspects of the information as the sensitivity, value, utility, and provenance of that information.

Declassification – classified information that no longer meets the standards for classification under EO 12958, has it's classification removed and is then considered unclassified. This does not constitute automatic public release. This is done using the security classification guidance published by the OCA or by an authorized declassification authority.

Declassification Authority – can be either the OCA, the OCA's successor, a supervisory official of the OCA or successor, or an official

delegated as having declassification authority in writing by the agency head (i.e. OCA).

Derivative Classification – information derivatively classified on the basis of source documents or classifications guides. Already classified information restated, paraphrased, or regenerated in a new form. Examples of a new form could be video, cassette, CD Rom, diskette, research, inspection, or audit report.

Document – is any recorded information, regardless of the nature of the medium or the method or circumstances of recording.

Downgrading – changing the classification from a higher level of classification to a lower level of classification (i.e. Secret to Confidential).

Foreign Government Information – information provided to the U.S. government or information produced by the U.S. government pursuant to or as a result of a joint arrangement with a foreign government.

Infraction – knowing, willful, or negligent action contrary to the requirements of the EO or its implementing directives that does not constitute a "violation". An example would be to not sign off on a form as closing a security cabinet. Administrative in nature.

ISOO – Information Security Oversight Office - This office was formed within the National Archives and the Director of ISOO is approved by the President. They have oversight for the protection of national security classified information within all federal government agencies. They publish the implementing directives to the Executive Order 12958.

Mandatory Declassification Review – the review for declassification of classified information in response to a request for declassification that meets the requirements under section 3.5 of the EO.

National Security – the national defense or foreign relations of the United States.

"Original Classification Authority with jurisdiction over the information" includes:

a. The official who authorized the original classification, if that official is still serving in the same position.

b. The originator's current successor in function;

c. The supervisory official of either; or

d. The senior agency official under Executive Order 12958 (the Order)

Self-Inspection – the internal review and evaluation of individual agency activities and the agency as a whole with respect to the implementation of the program established under the EO and its implementing directives.

Senior Agency Official – the official designated by the agency head to direct and administer the agency's program under which information is classified, safeguarded, and declassified.

Special Access Program – a program established for a specific class of classified information that imposes safeguarding and access requirements that exceed those normally required for classified information at the same level.

Systematic Declassification Review – a review for declassification of classified information contained in records that have been determined by the Archivist to have permanent historical value in accordance with title 44, United States Code.

Unauthorized Disclosure – a communication or physical transfer of classified information to an unauthorized recipient.

Violation – knowing, willful, or negligent action that:

a. could reasonably be expected to result in an unauthorized disclosure of classified information;

b. results in classifying or continuing to classify information contrary to the EO or its implementing directives; or

c. results in the unauthorized creation of a special access program.