U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL MANUAL	Number: 3440-001
SUBJECT: Classification, Declassification, and Safeguarding Classified Information	DATE: August 10, 1983
	OPI: Security and Employee Relations Staff, Office of Personnel

1 PURPOSE

This Manual provides a coordinated and uniform USDA policy in the classification, declassification, and safeguarding of national security or classified information. The regulations and procedures apply to all classified material in the custody of USDA regardless of whether the material was originated within USDA or released to it.

2 DESCRIPTION OF MANUAL

The Manual reprints material from 7 CFR Part 10, 48 FR 11404, March 18, 1983, and also provides supplemental procedures to be followed within the Department. Material that is reprinted from the Code of Federal Regulations and the Federal Register is preceded by an asterisk (*) in the left hand margin and concludes with the notation "* (REG)".

3 AUTHORITY

This Manual is published pursuant to the requirements of Executive Order 12356 and the Information Security Oversight Office Directive relating to national security information.

4 SPECIAL INSTRUCTIONS/CANCELLATIONS

Form AD-976 (June 1981), Regulations for Classification, Declassification, and Safeguarding Classified Information is hereby rescinded.

5 AVAILABILITY

Copies of this Manual should be maintained in each office involved with classified material. Requests for copies of this Manual should be on AD-14, Request for Supplies, Forms, and/or Publications, and submitted to USDA, Office of Operations Warehouse, 3702 Ironwood Place, Landover, Maryland, 20785.

Chapter 1

General Provisions

101 FOREWORD

The interests of the United States and its citizens are best served by making information regarding the affairs of Government readily available to the public. This concept of an informed citizenry is reflected in the Freedom of Information Act, the Privacy Act, and in the current public information policies of the executive branch as prescribed in Executive Order 12356.

Within the Federal Government, however, there is certain classified material and information which, because it bears directly on the effectiveness of our national security and the conduct of our foreign relations, must be safeguarded for the security of the United States and the safety of our people and our allies. To protect against actions hostile to the United States, of both an overt and covert nature, it is our duty, both as USDA employees and as citizens, that such classified material and information be given only limited dissemination. Such classified material and information is expressly exempted from mandatory public disclosure by Section 552(b) (1) of Title 5, United States Code.

To insure that such classified material and information is safeguarded, but only to the extent and for such period as is necessary, this Manual identifies the material to be safeguarded, prescribes classification, downgrading, declassification, and safeguarding procedures to be followed, and establishes a monitoring system to insure its effectiveness.

102 SCOPE

All employees of USDA, including individuals serving in an advisory or consultative capacity, are subject to the regulations and procedures set forth herein. Failure on the part of the employees of USDA to observe these regulations constitutes grounds for disciplinary action, including dismissal. USDA personnel entrusted with classified material and information furnished by a foreign government or by international organizations of Governments are cautioned to contact the Department Security Officer for details concerning specialized security requirements.

103 DEFINITIONS

1. The following definitions have been published in 7 CFR Part 10 dated March 18, 1983.

   (a) Order means Executive Order 12356.

   (b) USDA Agency means a major line or program unit of the Department headed by an Administrator or equivalent who

reports to the Secretary, Deputy Secretary, Under Secretary, or Assistant Secretary.

(c) Agency includes any executive department, military department, intelligence agency, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency.

(d) USDA Agency Head means the Administrator or the Chief Executive Officer of a USDA Agency in the Department.

(e) Original Classification means the initial determination by a United States Government employee who has or had original classification authority pursuant to the Order or predecessor Orders, that information owned by, produced for or by, or under the control of the United States Government requires protection against unauthorized disclosure and is so designated.

(f) Classification Guide means a document issued by an authorized original classifier that prescribes the level of classification and appropriate declassification instructions for specified information to be classified on a derivative basis.

(g) Derivative Classification means that information used in a new document is in substance the same information currently classified in a source document or classification guide. The extracted information used in the new document must be classified at the same level as in the source document.

(h) Multiple Sources means the term used to indicate that a document is derivatively classified when it contains classified information derived from more than one source.

(i) Intelligence Activity means an activity that an agency within the intelligence Community is authorized to conduct pursuant to Executive Order 12333.

(j) Unauthorized Disclosure means a communication or physical transfer of classified information to an unauthorized recipient. *(REG)

2 Additional definitions are as follows:

(a) Access means the ability and opportunity to obtain knowledge or possession of classified information. An individual does not have access to classified information merely by being in a place where information is kept. Access is restricted by a determination of a need-to-know and a determination of trustworthiness.

(b) Agency Classified Material Control Officer is the Security Officer of an Agency in the National

Headquarters.

(c) Authorized Individuals are those persons who have a need-to-know for the classified information involved, and who have been determined to be trustworthy by the Department Security Officer based on the results of an appropriate investigation.

(d) Classifier means for USDA an individual who makes a derivative classification determination and applies a security classification to official information. A USDA classifier may assign a derivative security classification based either on a properly classified source or a classification guide received from the Department which originally classified the information.

(e) Clearance means an administrative determination under the provisions of DPM 732 by competent authority that an individual has been adjudged eligible for access to classified information of a specified category.

(f) Compromise means a breach of security which results from an unauthorized person obtaining knowledge of classified information. Affected material is not automatically declassified.

(g) COSMIC is a special marking which indicates that the information is the property of NATO and subject to special security controls.

(h) Custodian is an individual who has possession or is otherwise charged with the responsibility for safeguarding and accounting for classified material.

(i) Declassification means a determination that classified information no longer requires, in the interest of national security, a degree of protection against unauthorized disclosure, coupled with a removal or cancellation of the classification.

(j) Disclosure means an officially authorized release or dissemination by competent authority whereby the information is furnished to a specific individual, group, or activity.

(k) Disseminate means to furnish classified material under continued control of the U.S. Government to persons having a proper clearance and a "need-to-know" e.g. to another U.S. Government agency or Department or to a contractor.

(l) Documents means any recorded information regardless of its physical form or characteristics including, but not limited to, the following: All written material, whether handwritten, printed, or typed; and painted, drawn, or engraved material; all sound or voice recordings; all printed photographs and exposed or printed film, still or

motion pictures; and all reproduction of the foregoing, by whatever process reproduced.

(m) Downgrade means to determine that classified information requires, in the interest of national security, a lower degree of protection against unauthorized disclosure than currently provided, coupled with a changing of the classification designation to reflect such lower degree.

(n) Foreign Government Information is (a) information provided to the United States by a foreign government or international organization of governments in the expectation, expressed or implied, that the information is to be kept in confidence; or (b) information produced by the United States pursuant to a written joint arrangement with a foreign government or international organization or governments requiring that either the information or the arrangement, or both, be kept in confidence.

(o) Formerly Restricted Data is information removed from the Restricted Data category upon determination jointly by the Department of Energy (or antecedent agencies) and the Department of Defense that such information relates primarily to the military utilization of atomic weapons and that such information can be adequately safeguarded as classified defense information. Such information is treated the same as Restricted Data for purposes of foreign dissemination.

(p) For Official Use Only (FOUO) is an administrative marking applied to official information which requires protection in accordance with statutory requirements or in the public interest, but which is not within the purview of the rules for safeguarding information in the interest of national security. Such information is not within the purview of this Manual.

(q) Industrial Security means that portion of the industrial security program which is concerned with the protection of classified information in the possession of U.S. industry.

(r) Information Security means safeguarding information against unauthorized disclosure, or, the result of any system of administrative policies and procedures for identifying, controlling, and protecting such information from unauthorized disclosure, the protection of which is authorized by Executive Order or Statute.

(s) Inventory is a procedure employed to verify accountability of classified material by comparing entries on a register against the document of entry on the record of destruction of a signed receipt.

(t) National Security is the national defense and foreign relations of the United States.

(u) NATO Classified Information is the term applied to all classified information circulated within and by NATO whether such information originates in the organization itself or is received from member nations or from their international organizations.

(v) Need-to-know is a term given to the requirement that the dissemination of classified information be limited strictly to those persons whose official or other governmental duties require knowledge or possession thereof. No person is entitled to knowledge or possession of classified information solely by virtue of his/her grade, office, or security clearance. Responsibility for determining whether a person's duties require that he/she is authorized to receive it rests upon each individual who has possession, knowledge, or control of the information involved and not upon the prospective recipient. This principle is applicable whether the prospective recipient is an individual, a contractor, another Federal agency, or a foreign government.

(w) Official Information is information which is owned by, produced by, or is subject for the control of the United States Government.

(x) Restricted Data is that data which is defined in Section 11(y) of the Atomic Energy Act of 1954, as amended as "all data concerning: (1) Design, manufacture or utilization of atomic weapons, (2) the production of special nuclear material, or (3) the use of special nuclear material in the production of energy, but to include data declassified or removal from RESTRICTED DATA Category pursuant to Section 142."

(y) Unauthorized Person is any person not authorized access to specific classified information, irrespective of that person's eligibility for such access (e.g., possession of an appropriate clearance).

Chapter 2

Implementation, Oversight, and Safeguard Responsibilities Concerning Classified Information

201 DEPARTMENT RESPONSIBILITY

* The Order requires that each agency originating or handling classified information shall designate a senior official to direct and administer its information security program. Within the Department, the Assistant Secretary for Administration has the responsibility for the information security program. As such, the Assistant Secretary for Administration has delegated primary responsibility for providing guidance, oversight, and developing procedures governing the Department information security programs to the Department Security Officer.

1. Assistant Secretary for Administration

   He/She has the following responsibilities:

   (a) Establish and monitor policies and procedures within the Department to prevent unauthorized classification, as well as under derivative classification, to protect against unauthorized disclosure of properly classified information, and to ensure timely declassification of Department documents which no longer require protection, in accordance with the provisions of the Order.

   (b) Oversee that a security education program for employees handling classified information is implemented and maintained.

   (c) Provide to the Secretary of Agriculture any necessary guidelines concerning derivative classification, originated information that may warrant classification, and declassification.

   (d) Chair the Department Review Committee which shall have authority to act on all suggestions and complaints with respect to the Department's administration of the Order.

2. Department Review Committee

   (a) The Department Review Committee is responsible for the following functions:

      (1) Provide assistance and advice to the Assistant Secretary for Administration in carrying out his/her responsibilities concerning implementation and administration of the Order, Information Security Oversight Office Directives.

      (2) Review all appeals of requests for records under the provisions of Mandatory Review for Declassification (Section 3.4 of the Order) when the proposed denial

is based on their continued classification under the Order.

(3) Recommend to the Secretary of Agriculture appropriate administrative sanctions to correct abuse or violation of any provision of the Order, Information Security Oversight Office Directives, or this regulation.

(b) Members of the Department Review Committee shall consist of:

(1) Assistant Secretary for Administration (Chairperson)

(2) Director of Personnel

(3) Department Security Officer,

(4) Appropriate USDA Agency Head

(5) Head of the Unit subordinate to the USDA Agency Head, who has a working knowledge of the subject matter or information under consideration. *(REG)

3. Department Security Officer

The Department Security Officer has the responsibility to plan and direct the Department-wide administration of these regulations. He/She is responsible for the development, supervision, and administration of Department security programs concerning National Security Information including the promulgation of Department-wide policy and procedures and auditing for compliance with security directives and regulations. He/She shall assure that active training and orientation programs are maintained for employees concerned with classified information. He/She shall provide information or reports to the Information Security Oversight Office in accordance with Section 5.2. of the Order.

1. Agency Head - Each agency head is directly responsible for safeguarding all classified material within his/her jurisdiction and control. He/She must initiate and supervise measures of instruction necessary to insure effective control at all times in line with Department policy and regulations. He/She must also insure that any employee who must have access to such classified material in pursuit of his/her position is appropriately cleared prior to assignment to the position. An agency head may delegate authority to perform security control functions charged to him/her, but he/she may not delegate his/her assigned responsibility. Security is a responsibility of leadership.

2. Agency Classified Material Control Officer

(a) The head of each agency shall designated a responsible employee of the agency to serve as the Agency Classified

Material Control Officer. He/She will be responsible to the agency head for maintaining adequate facilities, procedures, and controls for safeguarding classified material coming within the custody of the agency. He/She is also responsible for maintaining an active program of orientation and training to keep employees informed concerning these regulations, and to impress upon them their individual responsibility for exercising vigilance and care in safeguarding classified material.

(b) Each Classified Material Control Officer shall maintain a current record of all employee in his/her agency who have been cleared and authorized to have access to classified material. This Officer shall promptly advise the Department Security Officer when one of these employee leaves the service of his/her agency.

(c) The loss or compromise of classified material or information shall be promptly reported to the Department Security Officer.

(d) Neither the Classified Material Control Officer nor any other employee, regardless of grade or position, shall advise other agencies or establishments outside the Department concerning the level of security clearance of an employee. Such information will be furnished by the Department Security Officer.

3. USDA Field Offices and Installation - Employees in charge of field offices and installations are responsible for insuring the adequate protection of classified material in the possession of their respective offices and installations, including component activities geographically located apart from the parent office or installation, in accordance with the provisions set forth in this Manual.

203 EMPLOYEE RESPONSIBILITY

1. Each supervisor of a USDA division, office or other organizational unit to which classified material is entrusted will be responsible for insuring that:

(a) All such material is provided adequate safeguarding at all times and under all circumstances.

(b) Each USDA employee under his/her supervisor and or each non-USDA employee present is adequately instructed in and fully complies with all of the pertinent provisions of this Manual and such other requirements as may be established by the Classified Material Control Officer.

2. Each USDA employee who has reasons to believe that:

(a) A practice of condition exists which fails to provide for adequate safeguarding of any classified material will report the circumstances promptly to his/her immediate supervisor.

(b) The loss of compromise of classified material or information will be promptly reported to the Agency Classified Material Control Officer or the Department Security Officer.

3. Each USDA employee to whom classified material has been entrusted will:

(a) Follow each procedure established by his/her Agency Classified Material Control Officer for the purpose of preventing unauthorized access to classified material.

(b) Be responsible for insuring that the material in his/her possession or custody is kept in approved security storage equipment.

(c) Prior to giving a prospective recipient access to classified material or information, insure that he/she has both:

(1) A security clearance to at least the same category of classification as the-material or information involved; and

(2) a valid need-to-know in connection with his/her official duties.

(d) Prior to termination of employment or contemplated temporary separation for a sixty-day period or more, or reassignment to a non sensitive position within the Department, be briefed concerning his/her obligations with regard to maintaining security of classified national security information obtained during his/her service in the Department, and to bring to his/her attention the applicable statutory requirements in this connection. He/She shall be required to read and execute Form AD-491 "Security Debriefing Secrecy Agreement" in the presence of the Agency Classified Material Control Officer. He/She should be required, at that time, to surrender or account for any classified material in his/her personal possession or custody.

Chapter 3

Classification of National Security Information

301 CLASSIFICATION LEVELS

* 1. Only three (3) levels of classification are authorized: "Top Secret," "Secret," and 'Confidential."

(a) Top Secret. Information may be classified "Top Secret" if its unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to the national security.

(b) Secret. Information may be classified "Secret" if its unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

(c) Confidential. Information may be classified "Confidential" if its unauthorized disclosure could reasonably be expected to cause damage to the national security. *(REG)

2. Limitations on Classification

(a) Information shall not be classified (originally or derivatively) unless its disclosure reasonably could be expected to cause damage to the national security. Information shall not be classified 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.

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

3. Foreign Government Information

Foreign government information shall retain its original classification or if clarification is required, be assigned a United States classification designation which will insure a degree of protection equivalent to that required by the entity that furnished the information. In such a situation, the USDA Agency shall consult the Department Security Officer for guidance. Classification markings assigned by the USDA Agency shall be marked on the foreign government information in accordance with the provisions of Section 305-3(d) of this Manual.

408 MANDATORY REVIEW FOR DERIVATIVELY CLASSIFIED INFORMATION

1. Requests for mandatory review for USDA derivatively classified documents shall be processed by the Department Security Officer under the following procedures:

(a) The Department Security Officer shall contact the Agency responsible for originally classifying the source document for a declassification determination.

(b) If the agency determines that the originally classified document has been declassified, the Department Security Officer shall so mark the USDA derivatively classified document and release it to the requester.

(c) If the originally classified document will not be declassified, the Department Security Officer shall so notify the requester.

409 APPEALS

* 1. Appeals from denial of declassification and release of information shall be directed to the Department Review Committee, Administration Building, U.S. Department of Agriculture, Washington, D.C. 20250. The Committee shall determine whether all or part of the information should be declassified and released.

2. Appeals shall be reviewed and decided within thirty (30) working days of their receipt as follows:

(a) If the documents are declassified in their entirety, the Department Security Officer shall forward the documents to the requester.

(b)(1) If the documents are not declassified and released in their entirety, the Chairman, Department Review Committee, shall forward a letter of denial to the requester notifying the requester of the decision and a statement of justification for the denial.

(b)(2) If the decision of the Committee is to declassify and release a portion of the documents, the Chairman of the Committee shall forward a letter of partial denial to the requester. The letter shall include a statement of justification for the partial denial. Those portions of the documents which have been declassified shall be forwarded to the requester. *(REG)

Chapter 5

Access, Dissemination, and Accountability of Classified Information

501 GENERAL POLICY

Access to classified information or dissemination of classified information, orally, in writing, or by any other means, shall be limited to those persons whose official duties require knowledge or possession thereof.

No person has a right to have access to classified information solely by virtue of position, grade, or security clearance.

Information classified pursuant to this Order or predecessor orders shall be afforded a level of protection against unauthorized disclosure commensurate with its level of classification.

502 GUIDELINES FOR ACCESS TO CLASSIFIED INFORMATION

(a) Determination of Need-to-know. Classified information shall be disseminate to a person only when the holder of the classified information establishes in each instance, except as provided in Section 4.3 of the Order, that access is essential for the receiver of the classified information to accomplish his/her official Government duties.

(b) Determination of Trustworthiness. USDA employees are eligible for access to classified information after a determination of trustworthiness by the Department Security Officer based upon appropriate levels of security investigations in accordance with applicable Executive Orders, Department Regulations, and other appropriate directives.

503 DISSEMINATION RESTRICTIONS

1. Classified Information Originated by Another Agency Except as provided by directives issued by the President through the National Security Council, USDA personnel shall not disseminate classified information originated by another agency outside the Department without the consent of the originating agency.

2. USDA,Originated Classified Information USDA originated classified information under predecessor orders shall not be disseminated outside the Executive Branch unless the receiving agency can ensure that the information shall be safeguarded equivalent to that afforded within the Department. USDA personnel considering such dissemination shall consult with the Department Security Officer prior to the release of classified information by providing the propriety of the dissemination in the interest of the national security and the recipient's security clearance status and need-to-know.

504 ACCESS BY HISTORICAL RESEARCHERS AND FORMER PRESIDENTIAL APPOINTEES

1. The requirement in Section 4.1(a) of the Order that access to classified information may be granted only as is essential to the accomplishment of authorized and lawful Government purposes may be waived for persons who:

   (a) are engaged in historical research projects, or

   (b) have previously occupied policy-making positions to which they were appointed by the President.

2. All persons receiving access pursuant to this subparagraph must have been determined to be trustworthy by the Department Security Officer as a precondition before receiving access. Such determination shall be based on such investigation as the Department Security Officer deems appropriate.

3. Historical researchers and former Presidential appointees shall not have access to foreign government information without the written permission from appropriate authority of the foreign government concerned.

4. Waivers of the "need-to-know" requirement under this subparagraph may be granted by the Department Security Officer provided that the Head of the USDA Agency with classification jurisdiction over the information being sought:

   (a) makes a written determination that access is consistent with the interests of national security;

   (b) maintains custody of the classified information at a Department facility;

   (c) obtains the recipient's written and signed agreement to safeguard the information in accordance with the provisions of this Manual, and to authorize a review of any notes and manuscript for determination that no classified information is contained therein; and

   (d) limits the access granted to former Presidential appointees to items that the appointees originated, reviewed, signed, or received as a Presidential appointee and insures that such appointee does not remove or cause to be removed any classified information reviewed.

505 DISSEMINATION TO THE CONGRESS

Provided other Departmental policies and procedures regarding legislative affairs are met, classified information may be disseminated to the Congress when necessary in the interest of the national security with the authorization of the Secretary. As used herein, the Congress includes members, committees, subcommittees, and staffs of members and committees.

506 DISSEMINATION TO GENERAL ACCOUNTING OFFICE (GAO) REPRESENTATIVES

1. Properly cleared and identified representatives of GAO may be granted access on a need-to-know basis to USDA classified information by the Head of each USDA Agency when such information is relevant to the performance of GAO statutory responsibilities and duties. The GAO will announce in advance to the visited agency the purpose of the visit, names of GAO representatives, and if access to classified information is anticipated, a certification as to the level of clearance of each representative.

2. Requests for the following types of classified information shall be forwarded to the Head of each Agency, who shall consult with the Department Security Officer for determination of whether or not the information is relevant to the performance of GAO's statutory responsibilities and for authorization for release of access to:

   (a) Top Secret information.

   (b) Other sensitive classified information falling in the general areas of intelligence, and communications security.

   (c) Classified information originated by another department or agency of the Executive Branch, including FBI reports.

3. When classified information is furnished to GAO representatives, they shall be informed of the classified nature of the information and of the need for safeguarding it properly. In this way, the Comptroller General has agreed to establish a security system at least equal to that prescribed by the Executive Branch.

507 DISSEMINATION TO THE JUDICIARY

Any USDA employee or organization receiving an order or subpoena from a Federal or State court to produce national security information for litigative purposes shall contact the Department Security Officer and the Office of the General Counsel in order that coordinated efforts can be enacted to properly safeguard such information.

508 DISSEMINATION OF CLASSIFIED INFORMATION THROUGH MEETINGS AT USDA SITES

USDA personnel responsible for arranging or hosting a classified conference, committee meeting (policy or technical), or scientific and technical gathering are also responsible for instituting procedures that assure that security measures appropriate to the occasion are taken. The responsible person(s) shall:

1. Positively identify each attendee and insure that each attendee has been authorized access to information of equal or higher classification than the information to be disclosed.

2. Assure that unauthorized persons, which includes any media representatives, are not permitted into the meeting room, area, or auditorium. If necessary, USDA cleared personnel shall be posted at each entrance to prevent unauthorized persons from attending the meeting.

3. Insure that the area in which classified information is to be discussed affords adequate acoustical security against unauthorized disclosure.

4. Control and safeguard any classified document furnished to the attendees and retrieve the material or obtain receipts as required.

5. Advise speakers or persons who present classified information of any limitations on their presentations. Such limitations may be necessary due to the level of clearance and/or need-to-know of certain attendees.

509 DISSEMINATION BY TELEPHONE CONVERSATIONS

Classified information shall not be discussed over nonsecure telephones. Classified telephone conversations are authorized over approved secure communication circuits. Contact the Department Security Officer for information concerning use of secure telephones in appropriate situations.

510 ACCOUNTABILITY AND CONTROL OF CLASSIFIED MATERIAL

1. Material Subject to Accountability.

(a) All Top Secret and Secret material received by a USDA Agency shall be immediately registered by a designated Accountability Records Clerk in the office of the recipient agency. Such registering process shall require the use of a Register of Classified Documents and shall reflect the recording of:

(1) control number

(2) level of classification

(3) date received

(4) title or description of the document

(5) number of copies (if any)

(6) originator and date of the document

(7) disposition and date

(b) Responsible office heads shall determine accountability procedures for internal control of Confidential material. The volume of documents handled and personnel resources

available must be considered in determining the level of security measures enacted while at the same time maintaining efficiency.

2. Recording Individual Access to Top Secret Documents

The name and title of all individuals, including clerical personnel, to whom information in Top Secret documents has been disclosed, and the date of such disclosure, shall be recorded. A sheet of paper permanently attached to the classified document may be used as a disclosure record for these purposes. Such records shall be retained for two years after the document concerned is transferred, downgraded, or destroyed.

3. Control of Secret and Confidential Information

(a) Receipts. Since the FAS mailroom receives the vast majority of classified material sent to the Department, FAS-170 form (Classified Material Control and Receipt) is primarily used for internal transmittal and accountability of material classified Secret or Confidential from FAS to other USDA Agencies. A Classified Material Control Receipt (AD-471) may also be used. FAS mailroom personnel retain a carbon copy of the form FAS-170 until the recipient USDA Agency returns the classified document to FAS for destruction or rerouting.

(b) Secret material shall be controlled by a chain of receipts covering each individual who receives custody within USDA Agencies. Either receipt form may be used for such purposes. This process is in addition to the use of a Register of Classified Documents by each recipient office. Responsible office heads shall determine administrative procedures required for the internal control of Confidential material.

4. Reproduction Controls

(a) Top Secret and Secret documents shall not be reproduced without the consent of the originator. The name of the agency and authorizing official shall be made a matter of record in the subject file or Register of Classified Documents.

(b) Unless restricted by the originating agency, Confidential documents may be reproduced to the extent required by operational needs. Efforts should be made to limit the number of copies reproduced.

(c) Reproduced copies of classified documents shall be subject to the same accountability and controls as the original documents.

(d) Paragraphs (a) and (b) of this section shall not restrict the reproduction of documents to facilitate review for declassification.

(e) Any reproduction of classified documents shall be limited for use only within the Department.

5. Employee's Control of Classified Information

(a) Whenever classified information is in actual use or in the immediate work area of an employee authorized to possess it, the material shall be:

(1) kept under continuing control and supervision by the employee,

(2) covered, turned face down, placed in a security storage container, or otherwise adequately protected whenever an unauthorized person enters the immediate work area;

(3) secured in a security storage container as soon as practicable after use, while absent from the general work area, and at the end of each business day.

(b) Classified Document Cover Sheets

Classified document cover sheets (Top Secret Cover Sheet, SF 703; Secret Cover Sheet, SF 704; Confidential Cover Sheet, SF 705) shall be used during times of inner office coordination and review in order to alert personnel that a document is classified and to protect the document from unauthorized scrutiny. Such cover sheets shall be removed prior to transmission outside the Department or destruction, The use of cover sheets should assist personnel in identifying classified documents in their immediate work area and prevent inadvertent nonsecuring of documents when departing the work area either during the work day or at the close of business.

Agencies may obtain copies of cover sheet standard forms by ordering from the Landover Forms warehouse. The standard form number and title of each form is as follows:

SF 703 - Top Secret Cover Sheet
SF 704 - Secret Cover Sheet
SF 705 - Confidential Cover Sheet ### 9/30/86)

(c) Miscellaneous Items. Drafts, carbon sheets, notes, and worksheets containing Classified information must be given the same classification and safeguarding in the same manner as the classified information they contain or shredded by either the preparer or the Agency Classified Material Control Officer.

Chapter 6

Storage of Classified Material

601 POLICY

1. Classified material may be used, held, or stored only where there are facilities or under conditions adequate to prevent unauthorized persons from gaining access to it. The exact nature of security requirements will depend on a thorough security evaluation of local conditions and circumstances. They must allow the accomplishment of essential functions while affording classified material reasonable and appropriate degrees of security, with a minimum of risk. The requirements specified in this Manual represent the minimum acceptable standards.

2. Funds, weapons, medical items, or other items of intrinsic value shall not be stored in containers along with classified material.

602 STANDARDS FOR STORAGE EQUIPMENT

The General Services Administration (GSA) establishes and publishes minimum uniform standards, specifications, and supply schedules for security containers and related security devices suitable for storage and safeguarding of classified material throughout the Government. Whenever it becomes necessary to obtain or purchase new security storage safes or containers, it shall be, to the maximum extent practicable, of the type designated as such on the Federal Supply Schedule of GSA.

603 STORAGE OF VARIOUS CATEGORIES OF CLASSIFIED MATERIAL

1. Whenever classified material is not under the personal control of an authorized and properly cleared person, it shall be stored in a locked security container as prescribed below:

   (a) Top Secret and Secret Material. Too Secret and Secret material shall be stored in a safe or safe-type steel file container with an approved, built-in, three-position, dial-type changeable combination lock or in a vault protected by an alarm system and/or response force. All corridor doors of a room where Top Secret and Secret material is stored shall be locked when the room is unoccupied.

   (b) Confidential Material - Confidential material may be stored in a manner authorized for Top Secret and Secret material or in a steel filing cabinet equipped with a steel lock bar, provided it is secured by a GSA approved changeable combination padlock. Where Confidential material is stored, all corridor doors should be locked when the room is unoccupied.

(c) Storage of Classified Cryptographic Material - Classified cryptographic information will be stored in conformity with requirements established by the Department Security Officer on a case-by-case basis.

(d) Storage of Restricted Data and Formerly Restricted Data Restricted data and formerly restricted data will be stored in conformity with requirements of paragraph (a) or (b) as appropriate for the specific level of security classification on the material itself.

(e) Storage of Hazardous or Bulky Classified Material - When, due to its nature or size, it is hazardous or otherwise impractical to store classified material in accordance with the usual requirements, the material will be stored within a controlled area which has been specifically approved for this purpose by the Department Security Officer. To insure continuity of safeguarding, such material will be removed from the controlled area only under conditions specifically approved by the Department Security Officer.

(f) Storage of Classified Waste and Reproduction Materials - Pending actual destruction, all waste and reproduction materials which contain classified information will be stored in conformity with the requirements of paragraphs (a) and (b), as appropriate, for the specific level of security classification of the information involved.

(g) Storage of Material Marked Limited Official Use (LOU) - Officially limited information is important, delicate, sensitive or proprietary information which is provided to this Department usually by the Department of State offices, both domestic and from embassies or posts in foreign countries. Information marked LOU is not classified information under the criteria of the Order, but its use and distribution must be restricted to officials who have a need to know. Information so marked shall be handled, safeguarded, and stored in a manner equivalent to information classified CONFIDENTIAL.

604 CHANGING COMBINATIONS TO SECURITY CONTAINERS

1. Equipment in Service. Combinations to security containers shall be changed only by individuals having an appropriate security clearance and who know how to correctly change such combinations. Combinations shall be changed when:

(a) the container is placed in use;

(b) a person knowing the combination no longer requires or is authorized access to classified information stored in the container;

(c) the combination or record of combination has been subject to compromise;

(d) it has not been changed in a year;

(e) the container is taken out of service.

2. Equipment Out of Service. When security equipment is taken out of service, it shall be inspected to ensure that no classified material remains. The built-in combination lock shall be reset to the standard combination (50-25-50). Combination padlocks shall be reset to the standard combination (10-20-30).

3. Security Container Signs. Security containers used for the storage of classified material shall not be left unattended until it has been locked by an authorized person and checked by a second person. Reversible "Open-closed" magnetic signs, available through normal supply channels shall be prominently displayed on such equipment as a reminder of its security status to responsible persons. Each security container will have attached conspicuously a "safe or security cabinet record" form on which an authorized person will record the date and time each day that they initially unlock and finally lock the container, followed by their initials. when a second person is available, the "checked by" column of the form shall be annotated to reflect that the container has been checked to ensure it has been locked.

4. Classification of Combinations (Security Container Information SF 700)

(a) Records of the combination of a lock used for the storage of classified information shall be afforded protection equal to that given the highest level of the classified information stored therein. Combinations shall be memorized and/or recorded on SF 700, Security Container Information, and properly stored in a security container, Each office shall establish procedures for the secure maintenance of an annotated SF 700.

(b) Standard Form 700 shall also be used to show the location of each container, date combination changed, name and signature of person who changed the combination, and the name, name address and home telephone number of the person(s) to be contacted if the container is found open and unattended by an authorized person.

*605 CLOSE OF BUSINESS INSPECTION OF WORK AREA

1. Activity Security Checklist SF 701

(a) Designated personnel working in a work area entrusted with classified information will systematically inspect their respective work areas at the close of each business day to ensure that all classified information is properly stored and that all security containers are adequately secured. Activity Security Checklist SF 701 provides a systematic means for each work area to conduct a close of business security inspection and to allow for employee accountability in the event that security irregularities

are discovered. If any storage equipment, controlled area, or classified material is found not to be protected in accordance with the requirements of this Manual, the Department Security Officer will be notified and corrective action taken in compliance with such procedures as he/she may establish.

(b) Standard Form 701 shall be destroyed at the end of each monthly use. Standard Form 701 forms can be ordered from the Landover Forms Warehouse.

2. Security Container Check Sheet SF 702

(a) Standard Form 702, Security Container Check Sheet, shall be placed on each container in which classified information is stored to record each time the container is opened and closed, by whom, and a closing check.

(b) Standard Form 702 shall be destroyed at the end of each monthly use. Standard Form 702 forms can be ordered from the Landover Forms Warehouse. ### 9/30/86)

Chapter 7

Transmission of Classified Information and Material

701 PREPARATION AND RECEIPTING

1. Outside the Department

   (a) Classified material being prepared for transmission outside the Department shall be prepared in the following manner:

      (1) The material will be securely enclosed in sealed, opaque inner and outer envelopes of sufficient strength to withstand rough handling.

      (2) The inner envelope shall be plainly marked with the highest classification of the classified material, and addresses of both sender and addressee.

      (3) The outer envelope will be addressed with no indication of the classification of its contents and reflect the return address of the sender.

      (4) A Classified Material Control Receipt (AD-471) shall be completed and enclosed in the inner envelope. The receipt shall identify the sender, addressee, and the document, but shall not contain classified information. The sender shall trace the whereabouts of the receipt if not returned by the recipient within a reasonable timeframe.

   (b) Whenever, due to its nature, weight, or size, classified material cannot be prepared for transmission as indicated in this paragraph, the preparer shall contact the Department Security Officer for guidance.

2. Within the Department

   (a) Within the Department, classified material may be transmitted between offices or agencies by direct contact of the officials concerned and/or by use of a single sealed opaque envelope with no security classification category marked on the outside of the envelope. The complete addresses of both the sender and the recipient shall be shown on the envelope. In addition the notice "To Be Opened By Addressee Only" shall be typed on the front of the envelope. In lieu of receipts, Registers of Classified Documents shall be annotated by each office concerned to reflect the internal transmission for Secret or Confidential material.

   (b) Classified material shall never be delivered to unoccupied rooms or offices.

702 TRANSMISSION OF TOP SECRET MATERIAL AND INFORMATION

Transmission of Top Secret material and information shall be effected only by:

(a) Authorized and cleared messenger-courier services approved by the Department Security Officer;

(b) The Department of State courier system;

(c) The Armed Forces courier Service;

(d) Cleared and designated Department employee traveling on a conveyance owned, controlled or chartered by the Government;

(e) Cleared and designated Department employees traveling by surface transportation;

(f) Cleared and designated Department employees traveling on scheduled commercial aircraft within and between the United States, its territories, and Canada;

(g) A cryptographic communication system authorized by the Director, National Security Agency.

703 TRANSMISSION OF SECRET AND CONFIDENTIAL MATERIAL AND INFORMATION

Transmission of Secret and Confidential material and information shall be effected by:

(a) Any of the means approved for the transmission of Top Secret material and information;

(b) United States Postal Service registered mail with registered mail receipt within and between the 50 states, the District of Columbia, and Puerto Rico;

(c) United States Postal Service registered mail with registered mail receipt through DOD Postal Service facilities outside the 50 States, the District of Columbia, and Puerto Rico, provided that the material does not at any time pass out of United States citizen control and does not pass through a foreign postal system or any foreign inspection;

(d) United States Postal Service and Canadian registered mail with registered mail receipt between United States Government and Canadian government installations in the United States and Canada;

(e) Government and Government contract vehicles including aircraft, ships of the United States Navy, civil service operated United States Naval ships, and ships of the United States registry when these carries are under appropriately cleared escort personnel. Appropriately cleared operators of vehicles, officers of ships or pilots of aircraft who are United States citizens may be designated as escorts provided the control of the carriers is maintained on a 24 hour basis.

704 HANDCARRYING OF CLASSIFIED INFORMATION IN TRAVEL STATUS

1. General Provisions. Personnel in travel status shall handcarry classified material domestically or across international boundaries only in exceptional circumstances. In each instance, a determination shall be made on a case-by-case basis by the responsible agency division chief that it is necessary for the appropriately cleared traveler to handcarry classified material. Whenever possible, classified material shall be transmitted by other authorized means to the location being visited.

2. Specific Safeguards. If it is determined that the handcarrying of classified materia by an individual in travel status is in the best interests of the Government, and there are no other authorized means available to accomplish operational objectives in a timely manner, the following safeguards shall be provided for:

   (a) Classified material shall be in the physical possession of the traveler. Handcarrying of material on trips that involve an overnight stopover is not permissible without advance arrangements for proper overnight storage in a Government installation. Classified material shall not be stored in a hotel room or safe, locked in automobiles, private residences, or vehicle detachable storage compartments.

   (b) Classified material shall not be read, studied, displayed, or used in any manner in public conveyances or places.

   (c) The traveler shall maintain in his/her possession a written Department authorization memorandum, cosigned by the appropriate division chief and the Department Security Officer, authorizing the transportation of classified material. This authorization memorandum together with official travel orders should, in most instances, permit the traveler to pass through any customs without the need for subjecting the classified material to inspection. If difficulty is encountered, the traveler should tactfully refuse to exhibit the classified material to customs inspection and should insist on the help of the local United States diplomatic representative at the port of entry or departure.

   (d) The material shall be inventoried by the traveler's office prior to departure and a record copy retained for accounting purposes when the traveler returns to his/her office.

   (e) When the traveler completes the visit, he/she shall arrange to have the classified material returned to his/her office by approved means. Returned material shall be checked against the office record copy retained for accounting purposes. If any classified material is left with the office being visited, the traveler shall

obtain a receipt.

(f) Travelers authorized to carry classified material shall be informed of the provisions of this section prior to departure from their duty office.

Chapter 8

Disposal and Destruction of Classified Information

801 POLICY

1. Classified information no longer needed in current working files or for reference or record purposes shall be destroyed by burning or shredding in the presence of designated or authorized persons. The method of destruction must preclude recognition or reconstruction of the classified information. Surplus material should be destroyed as soon as practicable to prevent an unnecessary accumulation of classified material.

2. All classified material, including waste and reproduction materials containing classified information, shall be safeguarded as prescribed in this Manual for the specific category of security classification involved until the material is actually disposed of or destroyed.

3. The provisions of this Chapter apply generally to the routine disposition or destruction of classified material. When a particular document contains specific instructions to the contrary, however, those specific instructions shall be followed.

4. When doubt exists as to the propriety of destroying classified material received from another Federal department or agency, the material shall be returned to, or permission to destroy the material obtained from, that department or agency.

5. Approval of Use of Shredding Equipment

   Prior to obtaining shredding equipment, agency management services personnel should check with the Department Security Officer to ensure that the equipment being considered meets destruction standards.

6. Destruction By Burning. Any classified information to be destroyed by burning shall be torn and placed in burnbags which shall be clearly labeled "Burn." Burnbags awaiting destruction shall be safeguarded commensurate with the classification of the information contained in the bags.

802 TOP SECRET INFORMATION

Top Secret information shall be disposed of either by returning the information to the originating agency or delivery to the Department Security Officer for destruction.

803 CLASSIFIED CRYPTOGRAPHIC INFORMATION

Material embodying classified cryptographic information shall be delivered to the Management Services Division, Foreign Agricultural Service, for destruction.

804 RECORDS OF DESTRUCTION

1. Records of destruction are required for Top Secret and Secret information and shall be dated and signed by two personnel witnessing actual destruction. Records of destruction shall contain the identification of the document(s) destroyed, the method of destruction used, the time and place of destruction, the reason for destruction, and the names of the destroying person and witness. Such records shall be retained by the Agency for two years from the date of destruction.

2. All holders of classified information are authorized to destroy such information when appropriate to do so. Any witness to the destruction must possess a security clearance at the same or higher level than the classification of the information being destroyed.

Chapter 9

Security Violations and Administrative Sanctions

901 VIOLATIONS SUBJECT TO SANCTIONS

1. Officials and employees of the Department are subject to appropriate administrative sanctions if they:

   (a) Knowingly and willfully classify or continue the classification of information in violation of Executive Order 12356, any implementing directive, or this regulation;

   (b) Knowingly, willfully and without authorization disclose information classified under the Order, prior Orders, or compromise classified information through negligence; or

   (c) Knowingly and willfully violate any other provision of the Order, any implementing directives, or this regulation.

2. Sanctions include but are not limited to warning notices, reprimands, suspension or termination of security clearance and as permitted by law, suspension without pay, or removal. Sanctions shall be imposed upon any person subject to these regulations and determined responsible for a violation specified under this chapter by the appropriate Department or Agency official upon consultation with the Department Security Officer. In cases involving the compromise of classified information, the FBI and Office of the U.S. Attorney shall be consulted regarding possible violation of criminal statutes.

902 REPORTING SECURITY VIOLATIONS

Any person subject to these regulations who has knowledge of a violation pursuant to section 901 (including the known or suspected loss or compromise of classified information) shall promptly report the circumstances to the Department Security Officer. The Department Security Officer shall take the following action:

1. Prompt notification to the originating agency, if appropriate.

2. Prepare a written report for the Agency Personnel Director which shall include the date the violation occurred; the date of the discovery of the violation; specific identification of the information involved; the classification and/or any caveats regarding the information; probability of loss or compromise; assessment of damage incurred from a national security viewpoint; corrective measures taken, the person(s) responsible for the violation; and recommended administrative, disciplinary, or legal action which should be taken.

903 CORRECTIVE ACTION

The Department Security Officer shall ensure that appropriate and

prompt remedial action is taken whenever a violation of Section 901 occurs or repeated administrative discrepancies or repeated disregard of requirements of this regulation occurs. Liaison with all other agencies involved will be conducted when such violations occur.

904 ACTION REQUIRED FOR COMPROMISE OF CLASSIFIED NATO INFORMATION

In the event that a USDA Agency reports a possible loss or compromise of classified NATO information, the Department Security Officer shall submit an initial report of the incident to the United States Security Authority for NATO Affairs (USSA) and shall initiate an investigation in accordance with the provision of USSA instructions.

Chapter 10

Security Education Program

1001 RESPONSIBILITY AND PURPOSE

All USDA employees who hold security clearances and occupy critical or noncritical sensitive positions do not require access to classified information. Those USDA employees who are entrusted with classified information must be made aware of their responsibilities. Each Agency Classified Material Control Officer shall establish a security education program to indoctrinate employees involved with classified information in their security responsibilities and their responsibilities for familiarizing themselves with and adhering to the provisions of this regulation.

1002 SCOPE AND PRINCIPLES

1. The security education program shall include all USDA personnel entrusted with classified information regardless of their position or grade. Emphasis must be placed on the achievement of the real goals of the program. Each program shall include at a minimum the following:

   (a) Advise employees of the need for protecting classified information, the adverse effects to the national security that could result from unauthorized disclosure, and their personal responsibility for safeguarding classified information in their possession.

   (b) Indoctrinate employees fully in the principles, criteria, and procedures for derivative classification, downgrading and declassification, including appropriate marking, of the information as prescribed in this Manual. Employees should be alerted to the strict prohibitions on improper use and abuses of the classification and declassification systems.

   (c) Familiarize employees with the specific security requirements of their particular assignment.

   (d) Inform employees of their responsibility to report any suspicious act that may be considered an attempt by foreign intelligence agents to obtain classified information.

   (e) Advise employees of the hazards involved and the strict prohibitions against discussing classified information over the telephone, or in such a manner as to be intercepted or overheard by unauthorized persons.

   (f) Inform employees that disciplinary actions may result from violation, neglect, or disregard of Executive Order 12356 and any implementing directives of this Manual.

   (g) Instruct employees that prior to disseminating classified

information, they must determine that the prospective recipient (1) has been cleared for access, (2) needs the information in order to perform his/her official duties, and (3) can properly protect (or store) the information.

2. When indoctrinating employees assigned to duties requiring access to classified information, the Agency Classified Material Control Officer should utilize this Manual and the Department Security Officer's memorandum dated March 2, 1981, Subject: "Security Responsibilities For All Employees Cleared to Handle Defense Classified Information Vital to National Security."

1003 FOREIGN TRAVEL BRIEFINGS

Employees, whether they have or have not had access to classified information, shall be given a "foreign travel briefing" as a defensive measure prior to travel to Russia and the Peoples Republic of China (PRC). Employees who frequently travel to the two countries need not be briefed for each such occasion. A thorough briefing at least once each six months shall suffice.

1004 DEBRIEFINGS

Upon termination of employment at USDA or reassignment to USDA duties designated nonsensitive, employees shall be debriefed by the Agency Classified Material Control Officer or an agency employee designated by him/her. The affected employee shall return all classified material and shall execute a Security Debriefing Secrecy Agreement (AD-491) which shall be forwarded to the Department Security Officer.

1005 EMERGENCY PLANNING

Each USDA Agency and the Office of the Secretary shall develop plans for the protection, removal, or destruction of classified material in case of fire, natural disaster, or civil disobedience in the United States. USDA personnel assigned to U.S. Embassies in foreign nations shall consult the Resident Security Officer for guidance and Embassy procedures for the disposition of classified material in emergency situations.

Chapter 11

Executive Branch Oversight and Policy

1101 NATIONAL SECURITY COUNCIL

Pursuant to the provisions of the Order, the National Security Council shall provide overall policy direction for the information security programs.

1102 ADMINISTRATOR OF GENERAL SERVICES

The Administrator of General Services is responsible for implementing and monitoring the information security program established pursuant to the Order. In accordance with the Order, this responsibility has been delegated to the Director of the Information Security Oversight Office.

1103 FUNCTIONS OF THE DIRECTOR OF THE ISOO

1. The Director of the ISOO is charged with the following principal functions which pertain to USDA:

   (a) Oversee USDA actions to ensure compliance with Executive Order 12356 and implementing directives.

   (b) Consider and take action on complaints and suggestions from persons within or outside the Government with respect to the administration of the information security program, including appeals from decisions on declassification requests.

   (c) Report annually to the President through the Administrator of General Services and the National Security Council on the implementation of the Order.

   (d) Review all USDA implementing regulations and guidelines for systematic declassification review. The Director may require any regulation or guideline to be charged if it is not consistent with the Order or implementing directive. Any such decision by the Director may be appealed to the National Security Council.

   (e) Conduct on-site reviews of the information security program of each USDA Agency that handles classified information and to require of the Department such reports, information, and other cooperation as necessary to fulfil the Director's responsibilities.

   (f) Review any request for original classification authority and, if deemed appropriate, recommend Presidential approval.

(g) Has the authority to prescribe, after consultation with the Department Security Officer, standard forms that will promote the implementation of the information security program.

(h) Has the authority to convene and chair interagency meetings to discuss matters pertaining to the information security program.

Appendix A

THIS SAMPLE MEMORANDUM DOES NOT CONTAIN CLASSIFIED INFORMATION CONFIDENTIAL (1)/

SUBJECT: Minimum Required Markings for Classified Documents (u)(2)/

TO: All Executive Branch Agencies

(6)/(c) Each portion of a classified document shall be marked to indicate the highest classification of information it contains. (For example, this paragraph is marked as if it contained information at the CONFIDENTIAL level).

(u) The bracketed numbers on this page indicate those markings required for all classified documents. The footnotes refer to the appropriate paragraph of this manual.

(u) Other markings shall be applied to classified material depending on the content:

A document that does not contain classified information but is used to transmit classified material (Section 305-3(a))

A document that contains foreign government information (Section 305-3(d))

A document that contains information from sensitive intelligence sources and methods (Section 305-3(c))

Signature of Author
Title

(3)/ Derivatively Classified by (name of USDA employee)
(4)/ Derived from (identity of original classifier
(5)/ Declassify on (information from source document)

Footnotes

(1)/ Page Markings - Section 305-2(a)(2)
(2)/ Subjects and Titles - Section 305-2(a)(3)
(3)/ Identity of USDA classifier - Section 305-2(a)(4)
(4)/ Identity of Classifier of source document - Section 305-2(a)(4)
(5)/ Date/Event for declassification - Section 305-2(a)(4) and (5)
(6)/ Mandatory portion marking - Section 305-2(a)(3)