



Initial Security Indoctrination Briefing

Office of Homeland Security and Emergency
Coordination

Personnel and Document Security Division
Classified National Security Programs Branch

This presentation is **UNCLASSIFIED**



Agenda

After this briefing, you will have received a basic indoctrination on:

- Policy for classified national security information (CNSI);
- Classification management;
- Physical security;
- Information security systems;
- Infractions/violations;
- Reporting;
- Operational security;
- Helpful resources.

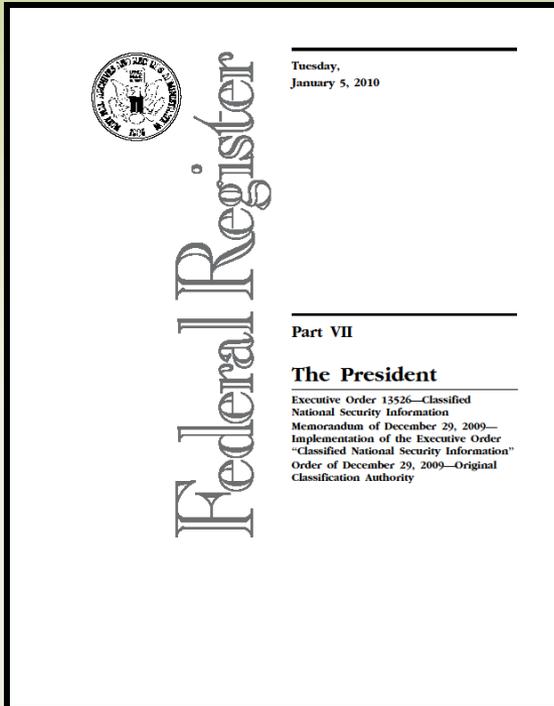


Policy





Executive Order 13526



All government agencies and individuals with access to Classified National Security 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.

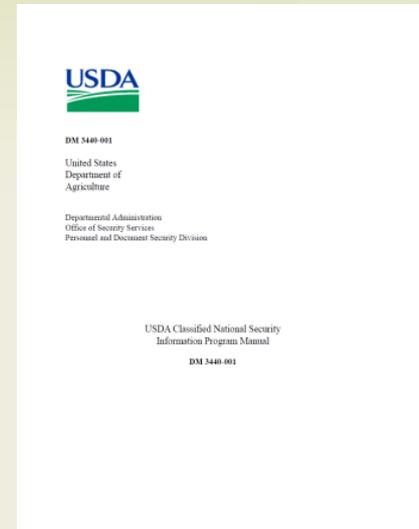
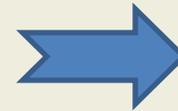
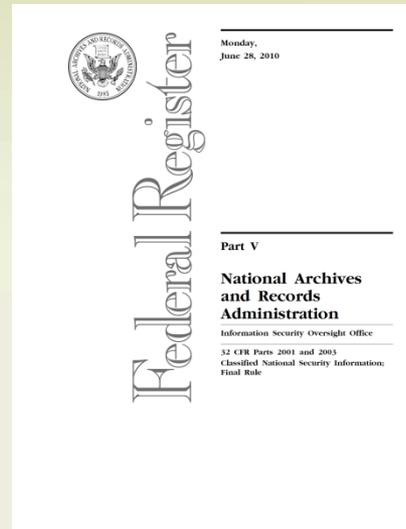
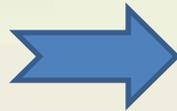


National Policy to Departmental Policy

E.O. 13526

Implementing Directive No. 1

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.



Senior Agency Official

Director of the Office of Homeland Security and Emergency Coordination (OHSEC)

Senior Agency Official for all CNSI in USDA. Responsibilities are:

- Establishing and administering the USDA CNSI Program.
- Maintaining an oversight role to ensure consistent and effective implementation of the Information Security Program throughout USD.
- Serving as the deciding official for the suspension, denial, and revocation of security clearances involving USDA personnel.



Mr. Todd Repass

Director

Office of Homeland Security and Emergency
Coordination



Personnel and Document Security Division (PDSD)

Personnel Security Branch

- Adjudicate national security clearances and public trust

Classified National Security Programs Branch

- Implementing and managing USDA's CNSI program
- Special Security Officer (SSO)

Information Security Coordinator (ISC)

- Primary liaison between their agency and the SSO.



Clearance Holders

Employees, contractors, and individuals maintaining a security clearance working with CNSI at USDA

- Adhering to the provisions of DR/DM 3440-001;
- Protecting CNSI from individuals who do not have a need-to-know, maintaining the proper security clearance, and having access to the proper security container to store CNSI;
- Reporting potentially derogatory information to their ISC's or the SSO;
- Immediately reporting security incidents and security violations to their respective ISC's or the SSO;
- Completing the initial security indoctrination training, annual security refresher training, required specialized training, and security debriefings; and
- Meeting safeguarding requirements prescribed by DM 3440-001.

Classification Management





What is Classified National Security 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.



CNSI Levels

There are only THREE levels of CNSI:

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)

- 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.



Classification Prohibitions & Limitations

In no case shall information be classified, continue to be maintained as classified, or fail to be declassified in order to:

- Conceal violations of law, inefficiency, or administrative error;
- Prevent embarrassment to a person, organization, or agency;
- Restrain competition; or
- Prevent or delay the release of information that does not require protection in the interest of the national security.



How to Classify

There are 2 ways to classify information:

- Original Classification Authority (OCA);
- Derivative Classification



Original Classification Authority

Original Classification Authority (OCA) means an agency or department 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.



OCA 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 declassification
- ✓ A “Declassify on” line that provides for the automatic declassification of the document



SECRET

MEMORANDUM February 25, 2012

TO: Hazel Nutt
FROM: Al K. Seltzer
SUBJECT: (U) Note How Subject Line is Also Portion Marked

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: Eaton Wright
Office Director
Reason: 1.4 (a),(d)
Declassify On: 2020 Feb, 24

SECRET

For Training Purposes Only



Derivative Classification

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



Derivative Marking Requirements

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: 2021 Jun 1



SECRET

MEMORANDUM

February 25, 2012

TO: Hazel Nutt
FROM: Al K. Seltzer
SUBJECT: (U) Note How Subject Line is Also Portion Marked

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.

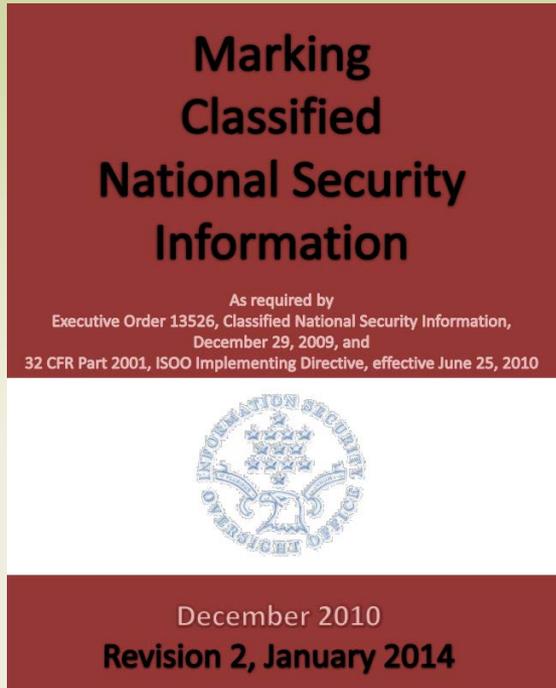
Derived from: USDA FSIS Report
Dated June 1, 2011
Declassify On: 2021 Jun 1

SECRET

For Training Purposes Only



ISOO Marking Guide



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

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



Classification by Compilation

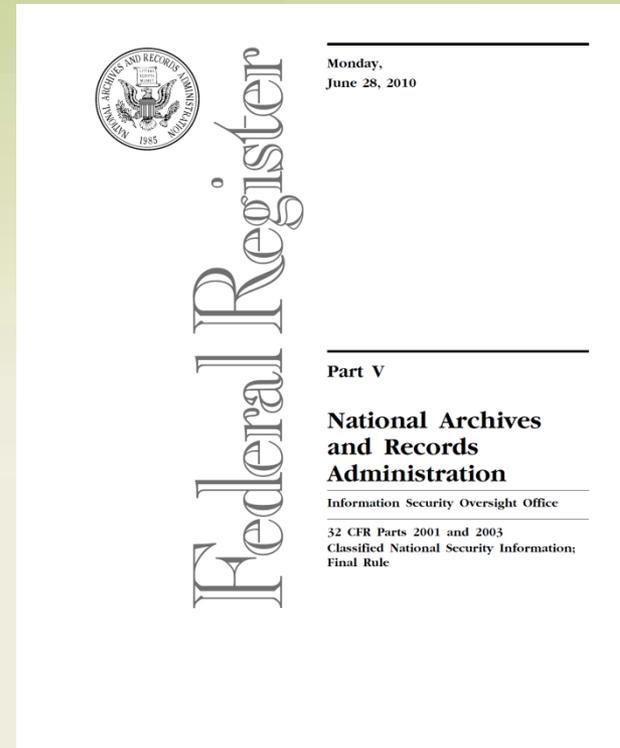
- Classification by compilation is an aggregation of pre-existing unclassified items of information. The compiled information may be classified if it reveals an additional association or relationship that meets the standards for classification and is not otherwise revealed in the individual items of information.
- Bringing together information that is already classified from more than one source document is not a compilation; it is derivative classification. However, information from multiple sources that is already classified at one level may result in a higher level of classification when it is compiled.



Declassification

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

PDSD/SSO is the point-of-contact for all declassification and downgrading requests for USDA. Contact your ISC for further guidance and instructions. No CNSI will be automatically declassified without review first from PSDS.





Reclassification

Information may not be reclassified after declassification and released to the public unless:

- The reclassification is personally approved in writing by the agency head based on a document-by-document determination by the agency that reclassification is required to prevent significant and demonstrable damage to the national security;
- The information may be reasonably recovered without bringing undue attention to the information.



CNSI Challenges

- Any individual with access to CNSI who believes that a classification status is improper, is encouraged and expected to challenge the classification status of the information in accordance with USDA procedures.
- USDA has established procedures for the challenge of the classification status of information that individuals believe is improperly classified or unclassified. These procedures ensure that:
 - Individuals are not subject to retribution for bringing such actions;
 - An opportunity is provided for review by an impartial official or panel; and
 - Individuals are advised of their right to appeal agency decisions to the Interagency Security Classification Appeals Panel established under E.O. 13526.



CNSI Challenge Process

To challenge the classification of information:

- Prepare written correspondence explaining all concerns relative to the challenge;
- Identify the exact document or information in question;
- Provide any back-up information or material to support the challenge; and
- Forward the package, in a manner required for CNSI, to PDSD for evaluation.



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

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

For Training Purposes Only

GEHEIM
SECRET

DEUTSCHE INDUSTRIE
NORMEN

22 Februar 1998

GERMAN INDUSTRIAL STANDARDS) (U)

THIS DOCUMENT CONTAINS GERMAN
GOVERNMENT INFORMATION

GEHEIM

SECRET

For Training Purposes Only



Physical security





Requirements

Classified information, regardless of its form, shall be afforded a level of protection against loss or unauthorized disclosure commensurate with its level of classification at all times; and stored only under conditions designed to deter and detect unauthorized access to the information.

Chapter 5 of DM 3440-001 identifies physical requirements for the protection of CNSI.

All equipment used for CNSI purposes shall be approved by either the ISC or the SSO.



Secure Work Area

All CNSI must be discussed, stored, processed and destroyed in a Secure Work Area (SWA).

- A SWA is an area that has been evaluated and accredited for CNSI use;
- SWA accreditations are issued by the SSO or a delegated ISC;
- SWA's will have a responsible person appointed to handle the day-to-day management of the SWA;
- All SWAs will have an approved Standard Operating Procedure (SOP) that provides a general user with the "how to's" for working in the SWA environment.



Storing

GSA-approved security containers are identified by a silver label on the control drawer (where lock is located) stating “General Services Administration Approved Security Container.” Contact your ISC or the SSO if you are in doubt of whether a container is approved for the storage of CNSI.

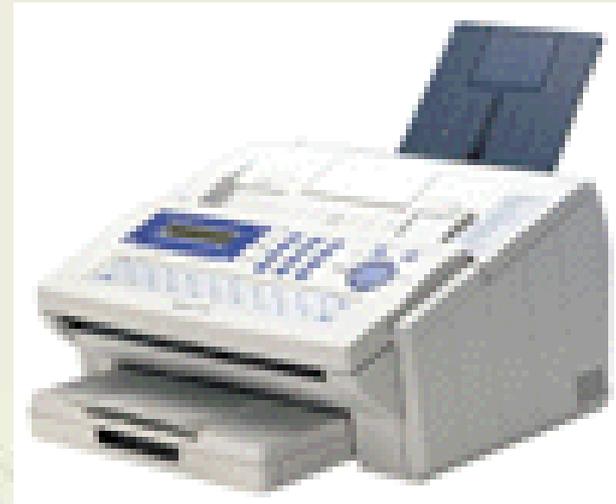




Secure Communications

CNSI will only be discussed on authorized equipment

- Persons discussing or transmitting CNSI are responsible for ensuring the intended recipients are approved for access to the same level of information being sent.





Transporting

Remember these rules when transporting CNSI:

- Preferred method is always electronic transmission first:
 - Homeland Security Data Network (HSDN), Secret level system; or
 - Secure fax;
- Transport CNSI only from one accredited space to another accredited space;
- You are liable for all CNSI in your possession;
- Do not open the package while in transit;
- CNSI may never be taken home.

Internal Transport of CNSI

- Inside USDA HQ complex:
 - Carried from one SWA to another;
 - Concealed in a folder or envelope to prevent viewing by unauthorized persons;
 - Use appropriate cover sheet;
 - No stopping for any means (lunch, farmers market, coffee break, etc.).





External Transport of CNSI

Outside USDA HQ complex:

- Coordinate with ISC or the SSO;
- **Must** have a Courier Card/Letter issued by the SSO;
- Items must be double-wrapped;
- Coordinate specialized shipping with the ISC or SSO.



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



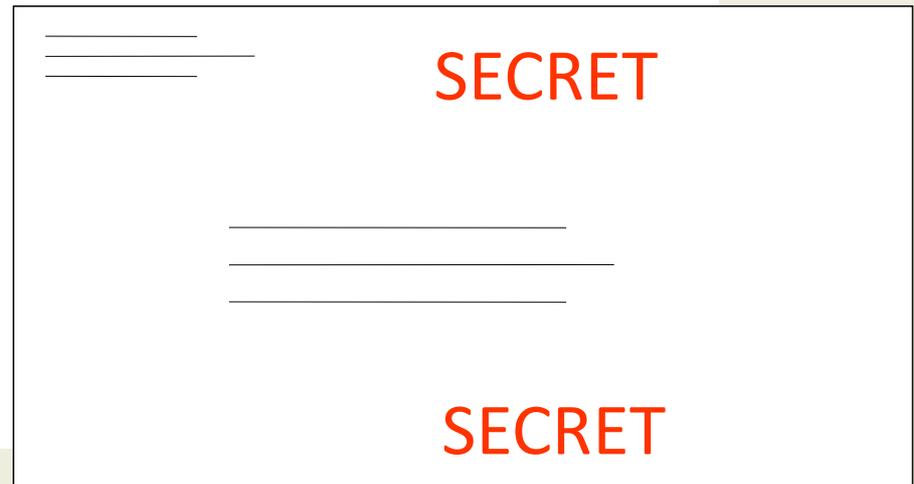


Double Wrapping - Inner Layer

Inner Envelope:

Opaque envelope - highest classification and dissemination controls at the top and bottom of both sides of envelope; wrapped to make detection of tampering easy;

- Address of recipient
- Return address (office where it should be returned if undeliverable, outer envelope is damaged or found open).



Double Wrapping - Outer Layer

Outer envelope:

- Opaque envelope;
- Wrapped to make detection of tampering easy;
- *NO* classification markings or dissemination controls;
- Recipients address
- Return address.
 - In the event a package is damaged in mailing or misplaced, specify to whom it should be returned.





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)*



Reproduction & Destruction

- Equipment used to reproduce CNSI must be approved by either the ISC or SSO;
- Equipment used to destroy CNSI must be on the National Security Agency Evaluated Products List
 - All non-paper media shall be destroyed by an ISC or the SSO.



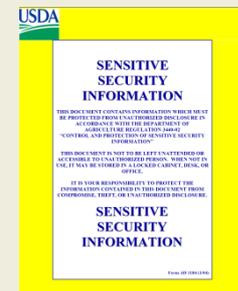
Cover Sheets

Cover sheets are used to protect the need-to-know of CNSI in an approved area for CNSI.

- Top Secret
 - Must have a cover sheet permanently affixed to it.

- Secret and Confidential
 - Whenever being transmitted via mail or courier;
 - Whenever being moved in public or common area within a SWA;

- Sensitive Security Information
 - As required



Labels

All equipment and media shall be explicitly labeled to indicate what classification level can be stored in the media, or introduced to the machine.



Information Security Systems





Processing CNSI

Prior to the introduction of any system into a room to be used for processing or viewing CNSI, the room must be accredited for CNSI purposes by either the ISC or SSO.

- At no time will any unclassified USDA enterprise computer, personal computer, or personal electronic device (PED) be used to process CNSI.
- Computer systems used view and/or process CNSI must be certified and accredited for CNSI by the USDA Designated Accrediting Authority (DAA). The DAA for USDA is the OCIO/ASOC. Contact your ISC for more assistance.
- All IT equipment (monitor, CPU, printer, scanner) and media shall be labeled to indicate the highest level of CNSI permitted for use, or that is present on the media.





Processing CNSI (cont)

OCIO Approved Computer Systems

DR 3140-001, USDA Information Systems Security Policy

No physical LAN/Internet Connectivity

Homeland Security Data Network

HSDN Computer Room

If you suspect your system has been breached contact the Agricultural Security Operations Center (ASOC) on cyber.incidents@asoc.usda.gov.

Infractions/Violations





Security Incidents

A security incident is defined as an event or action that is not in the best interest of the national security. All security incidents are to be reported either to the ISC or the SSO within 24 hours of occurrence or discovery.

- Security infraction - a failure to follow established policies and procedures that does not involve the loss, compromise or suspected compromise of CNSI.
- Security violation – any incident that involves the loss, compromise or suspected compromise of CNSI. Additionally, any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of CNSI.



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



Reporting Requirements

Cleared USDA employees are required to report potentially derogatory information to their ISC or the SSO involving:

- Significant changes to the SF-86;
- Financial concerns (affluence or derogatory);
- Arrests (felony and misdemeanor), traffic issues over \$300;
- Name change/change in marital status/residential status;
- Substance abuse rehabilitation;
- Mental/emotional counseling (outside of grief or family/marriage);
- Adverse information that could affect you maintaining your access to CNSI.





Reporting Responsibilities

It is important to remember that while you may be working for, or detailed to another organization (i.e., USAID); or temporary duty assignments overseas (USEMBASSY) does not relieve you of the requirement to report these issues to either your ISC or the SSO.



Foreign Influence

- Any close and continuing (ongoing or bond of affection) contact with a foreign national must be reported (includes immediate family members, intimate contacts, roommates, marriage, students, Au Pairs/nannies, associates in outside activities (bike clubs, church));
- Cleared employees must also report the following:
 - Personal contact with a foreign intelligence service, government of persons seeking CNSI;
 - If you elect to exercise any right, privilege or obligation of foreign citizenship.



Foreign Travel

- Foreign travel reporting (personal and official) is encouraged, but not required. This allows the SSO to provide helpful information on the security environment and the contact information of the closest American Embassy.
- DR 3580-003, Mobile Computing
http://www.ocio.usda.gov/sites/default/files/docs/2012/DR3580-003_Mobile_Computing.pdf



Operational Security





Awareness

- As a U.S. government employee, you can be targeted by a foreign intelligence or security service anywhere at any time. Although the Cold War has been over for more than two decades, many foreign governments still place a high priority on U.S. government information and technology. Many reports include that espionage directed against U.S. government and industry resources is at comparable, if not higher, levels than they were during the Cold War.
- Targets include theft of U.S. technology information;
 - Unclassified/Sensitive/Proprietary Information
 - USDA Research
 - Dual-Use/Export Controlled
 - Information that can be used for both military and commercial benefits
 - Classified National Security Information



IT Awareness

- Keep personal and departmental information out of blogs, social networks and other domains. This protects our sensitive information and PII from compromise.
- Remember – if you wouldn't leave it on the metro, don't put it on the internet!



Resources





Request to pass security clearance

- Requires supervisor's signature
- Classification level of meeting
- Identify event and security POCs
- PERM CERT needed?
- Password protect if emailing form (contains PII)
- 72 hours for external requests/24 hours for internal request
- Filled out in completion – incomplete forms could cause a delay in processing

 United States Department of Agriculture

PERSONNEL AND DOCUMENT SECURITY DIVISION
REQUEST FOR PASSING A SECURITY CLEARANCE
(PDSB requires 24 hours for internal requests, and 72 hours for external requests)

| | | | |
|---|---------------|---|---------|
| 1. Name of Requestor (Last, First, MI) | | 2. Date | |
| 3. USDA Agency | 4. Work Email | 5. Work Phone | |
| 6. Name of supervisor authorizing PDSB to pass the clearance for the requestor (Printed Name) | | | |
| 7. Supervisor Signature | | 8. Date | |
| Please complete this form in its entirety and submit to PDSB/CNSPB/SSO either by fax at (202) 720-1689, or email at pdsd@dm.usda.gov. Contact PDSB at (202) 720-7373 if you have any questions. Failure to complete all information may result in processing delays. | | | |
| 9. Name of individual who needs clearance passed (Last, First, MI) | | 10. SSN (Last 4 Only) | 11. DOB |
| 12. Organization and Location of Visit | | 13. Date(s) of Visit From: _____ To: _____ | |
| 14. Clearance Level Required for the Event (check one) <input type="checkbox"/> Confidential <input type="checkbox"/> Secret <input type="checkbox"/> Top Secret | | | |
| 15. Is SCI Access required? <input type="checkbox"/> Yes <input type="checkbox"/> No (If yes – list accesses here) _____ | | | |
| Information for Organization being visited | | | |
| 16. POC Name | | 17. POC Phone (unsecure) | |
| 18. Security POC Name | | 19. Security POC Phone (unsecure) | |
| 20. Security Office Fax # or Email (unsecure) | | | |
| 21. Reason for visit (meeting title, conference title, etc.) | | | |
| 22. Will the individual be making frequent visits to this facility during the year? <input type="checkbox"/> Yes <input type="checkbox"/> 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 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.

(Rev. 02/15)



Helpful websites

- Executive Order 13526:
<http://www.archives.gov/isoo/pdf/cnsi-eo.pdf>
- 32 CFR Part 2001, E.O. 13526 Implementing Directive:
<http://www.archives.gov/isoo/policy-documents/isoo-implementing-directive.pdf>
- Classified Non-Disclosure Agreement:
<http://www.archives.gov/isoo/security-forms/sf312.pdf>
- Presidential Decision Directive 19, Protecting Whistleblowers with Access to Classified Information:
<http://www.whitehouse.gov/sites/default/files/image/ppd-19.pdf>



Helpful websites (cont)

- DR 3440-001, USDA Classified National Security Information Program Regulation: <http://www.ocio.usda.gov/document/departamental-regulation-3440-001>
- DM 3440-001, USDA Classified National Security Information Program Manual: <http://www.ocio.usda.gov/document/departamental-manual-3440-001>
- DR 3440-002, Control and Protection of Sensitive Security Information: <http://www.ocio.usda.gov/directives/doc/DR3440-002.pdf>
- DM 3550-002, Sensitive but Unclassified (SBU) Information Protection: <http://www.ocio.usda.gov/sites/default/files/docs/2012/DM3550-002.pdf>
- OMB Memo M-06-15: Safeguarding Personable Identifiable Information (PII): <http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2006/m-06-15.pdf>
- CIA World Factbook: <https://www.cia.gov/library/publications/the-world-factbook/>
- Department of State, Smart Traveler Enrollment Program (STEP): <https://step.state.gov/step/>



Contact/Reporting Information

Personnel and Document Security Division

(202) 720-7373

pdsd@dm.usda.gov

Karen Maguire, Special Security Officer

(202) 720-5712

karen.maguire@dm.usda.gov



Questions





Paperwork

- SF-312, Classified Information Non-Disclosure Agreement
- Security Clearance Validation Form