



Information Security Overview

Classified National Security Programs Branch



This Presentation is **UNCLASSIFIED**



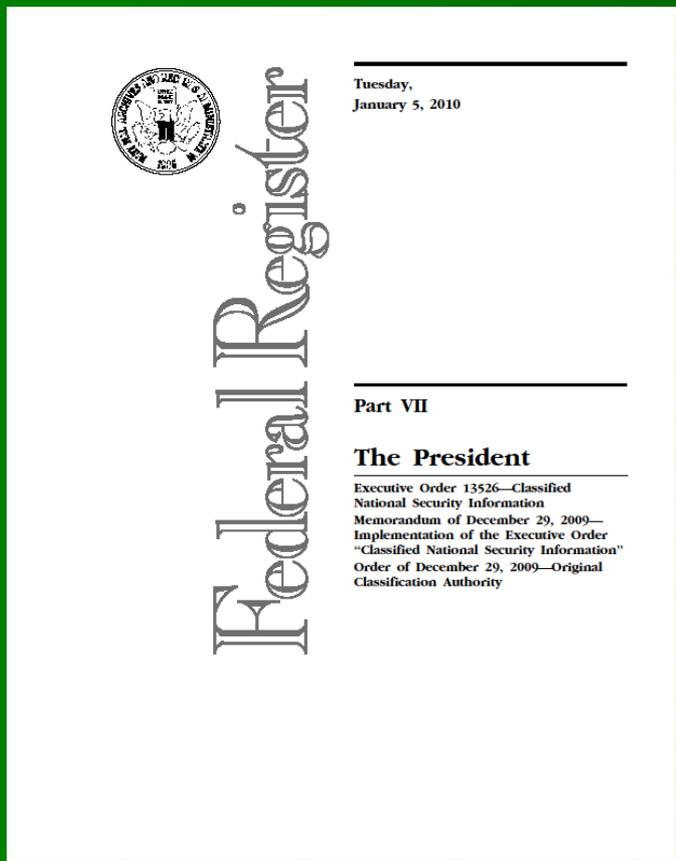
Overview

A security clearance is a privilege, not a right.

When you accept the privilege of access to Classified National Security Information, you are also accepting the *responsibilities* that accompany this privilege.



Executive Order 13526



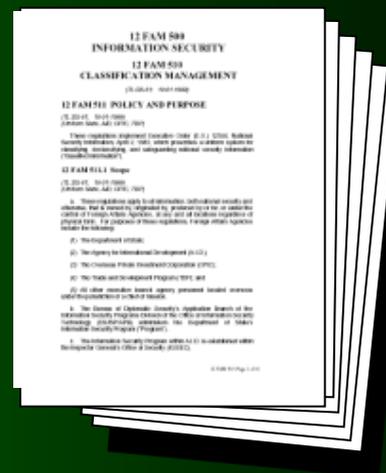
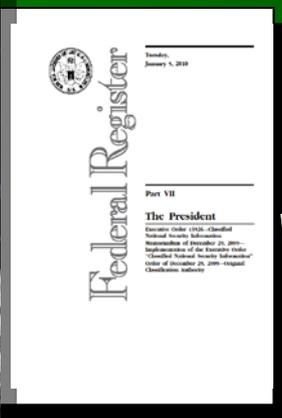
All government agencies and individuals with access to Classified National Security (classified) information, are bound by the basic rules and standards set forth for it's handling in Executive Order 13526, which is published in the Federal Register.



National Policy to Department Policy

E.O. 13526

DM 3440-001



DM 3440-001, USDA Classified National Security Information Program Manual is your basic reference for policy and is derived from E.O. 13526.



What is Classified Information?

Information is deemed “Classified” when it has been determined that the unauthorized disclosure of that information could be expected to cause some degree of damage to the national security and been designated a level of classification in order to protect it from such disclosure.



Classification Levels

There are only **THREE** levels of USG Classification

TOP SECRET

Exceptionally Grave Damage to the National Security

SECRET

Serious Damage to the National Security

CONFIDENTIAL

Damage to the National Security



Reasons for Classification

In accordance with E.O. 13526, information may only be classified if it involves one or more of the following categories:

- a. military plans, weapons systems, or operations;**
- b. foreign government information;**
- c. intelligence activities (including covert activities), intelligence sources or methods, or cryptology;**
- d. foreign relations or foreign activities of the United States, including confidential sources;**
- e. scientific, technological, or economic matters relating to the national security;**



Reasons for Classification (cont)

In accordance with E.O. 13526, information may only be classified if it involves one or more of the following categories (cont.):

- f. United States Government programs for safeguarding nuclear materials or facilities;**
- g. vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security;**
- h. The development, production, or use of weapons of mass destruction.**



Original Classification Authority

Original Classification Authority (OCA) means a proponent generates or creates classified information. Not all federal government agencies have this approval.

The Secretary of Agriculture was granted “OCA” on September 26, 2002 to the Secret level.



Marking Requirements

This sample document includes all essential markings required under E.O. 13526, including:

- ✓ Overall Classification Marking
- ✓ Portion marking
- ✓ A “Classified by” line that identifies the classifier by name and position
- ✓ A reason for classification
- ✓ A “Declassify on” line that provides for the automatic declassification of the document



SECRET

MEMORANDUM February 25, 2012

TO: John Q. Supervisor

FROM: Keith T. McElfresh

SUBJECT: Note How Subject Line is Also Portion Marked (U)

1. (U) Paragraph 1 contains only UNCLASSIFIED information and therefore bears a portion marking of “U” in parenthesis

2. (S) This paragraph contains information which is classified SECRET and is therefore parenthetically marked with the letter “S” to indicate that. It is also important to note that as this is the highest classification found in this document, the overall classification of the document is also SECRET.

3. (C) This paragraph contains CONFIDENTIAL information and is therefore parenthetically marked with the letter “C” to indicate that.

Classified By: Linda P. Manager
Office Director

Reason: 1.4 (a),(d)

Declassify On: 2020-05-24

SECRET



Derivative Classification Marking

USDA will primarily use derivative classification markings. The derivative classifier is responsible for carrying forward the classification and declassification instructions from the source document(s)

Example:

Derived From: Food Safety and Inspection Service (FSIS)

Food Products Security Report

Dated June 01, 2011

Declassify On: June 01, 2021



Declassification

All information classified must have provisions for automatic declassification. Declassification instructions are applied by the OCA or derived from source information. These instructions can typically be found in the classification instruction block.

**Derived From: USDA FSIS Report
Dated June 1, 2011
Declassify On: June 1, 2021**



SECRET

MEMORANDUM

January 3, 2012

TO: John Q. Supervisor

FROM: Keith T. McElfresh

SUBJECT: Note How Subject Line is Also Portion Marked (U)

1. (U) Paragraph 1 contains only UNCLASSIFIED information and therefore bears a portion marking of "U" in parenthesis
2. (S) This paragraph contains information which is classified SECRET and is therefore parenthetically marked with the letter "S" to indicate that. It is also important to note that as this is the highest classification found in this document, the overall classification of the document is also SECRET.
3. (C) This paragraph contains CONFIDENTIAL information and is therefore parenthetically marked with the letter "C" to indicate that.

Derived From: USDA FSIS Report
Dated June 1, 2011
Declassify On: June 1, 2021

SECRET



ISOO Marking Guide

Marking Classified National Security Information

As required by Executive Order 13526, Classified National Security Information,
December 29, 2009,
and
32 C.F.R. Part 2001, ISOO Implementing Directive, effective June 25, 2010



December 2010

**For detailed
information
regarding the proper
marking of classified
information, consult
ISOO's marking
guide.**

<http://www.archives.gov/isoo/training/marketing-booklet.pdf>



Sensitive Security Information (SSI)

Information that does not meet E.O. 13526 standards for classification but is not appropriate for public release due to privacy or operational concerns is referred to as Sensitive Security Information.

This includes many types of information including, but not limited to vulnerability assessments, security testing, risk evaluation, risk-management, etc.

- SSI is **NOT** a classification level -



SSI Categories (cont)

Physical Security

Laboratories, Research Centers;

Field Sites which may contain vulnerabilities.

Investigative and analytical materials.

Information that could result in physical risk to individuals.

Information that could result in damage to critical facilities.

Cyber Security Information

Network Drawings/Plans

Program/System Plans

Mission Critical/IT

Capital Planning/Investment Data

IT Configuration Mgt Data

IT Restricted Space Information

Incident/Vulnerability Reports

Risk Assessments/Checklists, etc.

Cyber Security Policies



Foreign Government Information

GEHEIM

**DEUTSCHE INDUSTRIE
NORMEN**

22 Februar 1998

GEHEIM

GEHEIM
SECRET

**DEUTSCHE INDUSTRIE
NORMEN**
(GERMAN INDUSTRIAL STANDARDS) (U)

22 Februar 1998

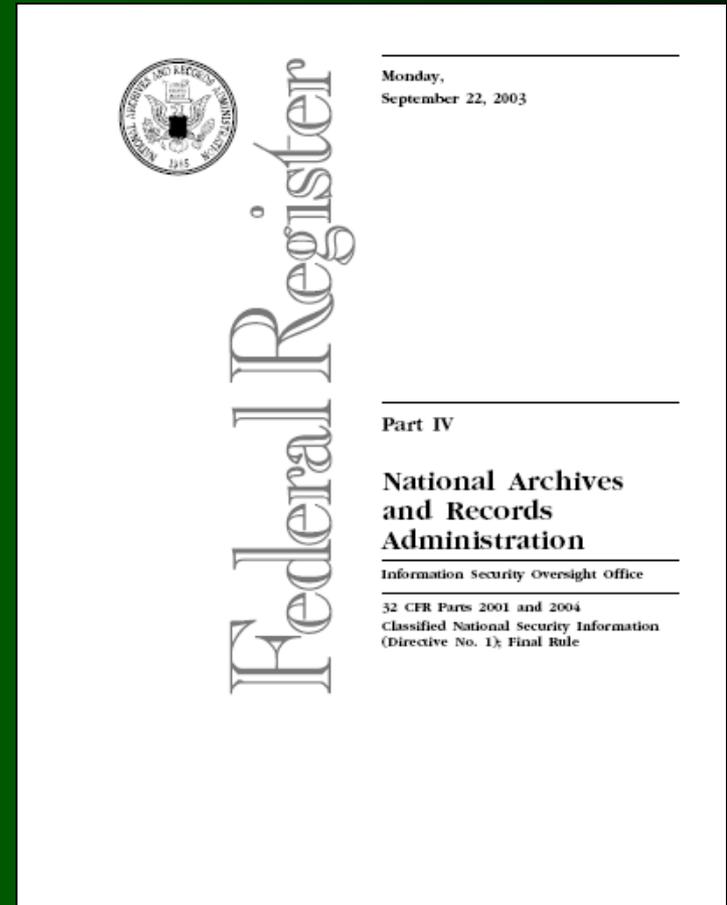
THIS DOCUMENT CONTAINS GERMAN
GOVERNMENT INFORMATION

SECRET
GEHEIM



Declassification

Guidance for the proper application of declassification standards and duration of classification can be found in E.O. 13526 and ISOO Directive #1.





Handling Requirements

NEED TO KNOW

A security clearance alone does not guarantee access to classified information. The individual must also have a bona fide need to know the information to accomplish their official duties.

Employees are responsible to ensure that they share classified information under their control only with individuals who have both the appropriate clearance, and a *genuine need to know*.



Handling Requirements

Classified information may **NEVER** be taken home

Classified information shall not be exposed in public in any capacity

- Classified information shall be properly double wrapped whenever it is moved in public
- Utilize cover sheets in high traffic or common areas
- Never read or process classified information on a public conveyance (e.g. buses, taxis, cars, planes, metro etc.)



Cover Sheets

TOP SECRET

Must have a TS cover sheet and access sheet permanently attached to it.

SECRET and CONFIDENTIAL

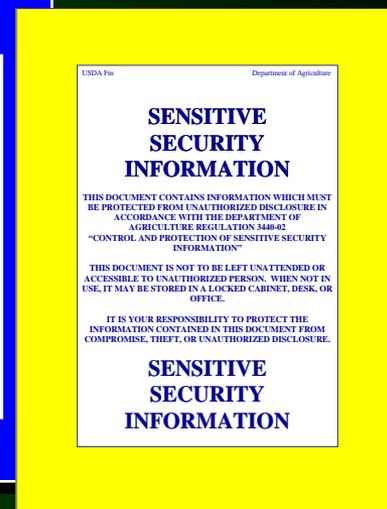
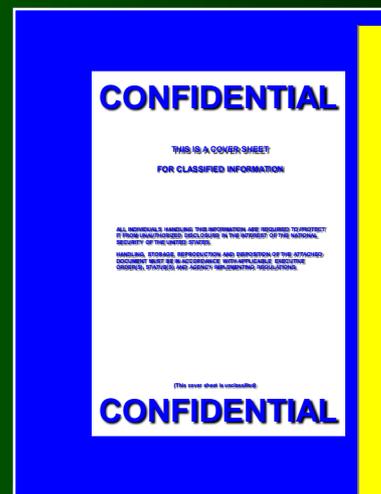
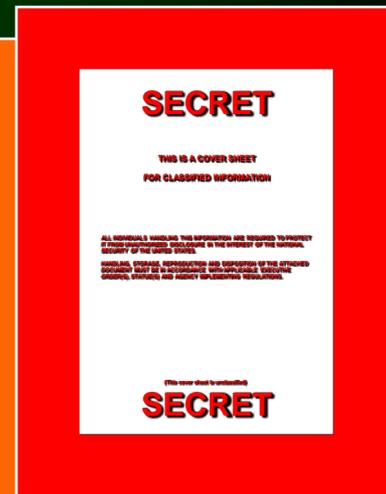
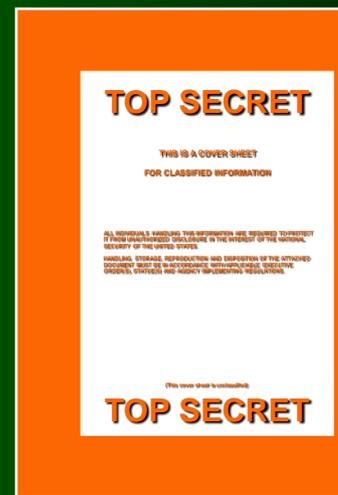
Whenever being transmitted via mail or courier.

Whenever being moved in public or a common area.

Whenever discretion requires it.

SENSITIVE SECURITY INFORMATION

As required

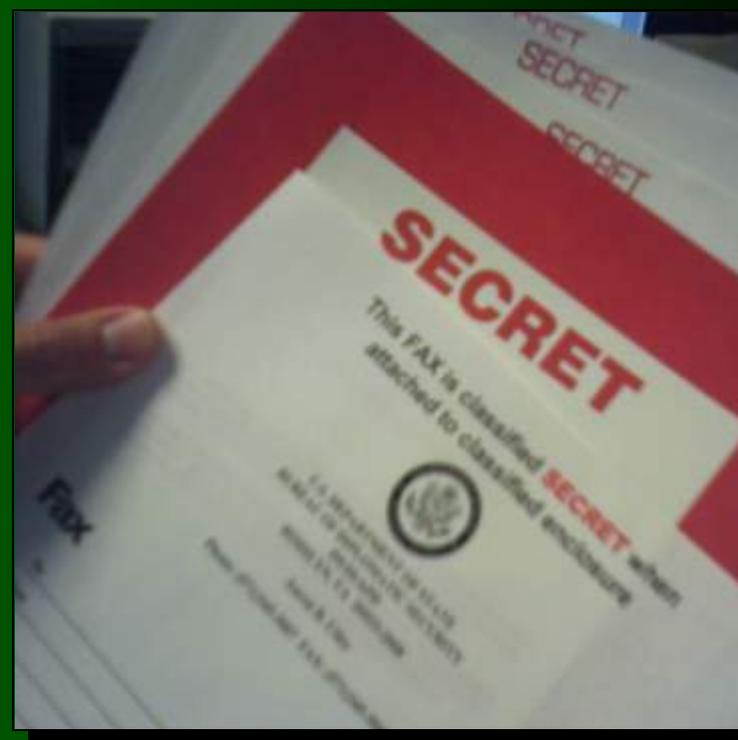




Additional Considerations

**Transmittal documents
(FAX covers, memo covers,
routing sheets etc.)**

- ✓ **Must be marked to indicate the classification of the information being transmitted.**
- ✓ **Unless the transmittal document itself contains classified information it must be marked to indicate that it is unclassified when separated from classified enclosure.**





Transmission Requirements

Classified information may only be transmitted via approved secure or encrypted methods. Ensure, not only, that the means of transmission (STE, courier, etc.) you intend to use is approved at the level you intend to process, but that you are properly instructed in the operation of any encrypting equipment that you may use.





Mailing/Transporting Classified Materials

TOP SECRET

Person to Person or DCS

SECRET

**Same as TS or Registered
Mail**

CONFIDENTIAL

Same as TS/Secret

Or

First Class Mail

****(Return Receipt provides name)***





Approved Domestic Carriers

Airborne Express

AirNet Systems

Associated Global Systems

Cavalier Logistics Management

CorTrans Logistics

DHL Airways

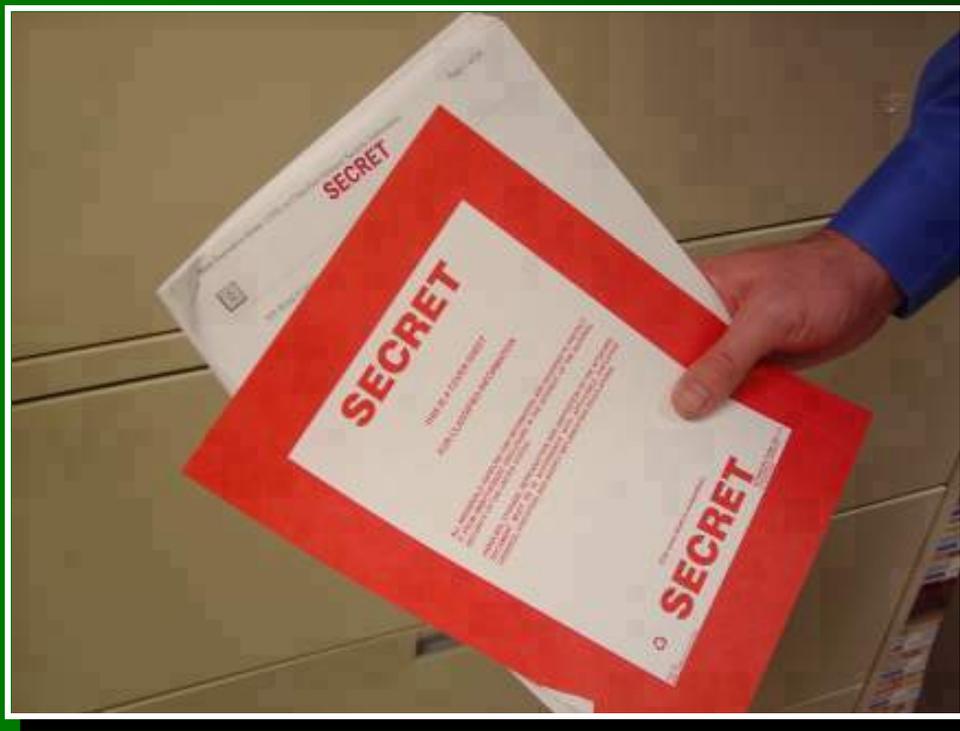
FedEx

Menlo Worldwide (formerly Emery)

UPS



Movement of Classified in HQ Building**



Ensure that any classified to be wrapped bears appropriate markings and a cover sheet.

****Please coordinate with your ISC if you are located at a field office.**



Double Wrapping



**Place marked classified material inside opaque envelope and seal.
This envelope is the “inner wrapping”.**



Double Wrapping



Tamper-proof the inner wrapping with tape. Ensure all envelope seams are sealed. There are many types of tape which are appropriate to this task (e.g. duct, packing, acrylic, etc.)



Double Wrapping



Tamper-proof the inner wrapping with tape. Ensure all envelope seams are sealed. There are many types of tape which are appropriate to this task (e.g. duct, packing, acrylic, etc.)



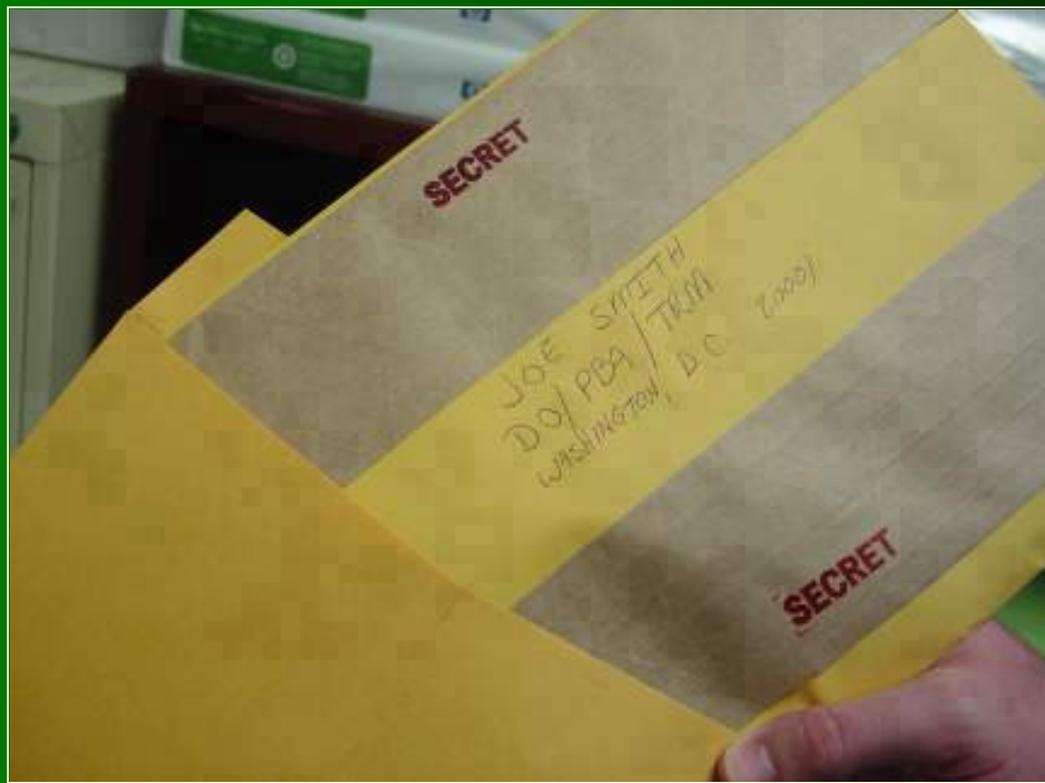
Double Wrapping



Affix appropriate marking to the inner wrapping. Markings should appear conspicuously on the top and bottom of both the front and back of the inner wrapping.



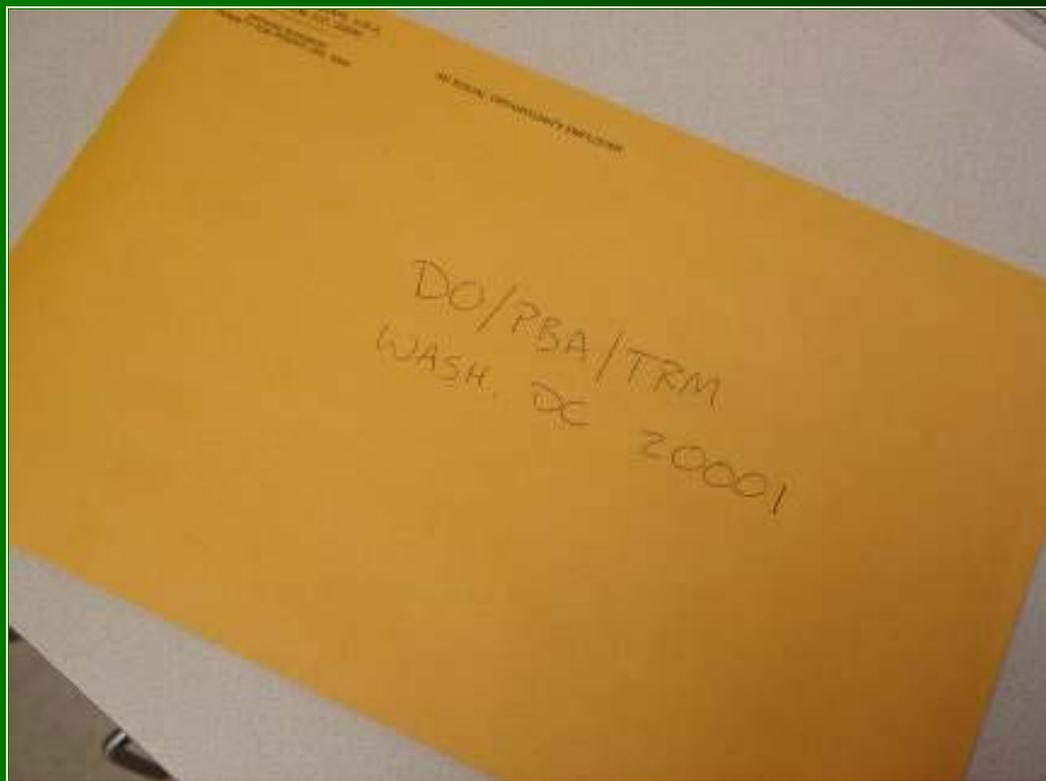
Double Wrapping



Address inner wrapping to an appropriate recipient by name and insert into another opaque envelope or opaque container with a locking mechanism (briefcase, locking folio, etc.).



Double Wrapping



Address outer wrapping to receiving office and seal envelope normally. Do not include the name of the recipient on the outer wrapping.



Traveling w/Classified Information

FBI Field Offices:

<http://www.fbi.gov/contact/fo/fo.htm>

USDA Ops Center: 1-877-677-2369

DOD Military Installation:

www.military.com/installationguides/chooseinstallation/1,11400,,00.html



Overseas

US Embassies





Reproduction Requirements



Classified information may only be reproduced on a machine specifically accredited for that purpose.

***EQUIPMENT MUST BE
PREAPPROVED BY PDSD***



Destruction Requirements

Classified information may only be disposed of in a manner approved for that purpose and accredited at the level of classified information which you intend to destroy.

Approved methods of destruction include (NSA approved) cross-cut shredding.





Processing Classified Information

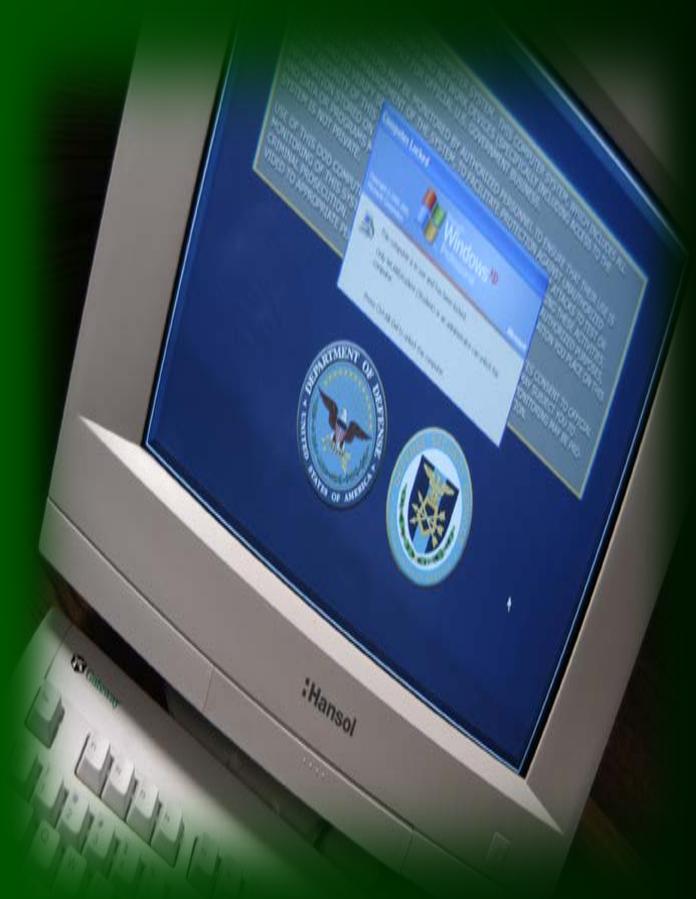
OCIO Approved Computer Systems

**DR 3140-001, USDA Information
Systems Security Policy**

No physical LAN/Internet Connectivity

Homeland Security Data Network

HSDN Computer Room



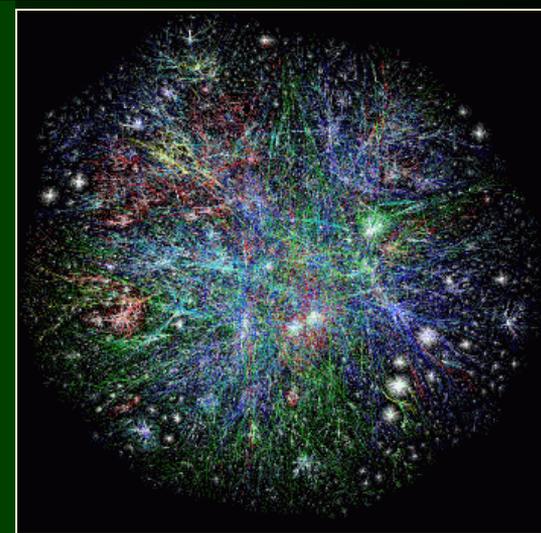


Cyber Security - IT

The Threat: Adversaries such as hackers, insiders, foreign intelligence collectors, terrorists, criminal elements, etc.

The Vulnerabilities: Blogs, social networking, chat rooms, discussion lists and personal and other public web sites. Blogs have become a robust source of information.

The Risk: Potential damage to the conduct of foreign relations; to a specific Department program, operation, investigation or security countermeasure; or to the credibility and professional reputation of the Department or its employees).





Operational Security and Cyber Awareness Tips

REMEMBER:

Anything you post online is accessible to everyone.

Keep personal and Department information out of blogs, social networks and other domains.

This protects our sensitive information and Personally Identifiable Information (PII) from compromise.





Infractions/Violations

Suspected loss or compromise (accidental/actual) of classified information including any amplifying information, tampering with a container used for classified storage requires reporting.

Infraction: Any knowing, willing or negligent act that puts classified information at risk.

Violation: Any knowing, willing or negligent act that results in an authorized disclosure of classified information.



Sanctions

Warnings

Reprimand

Suspension/Forfeiture of pay

Removal

Loss or denial of access to classified information

Removal of classification authority

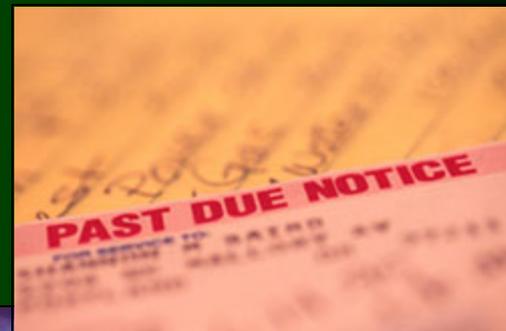
Actions may be taken under Titles 18/50 US Code



Reporting Requirements

Cleared USDA employees are required to report potentially derogatory information to PDSB involving:

- Serious financial issues (tax liens, judgments, impending bankruptcy, etc.)
- Serious involvements with law enforcement (arrests other than routine traffic issues, DUI, serious criminal issues, etc.)





Foreign Influence

- **Unreported personal contacts with foreign intelligence service, government or persons seeking classified information.**
- **Immediate family member who is a foreign national. if that relationship creates a heightened risk of foreign inducement, manipulation, pressure, or coercion**
- **Unreported close and continuing contact with a foreign national, including intimate contacts, roommate, or marriage.**
- **Exercise of any right, privilege or obligation of foreign citizenship**





Contact Reporting/Information

**Keith McElfresh, Chief, Classified National Security
Programs Branch, SSO**

(202) 260-0106

keith.mcelfresh@dm.usda.gov

Karen Maguire, Senior Information Security Specialist, SSO

(202) 720-5712

karen.maguire@dm.usda.gov

PDSD

(202) 720-7373

pdspd@dm.usda.gov



<http://www.dm.usda.gov/ohsec/pdsd/infosec.htm>



Form Ad-1189

Request to Pass Security Clearance

USDA UNITED STATES DEPARTMENT OF
AGRICULTURE
PERSONNEL AND DOCUMENT SECURITY DIVISION

REQUEST FOR PASSING A SECURITY CLEARANCE

Name of Requestor: _____ Agency: _____

Date: _____ Time: _____ Phone #: _____

Signature of Supervisor Authorizing PDSB to pass clearance (if different from
Name of Requestor): _____

Please complete the information below in its entirety and fax to (202) 720-1689.
Failure to complete all information may result in processing delays.

Name: _____

SSN (last four digits only): _____

DOB: _____

POB: _____

USDA Agency: _____

Location of Event: _____

Date/Time of Event: _____

Clearance Level (circle one): Confidential Secret Top Secret TS/SCI

Event POC and Phone #: _____

Security POC and Phone #: _____

Security Office Fax (unsecure) #: _____

Reason for event (meeting title, conference title, etc.): _____

Will you be making frequent visits to this facility during the year? YES NO

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN is needed to keep records accurate because other people may have the same name and birth date. Your SSN will be used to identify you precisely when it is necessary to 1) certify that you have access as indicated above. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such clearance verifications and passing

- Supervisory signature
- Classification level of meeting
- Identify Event and Security POCs
- Permcert needed?
- Password protect if emailing form to PDSB (contains PII)
- 72 hrs for external request/24hrs for internal request.



SF-312

CLASSIFIED INFORMATION NONDISCLOSURE AGREEMENT

AN AGREEMENT BETWEEN _____ AND THE UNITED STATES

(Name of Individual - Printed or typed)

1. Intending to be legally bound, I hereby accept the obligations contained in this Agreement in consideration of my being granted access to classified information. As used in this Agreement, classified information is marked or unmarked classified information, including oral communications, that is classified under the standards of Executive Order 12958, or under any other Executive Order or statute that prohibits the unauthorized disclosure of information in the interest of national security; and unclassified information that meets the standards for classification and is in the process of a classification determination as provided in Section 1.1, 1.2, 1.3 and 1.4(e) of Executive Order 12958, or under any other Executive Order or statute that requires protection for such information in the interest of national security. I understand and accept that by being granted access to classified information, special confidence and trust shall be placed in me by the United States Government.

2. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of classified information, including the procedures to be followed in ascertaining whether other persons to whom I intend these procedures.

3. I understand that the handling of classified information should be to the advantage of the United States. I shall have officially received information from the Department or Agency regarding the security classification status of classified information before I may be obligated to comply with laws and regulations that prohibit the unauthorized disclosure of classified information.

4. I have been advised that any breach of this Agreement may result in the termination of any security clearance I hold; removal from my position of special confidence and trust requiring such clearance; or termination of my employment or other relationships with the Department or Agencies that granted my security clearance or clearance. In addition, I have been advised that any unauthorized disclosure of classified information by me may constitute a violation of laws, including the provisions of Sections 641, 793, 794, 798, 1952 and 1924, Title 18, United States Code, the provisions of Section 783(b), Title 50, United States Code, and the provisions of the Intelligence Identities Protection Act of 1982. I recognize that nothing in this Agreement constitutes a waiver by the United States of the right to prosecute me for any statutory violation.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result or may result from any disclosure, publication or revelation of classified information not consistent with the terms of this Agreement.

6. I understand that the United States Government may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

7. I understand that all classified information to which I have access or may obtain access by signing this Agreement is now and will remain the property of, or under the control of the United States Government unless and until otherwise determined by an authorized official or final ruling of a court of law. I agree that I shall return all classified materials which have, or may come into my possession or for which I am responsible because of such access: (a) upon demand by an authorized representative of the United States Government; (b) upon the conclusion of my employment or other relationship with the Department or Agency that last granted me a security clearance or that provided me access to classified information; or (c) upon the conclusion of my employment or other relationship that requires access to classified information. If I do not return such materials upon request, I understand that this may be a violation of Sections 793 and/or 1924, Title 18, United States Code, a United States criminal law.

8. Unless and until I am released in writing by an authorized representative of the United States Government, I understand that all conditions and obligations imposed upon me by this Agreement apply during the time I am granted access to classified information, and at all times thereafter.

9. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions of this Agreement shall remain in full force and effect.

(Continue on reverse.)

10. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12958, Section 7211 of Title 5, United States Code (50 U.S.C. 17021b) or by the Military Code of Regulations, 32 CFR 1702.1(b) of illegality, 32 CFR 150 U.S.C. which protect 1952 and 1924 section 783(b)(1).
The definitions, requirements, obligations, restrictions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

11. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me the Executive Order and statutes referenced in this agreement and its implementing regulations, 32 CFR Section 2009.201 so that I may read them at my own convenience.

SIGNATURE _____ DATE (month/year) _____ SOCIAL SECURITY NUMBER _____
(See Notice below)

OFFICIAL NAME, TITLE, ORGANIZATION, ADDRESS AND IF APPLICABLE TELEPHONE NUMBER (Type or print)

WITNESS ACCEPTANCE
THE EXECUTION OF THIS AGREEMENT WAS WITNESSED BY THE UNDERSIGNED. THE UNDERSIGNED ACCEPTED THIS AGREEMENT ON BEHALF OF THE UNITED STATES GOVERNMENT.

SIGNATURE _____ DATE (month/year) _____ SIGNATURE _____ DATE (month/year) _____

NAME AND ADDRESS (Type or print) _____ NAME AND ADDRESS (Type or print) _____

SECURITY DEBRIEFING ACKNOWLEDGMENT

I declare that the provisions of the espionage laws, other Federal criminal laws and executive orders applicable to the safeguarding of classified information have been made available to me; that I have returned all classified information in my custody; that I will not communicate or transmit classified information to any unauthorized person or organization; that I will promptly report to the Federal Bureau of Investigation any attempt by an unauthorized person to solicit classified information, and that I have not struck out inappropriate words or words received a security debriefing.

SIGNATURE OF EMPLOYEE _____ DATE (month/year) _____

NAME OF WITNESS (Type or print) _____ SIGNATURE OF WITNESS _____

NOTICE: The Privacy Act, 5 U.S.C. 552a, requires that federal agencies inform individuals, at the time information is solicited from them, whether the disclosure is mandatory or voluntary, by what authority such information is solicited, and what uses will be made of the information. You are hereby advised that authority for soliciting your Social Security Number (SSN) is Executive Order 9397. Your SSN will be used to identify you precisely when it is necessary to identify you as having access to the information indicated above or to determine that you access to the information indicated has terminated. Although disclosure of your SSN is not mandatory, your failure to do so may impede the processing of such certifications or determinations or possibly result in the denial of you being granted access to classified information.

Your name, Last, First, M.I. as neat as possible

Sign, date, and SSN