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

DEPARTMENTAL REGULATION	Number: 3440-2
SUBJECT: Control and Protection of "Sensitive Security Information"	**DATE:** January 30, 2003
	OPI: Personnel and Document Security Division of the Office of Procurement and Property Management

TABLE OF CONTENTS

1 PURPOSE

This regulation establishes U.S. Department of Agriculture (USDA) procedures for identifying unclassified but sensitive information and safeguarding it against unauthorized use or disclosure. The regulation includes minimum protection requirements, including the identification of unclassified but sensitive information as "Sensitive Security Information," and recommends additional security safeguards to be applied where warranted by the sensitivity of the information.

2 SPECIAL INSTRUCTIONS

This regulation applies to all organizational elements within USDA.

3 POLICY

It is the policy of USDA to safeguard unclassified but sensitive security information within its control. USDA will withhold from release sensitive information that is not appropriate for public disclosure consistent with laws, regulations and court decisions.

It is important to note that the Secretary of Agriculture is authorized to originally classify information as "Secret" by order of the President 67 FR 61465 (September 26, 2002). Therefore, if USDA originates documents that it believes should be classified, Departmental Administration (DA) should be notified as soon as possible.

Information must not be designated as Sensitive Security Information (SSI) to conceal violations of law; inefficiency; administrative error; prevent embarrassment to a person, organization, department or agency; or restrain competition.

4 REFERENCES

Computer Security Act of 1987, P.L. No. 1000-235, 101 Stat. 1724 (1988)

Office of Management and Budget Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources

Freedom of Information Act, 5 USC §552 (2000)

Executive Order 12958, Classified National Security Information, April 12, 1995

U.S. Attorney General's Memorandum for Heads of All Federal Departments and Agencies Regarding the Freedom of Information Act (October 12, 2001)

DM 3440-001 Classification, Declassification, and Safeguarding Classified Information,

DR 3440-001 Classification, Declassification, and Safeguarding Classified Information.

DR 3450-002 FOIA Implementing Regulations.

DR 3040-001 Electronic Records Management Program.

DR 3060-1 USDA Correspondence Management Regulation, Section 17, Handling of Restricted Information.

DR 3080-1 Records Disposition.

5 BACKGROUND

The need has arisen to establish formal guidance for all organizational elements outlining procedures for identifying, safeguarding, using, and maintaining the disposition of unclassified information that is considered sensitive security information, such as information pertaining to threats, vulnerabilities, and risks to homeland security and physical security at USDA facilities.

6 DEFINITIONS

a Critical Infrastructure means physical and cyber-based systems, assets (including information whether stored on paper, electronically, or using other means), and services essential to the government or economy of the United States or to a political subdivision thereof, including, but not limited to, systems, facilities, and stockpiles necessary for the operation, maintenance, or distribution of essential goods and services, such as telecommunications (including voice and data transmission and the Internet), electrical power, gas and oil storage, transportation, banking and finance, public health (including biological, chemical, radiological, and other hazardous materials), water supply, waste water, emergency services (including medical, fire, and police services), and the continuity of government operations;

b Sensitive Security Information means unclassified information of a sensitive nature, that if publicly disclosed could be expected to have a harmful impact on the security of Federal operations or assets, the public health or safety of the citizens of the United States or its residents, or the nation's long-term economic prosperity; and which describes, discusses, or reflects:

(1) The ability of any element of the critical infrastructure of the United States to resist intrusion, interference, compromise, theft, or incapacitation by either physical or computer-based attack or other similar conduct that violates Federal, State, or local law; harms interstate, international commerce of the United States; or, threatens public health or safety;

(2) Any currently viable assessment, projection, or estimate of the security vulnerability of any element of the critical infrastructure of the United States, specifically including, but not limited to vulnerability assessment, security testing, risk evaluation, risk-management planning, or risk audit;

(3) Any currently applicable operational problem or solution regarding the security of any element of the critical infrastructure of the United States, specifically including but not limited to the repair, recovery, redesign, reconstruction, relocation, insurance, and continuity of operations of any element;

(4) The following categories are provided for illustration purposes only as examples of the types of information (regardless of format) that may be categorized as SSI:

1 Physical security status of USDA laboratories, research centers, field facilities, etc., which may also contain vulnerabilities;

2 Investigative and analytical materials concerning information about physical security at USDA facilities such as the above-named facilities;

3 Information that could result in physical risk to individuals;

4 Information that could result in serious damage to critical facilities and/or infrastructures;

5 Cyber Security Information, which includes, but is not limited to:

(a) Network Drawings or Plans

(b) Program and System Security Plans

(c) Mission Critical and Sensitive Information Technology (IT) Systems and Applications

(d) Capital Planning and Investment Control Data (I-TIPS)

(e) IT Configuration Management Data and Libraries

(f) IT Restricted Space (Drawings, Plans and Equipment Specifications as well as actual space)

(g) Incident and Vulnerability Reports

(h) Risk Assessment Reports, Checklists, Trusted Facilities Manual and Security Users Guide

(i) Cyber Security Policy Guidance and Manual Chapters

c Need-to-know means a determination made by an authorized holder of SSI that a prospective recipient requires access to that SSI in order to perform or assist in a lawful and authorized governmental function.

7 ABBREVIATIONS

DA Departmental Administration
FOIA Freedom of Information Act
IT Information Technology

OCIO Office of the Chief Information Officer
OGC Office of the General Counsel
OIG Office of the Inspector General
PA Privacy Act
SSI Sensitive Security Information

8 RESPONSIBILITIES

a Under and Assistant Secretaries, Agency Administrators, Regional Directors, Office Directors, and Heads of Field Establishments, hereinafter called Departmental Organizations, will be responsible for the identification and designation of information that warrants protection of SSI.

b Heads of Departmental Organizations will:

(1) Specify the categories or types of information, which originate in their organization or are prepared for the use of their organization, and that are designated as SSI. The SSI label may be removed from information requested in a FOIA request, if a Departmental Organization Head determines that the information is no longer qualified under the definition provided. If the sensitivity of the information requires protection in excess of the minimum levels established in this order, the Departmental Organizational Head should ensure that all offices with custody of the information know and comply with such criteria. All Departmental Organizations that originate SSI are responsible for conducting reviews, in compliance with DR 3080-01, Records Disposition.

(2) Identify those subordinate officials who have authority to determine which information originating under their supervision or cognizance requires protection against unauthorized disclosure. The officials so designated are responsible for ensuring that personnel under their direction are aware of information that is considered SSI.

c Agencies and Staff Offices will:

(a) Issue directives, if needed, establishing criteria for identifying SSI responsibility within their organizations. All directives will have prior approval by DA before being finalized and approved.

(b) Ensure that adequate security measures and procedures are implemented to protect SSI.

(c) Ensure that employees of their organizations are aware of their responsibility to protect SSI.

(d) Conduct a risk analysis and determination to identify potential threats and appropriate vulnerabilities to SSI in their custody.

(e) Determine the potential harm resulting from the loss, misuse, or unauthorized access to or modification of SSI in their custody.

(f) Identify appropriate information and designate it as SSI.

(g) Ensure that prompt and appropriate disciplinary action is taken against personnel responsible for unauthorized disclosure of SSI.

d Departmental Administration will:

Monitor and ensure compliance with this DR and provide guidance regarding identification and protection of SSI.

e The Office of the Chief Information Officer will:

(a) Establish records management disposition policies and procedures to ensure that records designated as SSI are maintained and disposed of according to USDA and Agency records control schedules.

(b) Partner with DA to ensure wise use is made of existing department resources in terms of security points of contact, security awareness training, and emergency procedures.

(c) Establish USDA policy and standards for IT system protection. System protection functions include encryption, network security products, reliability and security of computing systems, and physical barriers. OCIO will conduct compliance reviews to ensure that policy and standards are being followed.

(d) Establish strategies and procedures to reconstitute and restore critical information technology infrastructures after serious disruptions. OCIO will establish programs for restoration of services that includes risk management and consequence management analysis studies and tools, system survivability technologies, back-up and recovery capabilities, and cold/hot site strategies and requirements.

f The Office of the General Counsel will:

Provide concurrence prior to responding to any initial FOIA request, Privacy Act (PA) request, or any other request for records involving SSI. Agencies and Staff Offices should continue to comply with 7 C.F.R. 1.14 with regard to obtaining OGC concurrence when FOIA or PA appeals are denied, but shall also obtain OGC concurrence on any administrative appeal, whether it is granted or denied, for records involving SSI.

9 FREEDOM OF INFORMATION ACT REQUESTS

FOIA requests for access to SSI should be processed as set forth in Section 8f and in accordance with USDA regulations and the Attorney General's FOIA Memorandum of October 12, 2001, with consideration of all applicable FOIA exemptions, including one or more of the following:

a FOIA Exemptions Potentially Applicable to SSI:

(1) For SSI pertaining to USDA operations or assets, FOIA Exemption 2 should be considered;

(2) For current SSI consisting of private sector or industry information submitted voluntarily to USDA that is customarily protected by the submitter, FOIA Exemption 4 should be considered;

(3) For any SSI the disclosure of which is banned by federal statute, FOIA Exemption 3 should be considered;, and

(4) For any SSI that consists of information compiled for law enforcement purposes, FOIA Exemption 7 should be considered.

10 IDENTIFICATION AND MARKING

USDA material which contains information that the head of the USDA organization has determined requires protection against unauthorized disclosure must be marked in a conspicuous manner with the following notice: "Sensitive Security Information - Disseminate on a Need-to-Know Basis Only." The identification of SSI will be done by:

a Marking of the SSI notice at the bottom of the front cover (if one is present), the title page (if one is present), the first page, and the outside of the back cover (if one is present);

b Marking of the SSI notice at the top and bottom of every page in a document that contains SSI;

c Individual portion markings at the beginning of a paragraph containing SSI shall be done using the acronym SSI;

d Notating in a cover memo;

e Transmittal documents that have no classified information attached but do have SSI attachments shall have the statement "Sensitive Security Information Attachment - Disseminate on Need-to-Know Basis Only" affixed;

f Electronically transmitted messages or data containing SSI shall be preceded by the term "Sensitive Security Information - Disseminate on a Need-to-Know Basis Only" at the beginning of the text;

g Inclusion in a category identified as SSI use in an organization directive and known to all personnel handling the information;

h All documents that are distributed externally of USDA shall bear the marking on all pages:

"This document contains information which may be exempt from mandatory disclosure under FOIA. Exemption(s) _____ apply.", and

i Any other method authorized by DA.

The purpose of identifying SSI is to ensure that all recipients of the material are aware that the information requires protection and should be disseminated on a need-to-know basis only. The identification method selected should have a minimal effect on the operational efficiency of the organization.

11 CUSTODY AND STORAGE

a Employees who have custody of material designated as SSI shall exercise due caution to ensure that the information is not available to individuals who have no requirement for it. At a minimum, individuals who cannot demonstrate a "need-to-know" must not be able to enter areas unescorted or unobserved, and have visual access to SSI.

b During non-duty hours, SSI shall be afforded, at a minimum, protection of storage in a locked desk or file cabinet, or storage in a facility or area using physical access control measures that afford adequate protection to prevent unauthorized access. The sensitivity of some SSI material may require a higher level of protection such as a safe with a combination lock.

c SSI stored and processed by an IT facility shall have adequate physical, administrative, and technical safeguards.

12 DISSEMINATION AND TRANSMISSION

a Information that has been identified and is known by the recipient as SSI shall be safeguarded from disclosure to unauthorized individuals whether or not the material is physically marked. Safeguarding from disclosure includes precautions against oral disclosure, prevention of visual access to the information and precautions against release of the material to unauthorized personnel.

b SSI leaving the control of the originating organization must be transmitted in a single brown envelope or in a wrapping properly sealed and addressed.

c SSI may be transmitted via any form of commercial shipping or U.S. Postal Service method.

d SSI may be discussed on the telephone; however, the ease of interception of telephone conversations dictates that discretion be used where the threat of interception exists. In the latter case, the use of voice privacy equipment or secure telephones should be considered.

e SSI should not be transmitted or discussed along unsecured pagers, wireless devices or telephone equipment. These devices are not inherently secure and require additional encryption capabilities before they can be used.

f SSI may be transmitted via unclassified fax machines. However, the sensitivity of the material will determine the need for more secure communications transmission (secure fax). In the latter case, if the holder is unaware of which method to use, DA or OCIO will provide guidance on the appropriate method of transmission via phone, fax, or IT.

g The Internet is <u>not secure</u> and therefore should not be used to transmit SSI. It is critical to safeguard and adequately protect SSI from unlawful or improper disclosure. OCIO will provide guidance on the appropriate methods of transmission.

h SSI that is distributed outside of the Department shall be accompanied by a letter stating that this material is to be treated with the same control measures comparable to the receiving agency's prescribed measures established comparable to SSI, that at a minimum meet our security control measures (Sensitive But Unclassified, Limited Official Use Only, For Official Use Only, etc.). In the absence of the recipient agency's internal security procedures for this level, a letter accompanying the document with appropriate control measures shall be provided.

13 RECORDS DISPOSITION

a Where appropriate, SSI may be destroyed by tearing into small pieces and discarding with other waste material. Material of higher sensitivity must be destroyed by shredding. The level of sensitivity of the material will be an integral element in determining the appropriate method of destruction. Small segments of microfiche and microfilm may be readable, therefore, destruction into very small particles or strips is necessary. DA shall provide guidance to all Departmental organizations on current security requirements for shredders, and other methods of destruction.

b IT storage media containing SSI data should be overwritten with nonsensitive data prior to release of the storage media. All data storage devices shall be rendered unreadable by approved methods such as degaussing, overwriting (6-7 times with random 1's and 0's) or complete physical destruction prior to disposal. OCIO shall provide guidance to all Departmental organizations on current IT security requirements for proper destruction of IT storage media. For more guidance please refer to DR 3040-01.

c Records that carry the SSI designation should be handled according to an approved USDA or Agency records control schedule governing the subject content of the record. If a record designated as SSI requires a longer or shorter retention period, the USDA or Agency records management officer must be contacted to obtain a new disposition for that record.

14 DURATION OF SSI PROTECTION

Information shall not remain protected as SSI when it ceases to meet the criteria established in sections 6.b of this regulation. Information ordinarily should remain protected as SSI for no longer than 10 years, unless a designating official makes a new determination that protection is warranted for a longer period.

15 CONTRACTOR PERSONNEL

If SSI must be released to non-government personnel as part of a contract or grant, the head of the USDA organization, in conjunction with DA, shall determine whether the sensitivity of the information justifies a requirement for an investigation of contractor personnel handling the sensitive information. The procurement document must include the contractor background information requirements and other security requirements of the contract. The Security Points of Contact in the respective USDA organizations shall determine the extent of the investigation required, ranging from a suitability determination to a request for clearance for national security, and develop the mandatory security requirements for the contract. The contractual security requirements shall be forwarded to DA for concurrence prior to submitting the solicitation document to the procurement office.

16 PROTECTION OF INFORMATION TECHNOLOGY (IT) ASSETS

a Security and the need to encrypt or otherwise protect SSI are commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information. This includes assuring that systems and applications used by an agency operate effectively and provides appropriate confidentiality, integrity, and availability through the use of cost-effective management, personnel, operational, and technical controls. This approach emphasizes a risk-based determination for cost-effective security on SSI.

b Information that is considered sensitive by a responsible authority, or determined to have a high value or information that represents a high risk should be cryptographically protected if it is vulnerable to unauthorized disclosure or undetected modification during transmission or while in storage.

c The use of personal home computers to store or transmit SSI is prohibited due to the high security risks in protecting sensitive information on non-government owned systems. Government-owned equipment will be issued and configured to maintain strong security protection appropriate to the highest level of information contained on the computer.

17 MATERIAL FROM OTHER DEPARTMENTS

A number of government agencies have issued regulations for protecting sensitive information using designations such as For Official Use Only or Sensitive But Unclassified. Sensitive material from other government agencies should be safeguarded from unauthorized disclosure in accordance with this Regulation or provided additional protection in accordance with the specific requirements of the agency providing the sensitive information.

Attachment A

Office of the Attorney General
Washington, D. C. 20530

October 12, 2001

MEMORANDUM FOR HEADS OF ALL FEDERAL DEPARTMENTS AND AGENCIES

FROM: John Ashcroft, Attorney General

SUBJECT: The Freedom of Information Act

As you know, the Department of Justice and this Administration are committed to full compliance with the Freedom of Information Act (FOIA), 5 U.S.C. § 552 (2000). It is only through a well-informed citizenry that the leaders of our nation remain accountable to the governed and the American people can be assured that neither fraud nor government waste is concealed.

The Department of Justice and this Administration are equally committed to protecting other fundamental values that are held by our society. Among them are safeguarding our national security, enhancing the effectiveness of our law enforcement agencies, protecting sensitive business information and, not least, preserving personal privacy.

Our citizens have a strong interest as well in a government that is fully functional and efficient. Congress and the courts have long recognized that certain legal privileges ensure candid and complete agency deliberations without fear that they will be made public. Other privileges ensure that lawyers' deliberations and communications are kept private. No leader can operate effectively without confidential advice and counsel. Exemption 5 of the FOIA, 5 U.S.C. § 552(b)(5), incorporates these privileges and the sound policies underlying them.

I encourage your agency to carefully consider the protection of all such values

and interests when making disclosure determinations under the FOIA. Any discretionary decision by your agency to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information.

In making these decisions, you should consult with the Department of Justice's Office of Information and Privacy when significant FOIA issues arise, as well as with our Civil Division on FOIA litigation matters. When you carefully consider FOIA requests and decide to withhold records, in whole or in part, you can be assured that the Department of Justice will defend your decisions unless they lack a sound legal basis or present an unwarranted risk of adverse impact on the ability of other agencies to protect other important records.

This memorandum supersedes the Department of Justice's FOIA Memorandum of October 4, 1993, and it likewise creates no substantive or procedural right enforceable at law.

Go to: DOJ FOIA Page // DOJ Home Page