CLASSIFIED DOCUMENTS

Classification Procedures

Executive Order 13526, dated December 29, 2009, sets U.S. Government policy for classifying national security information that must be protected from unauthorized disclosure. The Information Security Oversight Office in the National Archives is charged with overseeing this program.

Original and Derivative Classification

Information is classified in one of two ways -- originally or derivatively. Original classification is the initial determination that information requires protection, because unauthorized disclosure of the information reasonably could be expected to result in damage to the national security. In order to justify classification, information must pertain to one or more of the following categories:

1. military plans, weapons systems, or operations;
2. foreign government information;
3. intelligence activities (including covert action), intelligence sources or methods, or cryptology;
4. foreign relations or foreign activities of the United States, including confidential sources.
5. scientific, technological, or economic matters relating to the national security;
6. United States Government programs for safeguarding nuclear materials or facilities;
7. vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security; or
8. the development, production, or use of weapons of mass destruction.

If there is significant doubt about the need to classify information, it shall not be classified. Only U.S. Government officials to whom this authority has been delegated in writing and who have been trained in classification requirements have the authority for original classification. Original classification authorities issue security classification guides that others use in making derivative classification decisions. Most government employees and contractors make derivative classification decisions.

Derivative classification is the act of classifying a specific item of information or material on the basis of an original classification decision already made by an authorized original classification authority. The source of authority for derivative classification ordinarily consists of a previously classified document or a classification guide issued by an original classification authority.

Defense contractors make derivative classification decisions based on the Contract Security Classification Specification that is issued with each classified contract. If a

contractor develops an unsolicited proposal or originates information not in the performance of a classified contract, the following rules apply. If the information was previously identified as classified, it should be classified derivatively. If the information was not previously classified, but the contractor believes the information may be or should be classified, the contractor should protect the information as though classified at the appropriate level and submit it to the agency that has an interest in the subject matter for a classification determination. In such a case, the material should be marked CLASSIFICATION DETERMINATION PENDING. Protect as though classified (TOP SECRET, SECRET, or CONFIDENTIAL).

Classification guidelines for defense contractors are in Chapter 4 of the National Industrial Security Program Operating Manual. Full text of the NISPOM is available on the Defense Security Service website.

The following general rules apply to all forms of classification:

- Information shall not be classified for any reason unrelated to the protection of national security.
- Classifiers and authorized holders of classified information are responsible for ensuring that information is appropriately classified and properly marked.
- Individuals who believe that information in their possession is inappropriately classified, or inappropriately unclassified, are expected to bring their concerns to the attention of responsible officials.

Classification Levels

Information that must be controlled to protect the national security is assigned one of three levels of classification, as follows:

- TOP SECRET information is information that, if disclosed without authorization, could reasonably be expected to cause exceptionally grave damage to the national security.
- SECRET information is information that, if disclosed without authorization, could reasonably be expected to cause serious damage to the national security.
- CONFIDENTIAL information is information that, if disclosed without authorization, could reasonably be expected to cause damage to the national security.

If there is significant doubt about the level of classification, the lower level of classification should be used.

Atomic energy information is classified under the Atomic Energy Act of 1954, and the procedures differ from those prescribed for national security information. Atomic

energy information is automatically classified and remains classified until a positive action is taken to declassify it. It may be declassified only by the Department of Energy. Consult your security officer for information on marking and handling atomic energy information. There are two types:

- RESTRICTED DATA covers "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," except for data that has been declassified or removed from the Restricted Data category.
- FORMERLY RESTRICTED DATA is information that has been removed from the Restricted Data category after Department of Energy and Department of Defense have jointly determined that the information relates primarily to the military utilization of atomic weapons and can be adequately safeguarded as National Security Information. The word "formerly" only means that such information is no longer subject to controls under the Atomic Energy Act. Formerly Restricted Data remains classified and subject to controls on national security information. Such data may not be given to any other nation except under specially approved agreements. It is identified and handled as RESTRICTED DATA when sent outside the United States.

RESTRICTED DATA and FORMERLY RESTRICTED DATA should also be marked with one of the three classification levels -- TOP SECRET, SECRET, or CONFIDENTIAL.

Classification Pending: Material that you generate, and that you believe may be classified and for which no classification guidance is available, must be protected and handled as though classified at the appropriate level until a classification determination is obtained from the appropriate government organization. This material should be marked as follows:

CLASSIFICATION DETERMINATION PENDING
PROTECT AS (APPROPRIATE CLASSIFICATION LEVEL)

The derivative and warning notice markings need not be applied in this situation. Reproduction should be held to an absolute minimum until a classification determination is received.

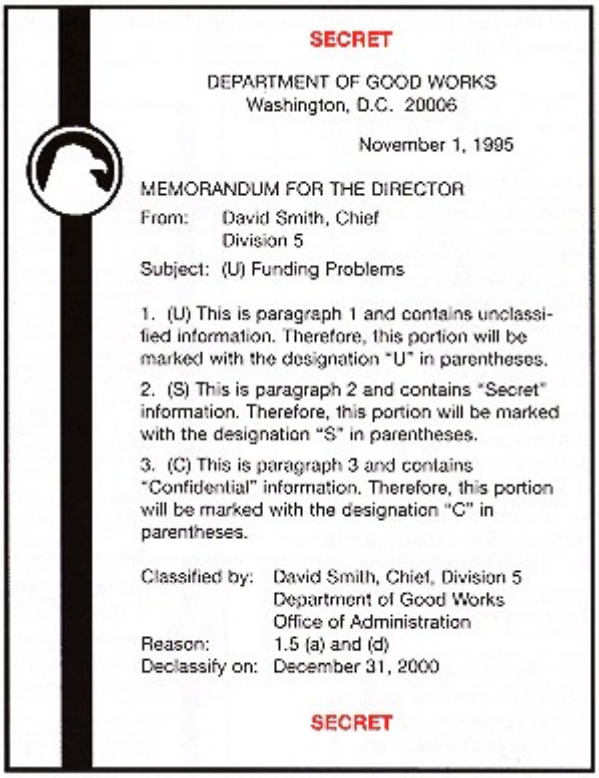
Markings for the "Classified by," "Derived from," and "Declassify on" Lines

All classified information shall be marked to reflect the source of the classification, reason for the classification, and instructions for declassification or downgrading. The markings used to show this information must appear toward the bottom on the cover, first page, title page, or in another prominent position. Non-documentary

material should show the required information on the material itself or, if not practical, in related or accompanying documentation.

"Classified by" Line: The "Classified by" line is used only on originally classified documents. It identifies the original classification authority by name or personal identifier and position. This is followed by a "Reasons" line that cites one of the eight classification categories listed above and specified in Executive Order 13526. There must also be a specific date for declassification, which may be a specific near-term date or event, 10 years, or at a maximum 25 years from the date of the original classification. If information should remain classified beyond 25 years, there are exemptions that may apply.

Example of original classification



SECRET

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

November 1, 1995

MEMORANDUM FOR THE DIRECTOR

From: David Smith, Chief
Division 5

Subject: (U) Funding Problems

1. (U) This is paragraph 1 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

2. (S) This is paragraph 2 and contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses.

3. (C) This is paragraph 3 and contains "Confidential" information. Therefore, this portion will be marked with the designation "C" in parentheses.

Classified by: David Smith, Chief, Division 5
Department of Good Works
Office of Administration
Reason: 1.5 (a) and (d)
Declassify on: December 31, 2000

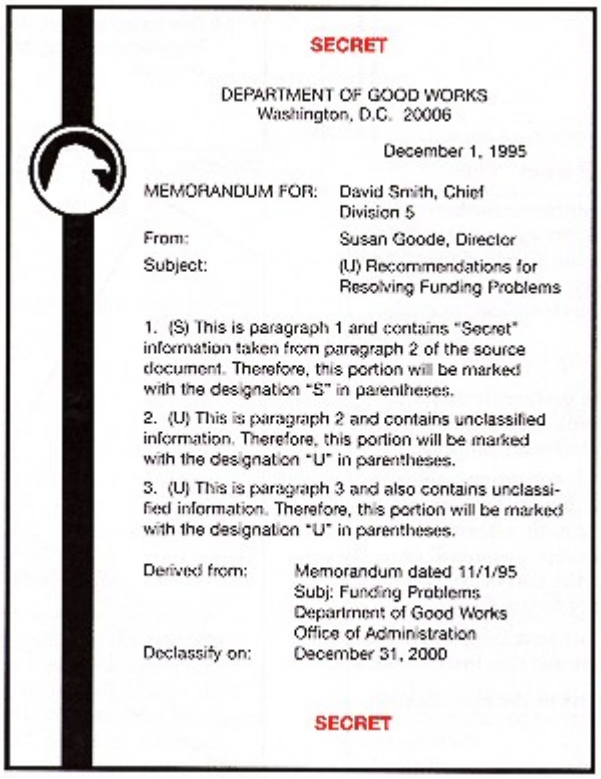
SECRET

"Derived from" Line: Any appropriately cleared employee has the authority to derivatively classify a document. The "Derived from" line cites the source document or classification guide which allowed you to determine that the information in your document is classified. The Declassify by date should be the same as the declassification date for the original classification. If your document classification is derived from "Multiple Sources" and different declassification instructions apply, use the date for the longest period of classification.

Duration of Classification: Whenever possible, the declassification date should be specified as a date or event that corresponds to the lapse of the information's national security sensitivity. However, the date or event must not exceed 25 years from the date of the original classification. If information should remain classified beyond 25 years, there are exemptions that may apply. This may be appropriate,

for example, if the information would reveal the identity of a confidential human source, or a human intelligence source, or key design concepts of weapons of mass destruction.

Example of derivative classification



SECRET

DEPARTMENT OF GOOD WORKS
Washington, D.C. 20006

December 1, 1995

MEMORANDUM FOR: David Smith, Chief
Division 5

From: Susan Goode, Director

Subject: (U) Recommendations for Resolving Funding Problems

1. (S) This is paragraph 1 and contains "Secret" information taken from paragraph 2 of the source document. Therefore, this portion will be marked with the designation "S" in parentheses.

2. (U) This is paragraph 2 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

3. (U) This is paragraph 3 and also contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses.

Derived from: Memorandum dated 11/1/95
Subj: Funding Problems
Department of Good Works
Office of Administration

Declassify on: December 31, 2000

SECRET

Downgrading and Declassification

Downgrading or Declassifying Classified Information: Information is downgraded or declassified based on the loss of sensitivity of the information due to the passage of time or on occurrence of a specific event. Declassification does not necessarily mean approval for public disclosure.

Marking Downgraded or Declassified Material: Classified information that is downgraded or declassified should be promptly and conspicuously marked to indicate the change.

Foreign Government Information: No U.S. document shall be downgraded below the highest level of foreign government information contained in the document, nor shall it be declassified without the written approval of the foreign government that originated the information.

Classified Information Appearing in Public Media: The fact that classified information has been made public does not mean it is automatically declassified. Information remains classified unless and until it is formally declassified. If you become aware of classified or other sensitive information appearing in the public media, bring it to the attention of your security office.

Challenging a Classification

Any approved holder of classified information who believes the information is classified improperly or unnecessarily, or that current security considerations justify downgrading to a lower classification or upgrading to a higher classification, or that security classification guidance is improper or inadequate, is encouraged and expected to question the classification status.

Government employees can appeal classification decisions through established agency procedures that protect individuals from retribution for bringing such actions, provide an opportunity for review by an impartial official or panel, and provide a right of appeal to the Interagency Security Classification Appeals Panel. Contractors should appeal such issues through their pertinent government contracting authority.

Members of the public can appeal any classification decision through the Interagency Security Classification Appeals Panel. The Information Security Oversight Office (ISOO) provides program and administrative support for this panel.

Declassification Program

A principal goal of Executive Order 13526 is better management of the declassification process. It establishes a National Declassification Center (NDC) within the National Archives to streamline the declassification process and implement a standardized training program regarding the declassification of records determined to have permanent historical value.

A Presidential Memorandum that accompanied this Executive Order noted a backlog of 400 million Federal records that are subject to automatic declassification. The President ordered that this backlog be addressed in a manner that will permit public access to all declassified records from this backlog no later than December 31, 2013.

Overview

A security clearance is a privilege, not a right. When you accept the privilege of access to classified information, you are also accepting the responsibilities that accompany this privilege. This guide informs you of your responsibilities and provides information to help you fulfill them.

Your responsibility to protect the classified information that you learn about is a LIFELONG obligation. It continues even after you no longer have an *active* security clearance.

The Nondisclosure Agreement you signed when accepting your clearance is a legally binding agreement between you and the U.S. Government in which you agreed to comply with procedures for safeguarding classified information and acknowledged that there are legal sanctions for violating this agreement. Deliberate violation for profit may be prosecuted. This agreement assigned to the U.S. Government the legal right to any payments, royalties or other benefits you might receive as a result of unauthorized disclosure of classified information. Your signed Nondisclosure Agreement is the only form held on file long after you retire (50 years!).

The various topics in this module of the Security Guide discuss procedures for handling, marking, safeguarding, and communicating classified information. The regulatory basis for these procedures is Executive Order 13526, Classified National Security Information, dated December 29, 2009. National guidance for implementing this order is in the Information Security Oversight Office implementing directive 32 C.F.R. Part 2001, effective June 25, 2010. Many individual departments, agencies, and offices also have their own implementing regulations, for example, Department of Defense Regulation 5200.1, Information Security Program, which is updated periodically as needed..

Failure to comply with these procedures may result in adverse administration action including revocation of your security clearance. When we study the history of foreign intelligence activities against the United States, one thing becomes very clear. When our adversaries or competitors are successful in obtaining classified or other sensitive information, it is usually due to negligence, willful disregard for security, or betrayal of trust by our own personnel.

Marking Classified Information

Physically marking classified information with appropriate classification and control markings serves to warn and inform holders of the degree of protection required. Other notations aid in derivative classification actions and facilitate downgrading or declassification. It is important that all classified information and material be marked to clearly convey the level of classification assigned, the portions that contain or reveal classified information, the period of time protection is required, and any other notations required for protection of the information or material.

The following is a summary of the most commonly used document control markings. More detailed information is available via the Internet from a variety of sources.1 Classification and control markings and country designators authorized for use by the Intelligence Community are compiled in the Authorized Classification and Control Markings Register maintained by the DNI Special Security Center, Controlled Access Program Coordination Office (CAPCO).

Overall Classification Markings

The overall (i.e., highest) classification of a document is marked at the top and bottom of the outside cover (if there is one), the title page (if there is one), the first page, and the outside of the back cover (if there is one) or back side of the last page.

Each interior page containing classified information is marked top and bottom with the overall (i.e., highest) classification of the page. Each unclassified interior page is marked 'Unclassified" at the top and bottom. Interior pages that are For Official Use Only need to be marked only at the bottom. Blank pages require no markings.

Attachments and annexes may become separated from the basic document. They should be marked as if they were separate documents.

Additionally, every classified document must show, on the face of the document, the agency and office that created it and date of creation. This information must be clear enough to allow someone receiving the document to contact the preparing office if questions or problems about classification arise.

U.S. documents that contain foreign government information shall be marked on the front, "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT (indicate level) INFORMATION."

Computer files must be marked with appropriate headers and footers to ensure that anything that is transmitted or printed will have the applicable classification and associated markings.

All removable storage media and devices such as diskettes, CD-ROMs, cassettes,

magnet tape reels, etc. must have an outer label with the appropriate markings.

Each slide must be marked on the slide itself or slide cover, as well as on the image that is projected.

Automated Information Processing Requirements

Use of automated information systems to route and control access to information requires standard procedures for how documents are marked. Classification and control markings must follow a specified format that enables automated systems to recognize the markings.

Any classified document, either in hard copy or automated, must contain a header and footer with the classification, any control markings, and declassification date or designation. These three elements -- classification, control marking(s), and declassification date -- must be separated by two forward slashes and no spaces. If multiple dissemination control markings are used, they are separated by a comma and no spaces, except that multiple SCI controls are separated by a single forward slash and no spaces. Declassification date must be marked by an eight-digit number (year, month, day), exemption category (such as X1), or as Manual Review (MR). This is illustrated by the following examples:

SECRET//SI/TK//NOFORN//X1

SECRET//ORCON,PROPIN//20091231

A control marking such as FOR OFFICIAL USE ONLY cannot stand alone. It must be preceded by a classification as in:

UNCLASSIFIED//FOR OFFICIAL USE ONLY

When marking foreign government classified information, the classification is preceded by two forward slashes and countries are identified by an approved three-letter designator, as in //NATO SECRET or //DEU SECRET for Germany.

Portion Marking

The title or subject of a classified document is marked with the appropriate classification abbreviation in parentheses -- (TS), (S), (C), or (U) immediately following and to the right of the title or subject. All documents containing information that requires control markings, regardless of classification, format, or medium, shall be portion marked. The overall classification of a document is equal to the highest classification level of any one portion found in the document.

Each portion of a classified document is to be marked with the appropriate classification abbreviation in parentheses immediately before the beginning of the portion. If the portion is numbered or lettered, place the abbreviation in parentheses

between the letter or number and the start of the text. A portion is ordinarily defined as a paragraph, but also includes subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, classified signature blocks, bullets and other portions with slide presentations and the like.

Portions of U.S. documents containing foreign government information are marked to reflect the foreign country of origin as well as the appropriate classification, for example, (U.K.-C). Portions of U.S. documents containing extracts from NATO documents are marked to reflect "NATO" or "COSMIC" as well as the appropriate classification, for example, (NATO-S) or (COSMIC-TS). Further information is available at Foreign Government Classified Information.

Point of Contact Marking

All intelligence reports shall include an Intelligence Community point of contact and contact instructions at the end of the report. This is required to expedite decisions on the sharing of the report.

Release to Foreign Countries/Organizations

In support of homeland security and coalition warfare, the U.S. Government has an increased need to share data with foreign countries, international organizations, and multinational forces. This has led to recent changes in the use of the "Released to..." (REL TO) control marking. This marking was previously only for use on intelligence information, but it is now authorized for use on all classified defense information.

Following the REL TO marking is a list of countries to which the information may be released through proper disclosure channels to specified foreign governments or international organizations. This list starts with USA and is followed by other countries listed alphabetically by the approved country code(s), international organization, or coalition force.

Example: TOP SECRET//REL TO USA, EGY and ISR

This format with // after the classification, a comma and space between each country, and with a lower case "and" with no comma before the last country code must be followed exactly to facilitate machine reading and sorting of the document. The approved three-letter country codes are available on the Internet at ftp.ripe.net/iso3166-countrycodes.txt. This marking shall appear at the top and bottom of the front cover (if there is one), the title page (if there is one), the first page and the outside of the back cover (if there is one). Each interior page containing classified information is marked top and bottom with the overall (i.e., highest) classification of the page.

When portion marking individual titles or paragraphs, the countries do not need to be listed unless they are different from the countries listed in the REL TO at the top and bottom of the page. For example: (TS:REL). If information is releasable to different countries than those listed in the overall REL TO marking, all the countries and organizations should be listed in the portion marking. For example: (S//REL TO USA, AUS, NZL and NATO).

The marking "Not Releasable to Foreign Nationals" (NOFORN) is still only authorized for use on intelligence that requires originator approval before being disclosed (see below).

Other Distribution Controls

In addition to its classification, intelligence information and certain scientific or technical information may also be subject to other controls on its distribution and handling. It is your responsibility to understand and comply with the control markings on classified information. If you are not sure, contact your security office. These control markings include:

- **Dissemination and Extraction of Information Controlled by Originator (ORCON)** or **(OC)** means that any additional distribution or inclusion in another document must be approved by the originator of the document. It is used on intelligence information that could permit identification of a sensitive intelligence source or method.
- **Not Releasable to Contractors/Consultants (NOCONTRACT)** has been discontinued but is still seen on older documents. Check with the originator of the document regarding any ongoing controls on the use of such a document. This caveat was used on intelligence information that is provided by a source on the express or implied condition that it not be made available to contractors; or that, if disclosed to a contractor, would actually or potentially give him/her a competitive advantage or cause a conflict of interest with his/her obligation to protect the information.
- **Caution - Proprietary Information Involved (PROPIN)** or **(PR)** is used with or without a security classification to identify information provided by a commercial firm or private source under an express or implied understanding that the information will be protected as a trade secret or proprietary data with actual value.
- **NOFORN** is for intelligence information that may not be passed to foreign nationals.
- **Authorized for Release to ____ (REL TO)** signifies intelligence information that is releasable to or has been released through proper disclosure channels to the named foreign government or international organization. See more

specific guidance in previous section.

- **RELIDO:** the release decision is delegated to Designated Intelligence Disclosure Officials.
- **REL TO.../RELIDO:** Releasable to U.S. citizens and foreign nationals of specified country(ies) and of additional countries identified by Designated Intelligence Disclosure Officials.
- **Sensitive Compartmented Information (SCI)** applies to certain intelligence sources, methods, or analytical processes that are subject to a formal access control system established by the Director of Central Intelligence. Special approval is required for access to SCI.
- **Communications Security (COMSEC)** is the protection of all elements of telecommunications -- encryption, transmission, emissions, and the physical security of equipment and materials.
- **Cryptographic Material (CRYPTO)** identifies information or materials that must be handled through special cryptographic channels.
- **Warning Notice - Intelligence Sources or Methods Involved (WNINTEL)** has been discontinued but is still seen on older documents. It was used on intelligence information that identifies or would reasonably permit identification of an intelligence source or method that is susceptible to countermeasures that could nullify or reduce its effectiveness.
- **Critical Nuclear Weapons Design Information (CNWDI)** or **(N)** applies to information that reveals the theory of operation or design of the components of a thermonuclear or fission bomb, warhead, demolition munition, or test device. Special handling procedures are required.

Department of Defense also uses the marking **Alternative or Compensatory Control Measures (ACCM)** for classified information that requires special security measures to safeguard classified intelligence or operations and support information when normal measures are insufficient to achieve strict need-to-know controls and where special access program (SAP) controls are not required. ACCM measures are defined as the maintenance of lists of personnel to whom the specific classified information has been or may be provided together with the use of an unclassified project nickname. The ACCM designation is used in conjunction with the security classification to identify the portion, page, or document containing ACCM information.

Handling Classified Information

As an approved custodian or user of classified information, you are personally responsible for the protection and control of this information. You must safeguard this information at all times to prevent loss or compromise and unauthorized disclosure, dissemination, or duplication. Unauthorized disclosure of classified material is punishable under the Federal Criminal Statutes or organizational policies.

Your security officer or supervisor will brief you on the specific rules for handling classified information that apply to your organization. Here are some standard procedures that apply to everyone.

Classified information that is not safeguarded in an approved security container shall be constantly under the control of a person having the proper security clearance and need-to-know. An end-of-day security check should ensure that all classified material is properly secured before closing for the night.

If you find classified material left unattended (for example, in a rest room, or on a desk), it is your responsibility to ensure that the material is properly protected. Stay with the classified material and notify the security office. If this is not possible, take the documents or other material to the security office, a supervisor, or another person authorized access to that information, or, if necessary, lock the material in your own safe overnight.

Classified material shall not be taken home, and you must not work on classified material at home.

Classified information shall not be disposed of in the waste basket. It must be placed in a designated container for an approved method of destruction such as shredding or burning.

Email and the Internet create many opportunities for inadvertent disclosure of classified information. Before sending an email, posting to a bulletin board, publishing anything on the Internet, or adding to an existing Web page, you must be *absolutely* certain none of the information is classified or sensitive unclassified information. Be familiar with your organization's policy for use of the Internet. Many organizations require prior review of ANY information put on the Internet.

Classified working papers such as notes and rough drafts should be dated when created, marked with the overall classification and with the annotation "Working Papers," and disposed of with other classified waste when no longer needed.

Computer diskettes, magnetic tape, CDs, carbon paper, and used typewriter ribbons may pose a problem when doing a security check, as visual examination does not readily reveal whether the items contain classified information. To reduce

the possibility of error, some offices treat all such items as classified even though they may not necessarily contain classified information.

Foreign government material shall be stored and access controlled generally in the same manner as U.S. classified material of an equivalent classification, with one exception. See Foreign Government Classified Information.

Top Secret information is subject to continuing accountability. Top Secret control officials are designated to receive, transmit, and maintain access and accountability records for Top Secret information. When information is transmitted from one Top Secret control official to another, the receipt is recorded and a receipt is returned to the sending official. Each item of Top Secret material is numbered in series, and each copy is also numbered.

Some classified Department of Defense information is subject to special controls called Alternative or Compensatory Control Measures (ACCM). ACCM are security measures used to safeguard classified intelligence or operations and support information when normal measures are insufficient to achieve strict need-to-know controls and where special access program (SAP) controls are not required. ACCM measures include the maintenance of lists of personnel to whom the specific classified information has been or may be provided, together with the use of an unclassified nickname and ACCM designation used in conjunction with the security classification to identify the portion, page, and document containing such specific classified information.

Mailing and Carrying Classified Materials

The following procedures apply to mailing or carrying classified materials. These procedures cover the most common circumstances but do not cover the shipment of bulky materials. It is intended as general guidance only and is not a substitute for review of the official regulations.

TOP SECRET material may not be sent through the mail under any circumstances. It must be transmitted by cleared courier or approved electronic means.

SECRET material may be transmitted by U.S. Postal Service registered mail or express mail within and between the United States and its territories. However, the "Waiver of Signature and Indemnity" block on the Express Mail Label 11-B may not be executed, and the use of external (street side) express mail collection boxes is prohibited. SECRET material may be sent through U.S. Postal Service registered mail through Army, Navy, or Air Force Postal Service facilities outside the United States, provided that the information does not at any time pass out of U.S. citizen control and does not pass through a foreign postal system or any foreign inspection. Federal Express may also be used for SECRET material for urgent, overnight delivery only, but contractors must receive approval from their government contracting authority to use this method.

CONFIDENTIAL material is subject to the same mailing procedures as Secret material, with the following exceptions: (1) CONFIDENTIAL material may be sent by U.S. Certified mail rather than by U.S. Registered mail. (2) Government agencies (but not contractors) may also send CONFIDENTIAL material by First Class mail between and among government agencies only. It cannot be sent to contractors via First Class mail. Under all circumstances, the outer envelope should be marked "Do Not Forward. Return to Sender." Under no circumstances shall the USPS Express Mail label 11-B "Waiver of Signature and Indemnity" be used.

Classified material must be mailed at the post office. Use of street mail collection boxes is prohibited.

Wrapping

All classified material must be double-wrapped with opaque inner and outer covers. It shall be marked as follows:

- Mark the inner envelope top and bottom on both sides, preferably in red, with the classification in capital letters. A box with classified material should be marked with the classification on all surfaces of the inner wrapping.
- Write the complete mailing address and complete return address on the inner

envelope. The address on the inner envelope should have the name of an appropriately cleared individual.

- On the outer envelope, write the complete mailing address and return address. Do not indicate on the outer envelope that it contains classified information. Classified mail or shipments should be addressed to the Commander or other head of the organization by title, not by name, or to an approved classified mailing address of a federal government activity or to a cleared contractor using the name and classified mailing address of the facility. An individual's name should not appear on the outer envelope. Instead of a person's name, use office code letters, numbers, or phrases in an attention line to aid in internal routing. When necessary to direct material to the attention of a particular individual, put the individual's name on an attention line in the letter of transmittal or on the inner container or wrapper.

For Official Use Only is a document control designation, not a classification. Such material may be mailed in a single envelope.

Receipts

A receipt identifying the sender, the addressee, and the document should be attached to or enclosed in the inner envelope as noted below. The receipt shall contain no classified information. It should be signed and returned to the sender.

Top Secret material must be transmitted under a continuous chain of receipts covering each individual who obtains custody.

For Secret material, a classified material receipt must be included with all material transmitted outside the facility.

For Confidential material, a receipt must be included only if the sender deems it necessary, or if the information is being transmitted to a foreign government.

Hand-Carrying Classified Material

For hand-carrying classified material, different procedures apply for surface transportation, commercial air, government air, and for transportation outside the continental U.S.

If you personally transport classified material by car or foot to another location, you must provide reasonable protection for the information under all foreseeable contingencies that might occur while in transit.

Automobile accident, theft and sudden illness are all foreseeable contingencies. This means the classified information must be double wrapped or packaged as though it were being sent by mail, kept under your constant control (i.e., not left in the trunk of your car while you run another errand), and delivered only to an authorized person. A briefcase may serve as the outer wrapper only if it is locked

and approved for carrying classified material. Prepare an inventory of the material and leave one copy in your office and another copy with a security officer or other responsible person.

For air travel, a written letter of authorization from your security office is required. Your security officer will advise you of appropriate procedures. Stricter procedures are required for air travel outside the United States. For air travel, a locked briefcase may *not* serve as the outer wrapper.

Foreign Government Classified Information

The U.S. Government has negotiated agreements with many foreign countries regarding the protection of classified information. These agreements commit the United States to provide substantially the same degree of protection for foreign classified information as it provides to U.S. information classified at the same level.

When contractors are awarded contracts that involve access to foreign classified information, they shall notify the U.S. government agency that monitors their security compliance. That agency will then administer oversight and ensure implementation of the security requirements of the contract on behalf of the foreign government.

Some additional requirements pertaining to foreign government information are given below.1

Marking Foreign Government Classified Material: Foreign government designations for classified information generally parallel U. S. security classification designations. However, some foreign governments have a fourth level of classification, Restricted, for which there is no equivalent U.S. classification. This information is to be protected and marked as Confidential information. When other foreign government material is received, the equivalent U.S. classification and the country of origin shall be marked on the front in English.

Marking U.S. Documents That Contain Foreign Government Information: U.S. documents that contain foreign government information shall be marked on the front, "THIS DOCUMENT CONTAINS FOREIGN GOVERNMENT (indicate level) INFORMATION." The portions of the document that contain foreign classified information shall be identified and marked to identify the classification level and the country of origin. No U.S. document shall be downgraded below the highest level of foreign government information contained in the document, nor shall it be declassified without the written approval of the foreign government that originated the information.

Marking Documents Prepared for Foreign Governments: Documents prepared for foreign governments that contain U.S. and foreign government information shall be marked as prescribed by the foreign government. In addition, they shall be marked on the front, "THIS DOCUMENT CONTAINS UNITED STATES CLASSIFIED INFORMATION." Portions shall be marked to identify the U.S. classified information.

Security Clearances: Personnel security clearances and facility clearances issued by the U.S. Government are valid for access to classified foreign government

information of a corresponding level. Contractor employees will be briefed and acknowledge in writing their responsibilities for handling foreign government information prior to being granted access.

Storage, Control, and Accountability: Foreign government material shall be stored and access controlled generally in the same manner as U.S. classified material of an equivalent classification, with one significant exception. Other governments and NATO have not lessened the accountability requirements for their Secret information. Therefore, we are required to provide a greater degree of control over foreign government Secret information. There must be records reflecting the transfer of responsibility and accountability of foreign Secret information.2 Also, foreign government material shall be stored in a manner that will avoid commingling with U.S. classified information. For example, it should be stored in separate files.

Disclosure and Use Limitations: Foreign government information shall not be disclosed to nationals of a third country, including intending citizens, or to any other third party, or be used for other than the purpose for which it was provided, without the prior written consent of the originating foreign government.

Export of Foreign Government Information: An export authorization is required for the export or re-export of export-controlled foreign government information except for technical data being returned to the original source of import. Foreign government information shall not be exported to a third party without the prior consent of the originating government.

Public Disclosure: The public disclosure of foreign government information requires the prior written approval of the contracting foreign government.

Reproduction: The reproduction of foreign government Top Secret information requires the written approval of the originating government.

Disposition: Upon completion of a contract, foreign government information shall be returned to the responsible U.S. Government agency or to the foreign government that provided the information unless the contract specifically authorizes destruction or retention of the information.

Security Violations

A security violation or infraction is any breach of security regulations, requirements, procedures or guidelines, whether or not a compromise results. No matter how minor, any security infraction must be reported immediately to the security office so that the incident may be evaluated and any appropriate action taken.

The following are examples of security violations:

- Leaving a classified file or security container unlocked and unattended either during or after normal working hours.
- Keeping classified material in a desk or unauthorized cabinet, container, or area.
- Leaving classified material unsecured or unattended on desks, tables, cabinets, or elsewhere in an unsecured area, either during or after normal working hours.
- Reproducing or transmitting classified material without proper authorization.
- Losing your security badge.
- Removing classified material from the work area in order to work on it at home.
- Granting a visitor, contractor, employee or any other person access to classified information without verifying both the individual's clearance level and need-to-know.
- Discussing classified information over the telephone, other than a phone approved for classified discussion.
- Discussing classified information in lobbies, cafeterias, corridors, or any other public area where the discussion might be overheard.
- Carrying safe combinations or computer passwords (identifiable as such) on one's person, writing them on calendar pads, keeping them in desk drawers, or otherwise failing to protect the security of a safe or computer.
- Failure to mark classified documents properly.
- Failure to follow appropriate procedures for destruction of classified material.

Major Violations

The significance of many security violations does not depend upon whether information was actually compromised. It depends upon the intentions and attitudes of the individual who committed the violation.

Ability and willingness to follow the rules for protection of classified information is a prerequisite for maintaining your security clearance. Although accidental and infrequent minor violations are to be expected, deliberate or repeated failure to

follow the rules is definitely not. It may be a symptom of underlying attitudes or emotional/personality problems that are a serious security concern.

The following behaviors are of particular concern and may affect your security clearance:

- A pattern of routine security violations due to inattention, carelessness, or a cynical attitude toward security discipline.
- Taking classified information home, ostensibly to work on it at home, or carrying it while in a travel status without proper authorization.
- Prying into projects or activities for which the person does not have (or no longer has) a need to know. This includes requests for classified publications from reference libraries without a valid need to know, or any attempt to gain unauthorized access to computer systems, information, or data bases.
- Intoxication while carrying classified materials or that causes one to speak inappropriately about classified matters or to unauthorized persons.
- Deliberate revelation of classified information to unauthorized persons to impress them with one's self-importance.
- Copying classified information in a manner designed to obscure classification markings. This may indicate intent to misuse classified information.
- Making unauthorized or excessive copies of classified material. Going to another office to copy classified material when copier equipment is available in one’s own work area is a potential indicator of unauthorized copies being made.
- Failing to report requests for classified information from unauthorized individuals.

Failure to report a security violation is itself a security violation and may be a serious concern. After the arrest of Navy spy Jerry Whitworth, who was part of the infamous John Walker spy ring, interviews with Whitworth's work colleagues identified one who had noticed classified papers in Whitworth's personal locker, another who had observed Whitworth monitoring and copying a sensitive communications line without authorization, and a third who knew Whitworth took classified materials home with him but believed he was doing it only to keep his work current. Failure to report these violations enabled Whitworth's espionage to continue.

Storing classified information at home is a very serious concern as it may indicate current or potential future espionage. At the time of their arrest, many well-known spies were found to have large quantities of classified documents at their residences. CIA spy Aldrich Ames had 144 classified documents at his home, while Edward Moore had 10 boxes of CIA documents at home. Of various Navy spies,

Jonathan Pollard had a suitcase full of classified materials, Michael Walker had 15 pounds of classified material, while Samuel Morison had two portions of Navy documents marked Secret.

Secure Use of Office Network

Government and most organizations in the private sector conduct their business in a networked environment that is guided by policies designed to protect the integrity of their network from hackers, protect their information from competitors or spies, and protect their organization from law suits that may be triggered by computer misuse. Government and industry devote substantial resources to creating, refining, and enforcing security procedures. You are responsible for becoming familiar with and complying with your organization's network security policies, procedures, and best practices. You should also become familiar with the separate module on Computer Vulnerabilities. The information here is repeated in that module along with considerable additional information relating to computer security.

Any misuse of your employer's secure network is sometimes illegal, often unethical, and always reflects poor judgment or lack of care in following security rules and regulations. Misuse may, unintentionally, create security vulnerabilities or cause the loss of information that should be protected. A pattern of inability or unwillingness to follow rules for the operation of the office computer network raises serious concerns about an employee's reliability and trustworthiness.

As we store more and more information in computer data bases, and as these data bases become more closely linked in networks, more people have broader access to more information than ever before. Computer technology has magnified many times the ability of a careless or disaffected employee to cause severe damage.

Owing to the magnitude of problems that can be caused by misuse of your office network, Misuse of Information Technology Systems is now one of the 13 criteria used in adjudicating approval or revocation of security clearances for access to classified information.

Large organizations are particularly vulnerable to a type of security attack called "social engineering." That's what hackers call conning legitimate computer users into providing useful information that helps the hacker gain unauthorized access to your organization's computer network.

The hacker pretends to be someone else, such as a senior officer in your organization, a new employee, or someone from your Help Desk. This person contacts you with a request or a question and engages you in conversation to get the desired information. It is often done by telephone, but may also be done by forged email messages, instant messaging or even an in-person visit. Be sure to read about it in Social Engineering and the two related case studies as this practice has a long history of success in penetrating otherwise secure organizations.

The next section provides a list of rules for the secure use of your office computer. After that is a list of behaviors that are not directly related to security but are widely regarded as a misuse of your computer.

Security Rules

The following are basic rules for secure use of your office computer:

- Do not enter into any computer network without authorization. Unauthorized entry into a protected or compartmented computer file is a serious security violation. It can be a basis for revocation of your security clearance. Whether motivated by the challenge of penetrating the system or by simple curiosity to see what is there, unauthorized entry is a deliberate disregard for rules and regulations. It can cause you to be suspected of espionage. At a minimum, it violates the need-to-know principle and in some cases is an invasion of privacy.
- Do not store or process classified information on any system not explicitly approved for classified processing.
- Do not ever attempt to circumvent or defeat the security or audit features of a system. Such an endeavor can only be permitted with the written consent and knowledge of the system owner.
- Do not install any software on your computer without the approval of your system administrator.
- Do not modify or alter the operating system or configuration of any system without first obtaining permission from the owner or administrator of that system.
- Do not use your office computer to gain unauthorized access to any other network.
- Do not use another individual's user ID, password, or identity.
- Do not permit an unauthorized individual (including spouse, relative or friend) access to any sensitive computer network.
- Do not reveal your Personal Identification Number (PIN) or password to *anyone* -- not even your network system administrator. See User Authenticaion and Passwords.
- Do not respond to any telephone call from anyone whom you do not personally know who asks questions about your computer, how you use your computer, or about your userid or password. See Social Engineering.
- Do not run scanning software which provides information about the network which can be used to hack into network assets without written authorization. Do not monitor the network, the data traversing it, or network traffic patterns.
- If you are the inadvertent recipient of classified or other protected information

sent via email or become aware of such information on an open bulletin board or website, you must report this to the security office.
- If available, use a locked screensaver to make certain no one can perform any activity under your User ID while you are away from your desk. Screensavers can be set up so that they activate after the computer has been idle for a specified time. Strange as it may seem, a coworker erasing or sabotaging your work is not uncommon. Or imagine the trouble you could have if nasty email messages were sent to your boss or anyone else from your computer, or your account were used to transfer illegal pornography.

Inappropriate Uses

Many offices permit some personal use of office equipment when such personal use involves minimal expense to the organization, is performed on your personal non-work time, does not interfere with the office's mission, and does not violate standards of ethical conduct.

The following activities are considered to be misuse of office equipment:

- Creating, downloading, viewing, storing, copying, or transmitting sexually explicit or sexually oriented materials. This can cause you to be fired from your job. Child pornography is a crime that will be prosecuted to the full extent of the law.
- Annoying or harassing another individual, for example through uninvited email of a personal nature or using lewd or offensive language. This can be grounds for firing you from your job, as the organization can be held legally liable for information transmitted over its network.
- Any other activity that is illegal, inappropriate, or offensive to fellow employees or the public. Such activities include hate speech or material that disparages others on the basis of race, creed, religion, color, sex, disability, national origin, or sexual orientation.
- Using the office computer for gambling.
- Using the computer for commercial purposes or in support of "for-profit" activities, or in support of other outside employment, business activity (e.g., consulting for pay, sales or administration of business transactions, sale of goods or services).
- Engaging in any outside fund-raising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- Creating, copying, transmitting, or retransmitting chain letters or other unauthorized mass mailings.
- Posting office information to any external blog, newsgroup, chat room, social

network, or other public forum without prior approval for public release.

- Any personal use that could cause congestion, delay, or disruption of service to any office equipment. This includes data streaming, sending pictures, video, sound files, or other large file attachments that can degrade computer network performance.
- Unauthorized acquisition, use, reproduction, transmission, or distribution of any controlled information. This includes copyrighted computer software; other copyrighted or trademarked material or material with intellectual property rights (beyond fair use); privacy information; and proprietary data or export-controlled data or software.
- Participating in any other prohibited activity.

Monitoring of Your Computer Use

All of your actions while you are online on a government or corporate network can be, and likely are being, monitored. Many government offices and most large corporations do this to ensure compliance with security regulations, protect themselves from loss of information, and protect themselves from law suits. An organization can be held liable for abusive, harassing, or other inappropriate messages sent over its computer network.

A 2009 survey of 220 large (over 1,000 employees) companies in the United States found that: 1

- 31% of the companies had fired at least one employee for violating email policies during the previous 12 months.
- 33% of companies surveyed employed personnel whose primary or exclusive function is to read or otherwise monitor outbound email.
- 34% of the surveyed companies said their business was impacted by the exposure of sensitive or embarrassing information during the previous 12 months.
- 43% investigated a suspected email leak of confidential or proprietary information in the previous 12 months.
- 24% said that employee email had been subpoenaed for law suits.

Using the SIPRNet

The Secret Internet Protocol Router Network (SIPRNet) is the Department of Defense network for the exchange of classified information and messages at the SECRET level. It supports the Global Command and Control System, the Defense Message System, and numerous other classified warfighting and planning applications. Although the SIPRNet uses the same communications procedures as the Internet, it has dedicated and encrypted lines that are separate from all other communications systems. It is the classified counterpart of the Unclassified but Sensitive Internet Protocol Router Network (NIPRNET), which provides seamless interoperability for unclassified combat support applications and controlled access to the Internet.

Access to the SIPRNet requires a SECRET level clearance or higher and a need to have information that is available only on the SIPRNet. Because the SIPRNet is an obvious target for hostile penetration, a number of strict security procedures are applied. Appropriate credentials and two-factor authentication are required. When using the SIPRNet, you must not leave the workstation unattended.

A computer with a non-removable hard drive used to access the SIPRNet must be located in an area approved for open storage of SECRET information. A computer with a removable hard drive does not have to be in an open storage location, but the hard drive must be appropriately marked with the classification of the material it contains and, when not in use, must be removed and stored in a container approved for the storage of SECRET information. If physical keys are used, they will be numbered and stored in a container approved for the storage of SECRET material.

Linking a computer with access to the SIPRNet to the Internet or to any other computer or media storage device that has not been approved for use with SECRET information is a serious security violation. Once any media storage device such as a CD or thumb drive has been connected to a computer with access to the SIPRNet, it becomes classified at the SECRET level. It must be protected accordingly and shall not be used on any unclassified computer.

Technological advances in storage devices are making it easier for classified information to be removed from secure areas. Data-storage devices such as Personal Digital Assistants (PDA), Key-chain drives, Memory watches etc, should not be allowed in an environment where classified information is processed because of their infrared and similar recording capabilities. For computers used to process classified information, it is recommended that infrared (IR) port beaming capability be disabled. If the IR port is unable to be disabled, cover the IR port with metallic tape.

The SIPRNet system maintains an audit trail of all users. This includes the identity of all persons accessing or attempting to access the SIPRNet, date and time of logon/logoff, and any noteworthy activities that might indicate an attempt to modify, bypass, or negate security safeguards.

State, Local, Tribal,
and Private Sector Entities

Historically, classified national security information has been shared only at the national level. Presidential Executive Order 13549, dated August 18, 2010, established a new Classified National Security Information Program designed to safeguard and govern access to classified national security information shared with state, local, tribal, and private sector (abbreviated as SLTPS) entities.

Department of Homeland Security spelled out the details for implementing this program in its February, 2012, directive, "Classified National Security Information Program for State, Local, Tribal, and Private Entities." The goal of this program is improved sharing of information related to domestic terrorism.

The STLPS rules for protecting classified information are generally they same as for Federal Government personnel, but the following points warrant mentioning here.

- The Homeland Security directive establishes a SLTPS Policy Advisory Committee as a forum to discuss SLTPS policy issues and make recommendations on proposed changes to policies and procedures.
- All information provided by a Federal agency to a STLPS entity shall remain under the control of the Federal Government.
- Personnel security clearances may be issued to SLTPS personnel, but only when the "write-for-release principle" that allows for the sanitation of classified information to the sensitive but unclassified level is inadequate. Those personnel selected for the granting of a security clearance shall have a demonstrated and foreseeable need for access to classified information and be in a position to capitalize on the value the classified information provides.
- Access to Sensitive Compartmented Information (SCI) may be granted on a case by case basis, when the person to whom the access is to be granted is or will be an active and continuing participant in or member of a Federally sponsored board, committee, working group, task force, operations center, or other entity where the integration of SLTPS personnel is essential and participation or membership requires or will require access to SCI.
- Classified information originating in one agency may be disseminated to another agency or to a SLTPS entity without the consent of the originating agency, as along as the criteria for access are met, unless the originating agency has determined that prior authorization is required for such dissemination and has marked or indicated such requirement on the medium containing the classified information.

- Documents created prior to June 28, 2010, shall not be disseminated to any other agency or SLTPS entity to which it has been made available without the consent of the originating agency.
- Reproduction of classified material must be done only on machines that have been approved for classified reproduction by DHS SLTPS/SMD or the sponsoring Federal agency, and such machines must not be connected to an unclassified LAN, allow for remote diagnostics, or be equipped with a hard-drive or other devices that retain memory or images.
- Any maintenance performed on a machine that has been used for the reproduction of classified information will be done by a cleared person or under the observation of a cleared person.
- Classified information shall not be sent through any type of inter-office distribution system.
- SLT personnel, and PS personnel that fall under the SLTPS Program, who have a justified need to hand-carry classified information outside of the building where the information is stored, require approval from DHS SLTPS/SMD or the sponsoring Federal agency. There is a special procedure for obtaining this approval.

Emergency Authority

In emergency situations in which there is an imminent threat to life or in defense of the homeland, agency heads or their designees may authorize the disclosure of classified information to an individual or individuals who are otherwise not routinely eligible for access. When this is done, the following conditions must be met:

- Limit the amount of classified information disclosed to the absolute minimum to achieve the purpose.
- Limit the number of individuals who receive it.Transmit the classified information via Federal Government channels by the most secure and expeditious method approved for transmission of classified information, or other means deemed necessary when time is of the essence.
- Provide instructions about what specific information is classified, how it should be safeguarded; physical custody of classified information must remain with an authorized Federal Government entity, in all but the most extraordinary circumstances.
- Provide appropriate briefings to the recipients on their responsibilities not to disclose the information and obtain a signed nondisclosure agreement.
- Within 72 hours of the disclosure of classified information, or the earliest opportunity that the emergency permits, but no later than 30 days after the release, the disclosing authority must notify the originating agency and provide information on what information was disclosed to whom and why, how the information was disclosed or transmitted; and how the information is being safeguarded now. A description of the security briefing that was provided and a copy of the signed nondisclosure agreement(s) should also be provided.