

Unit 5. Security

5-1. Information Security	5-1
024. Identifying classification directives and levels	5-1
025. Identifying classification authority	5-3
026. Using special handling instructions	5-6
027. Identifying foreign government information	5-7
028. Marking documents and products.....	5-10
029. Documenting receipt and transfer of classified material.....	5-14
030. Accounting for classified material	5-16
031. Safeguarding classified material.....	5-19
032. Destroying classified material	5-22
033. Releasing and disclosing classified information.....	5-23
034. Handling NATO classified	5-25
5-2. Other Security Related Programs.....	5-27
035. Operations Security	5-27
036. Communications Security.....	5-30
037. Computer Security	5-32

THIS unit provides information you need in order to protect classified information. As a member of the Air Force, you have taken an oath to protect and defend the United States from its enemies, both foreign and domestic. Part of that defense must be the safeguarding of classified information to which you have access. Regardless of whether the information is of the plain-vanilla variety or a more exotic mixture, you must be aware of how to protect it. We'll discuss identifying, marking, accounting for, safeguarding, and releasing classified material. Remember these as the five pillars of information security. Should one crumble, the entire building could collapse!

5-1. Information Security

The phrase "There is more than one answer to every question" is so true when it comes to classified information. It is absolutely vital that you know the classification of the source of your information and the classification of your end product to your customers. Part of your job will be to answer questions. You'll find that often your answers will be vague at the unclassified level and generally at the Secret level; however, the true answer often comes from Top Secret sources. Knowing the classification directives, levels, authorities, handling instructions, and how to deal with foreign information will help you answer questions without compromising classified information.

024. Identifying classification directives and levels

Directives

DoD 5200.1R, *Information Security (INFOSEC) Program*, and AFI 31-401, *Information Security Program Management* provides the basic policy on why we classify and the different levels of classification. The basic DoD policy is to make available to the public as much information as possible. Security classifications are applied only to protect national security.

Executive Order (EO) 12958, *Classified National Security Information*, addresses the changing needs for classification guidance. EO 12958 became effective 14 October 1995, and was revised in March

of 2003. This executive order established a process to identify information that must be protected as national security information.

Another directive with which you should be familiar is EO 12951, *Release of Imagery Acquired by Space-Based National Intelligence Reconnaissance Systems*. EO 12951 establishes procedures for the future declassification of imagery intelligence. Dated 22 February 1995, this executive order specifies the authority and duration of classification for satellite imagery.

Levels

When a need exists to classify information, the following three categories of classifications may be applied:

Top Secret (TS)

Top Secret identifies national security information or material that requires the *highest degree* of protection. Unauthorized disclosure of this information could reasonably be expected to cause exceptionally grave damage to the national security. Examples of exceptionally grave damage include the following:

- Armed hostilities against the US or its allies.
- Disruption of foreign relations vitally affecting national security.
- The compromise of vital national defense plans or complex cryptologic and communications intelligence systems.
- Revealing sensitive intelligence operations.
- The disclosure of scientific or technological developments vital to national security.

Secret (S)

Secret identifies national security information or material that requires a substantial degree of protection. Unauthorized disclosure of this information could reasonably be expected to cause serious damage to national security. Examples of serious damage include the following:

- Disruption of foreign relations significantly affecting national security.
- Significant impairment of a program or policy directly related to national security.
- Revealing significant military plans or intelligence operations.
- Compromise of significant military plans or intelligence operations.
- Compromise of significant scientific or technological developments relating to national security.

Confidential (C)

Confidential identifies national security information or material that requires some protection. Unauthorized disclosure could reasonably be expected to cause damage to national security. Examples of such damage include the following:

- The compromise of information that indicates the strength of ground, air, and naval forces in the US and overseas areas.
- Disclosure of technical information used for training, maintenance, and inspection of classified munitions of war.
- Revealing performance characteristics, test, design, and production data on munitions of war.

Special Access Program (SAP)

A special access program is one imposing need-to-know or access controls beyond those normally required. Such a program includes, but is not limited to, special clearance, adjudication or

investigative requirements, special designation of officials authorized to determine need-to-know or special lists of persons predetermined to have a need-to-know. Throughout your Air Force career, you will probably be indoctrinated into a number of these programs. The most common of these is Sensitive Compartmented Information (SCI).

Sensitive Compartmented Information (SCI)

SCI is classified information concerning, or derived from, intelligence sources, methods, or analytical processes that are required to be handled exclusively within formal access control systems established by the Director of Central Intelligence (DCI). All persons requiring access to SCI must have a Single Scope Background Investigation (SSBI) or SSBI-periodic reinvestigation prior to being indoctrinated into this program. Refer to AFMAN 14-304, *The Security, Use, and Dissemination of Sensitive Compartmented Information (SCI)* for additional information

025. Identifying classification authority

Only a few designated officials have the authority to assign an original security classification, and they cannot delegate this authority. When these officials are not available, we need guidelines for assigning a classification. These guidelines are found in security classification guide AFI 31-401 and AFMAN 14-304.

Classification guides

The security classification guide serves as written guidance of classification and declassification decisions on specific information for particular subjects or areas. It provides an authoritative basis for assigning or canceling a security classification. When you have a question concerning the proper classification to be assigned, use one of the classification guides for definitive guidance. Applying an improper classification may result in compromise of the information that needs to be protected.

Derivative classification

This is new material that derives its classification from information already classified. When you incorporate, restate, paraphrase, or generate material that is already classified, you must ensure the new material is appropriately classified. To do this, you must accomplish the following:

1. Respect the original classification decisions.
2. Verify the information's current level of classification as much as practical before assigning the new classification.
3. When the classification of a document is derived from more than one source document, classification guide, or a combination thereof, indicate "MULTIPLE SOURCES" on the "Classified by" line.
4. Provide a record of the multiple sources in the form of a letter or memorandum, which can be placed with the actual file, or record copy of the affected document.
5. Carry forward to the new material or document the assigned dates or X-series declassification codes (see page 5-5).

Reasons for classification

EO 12958, section 1.5 provides several reasons for the classification that is assigned to information. Information may not be considered for classification unless it concerns any of the following:

- (a) Military plans, weapon systems, or operations.
- (b) Foreign government information.
- (c) Intelligence activities (including special activities), intelligence sources or methods, or cryptology.
- (d) Foreign relations or foreign activities of the US, including confidential sources.

- (e) Scientific, technological, or economic matters relating to national security.
- (f) US Government programs for safeguarding nuclear materials or facilities.
- (g) Vulnerabilities or capabilities of systems, installations, projects or plans relating to the national security.

On 25 March 2003, the President signed Executive Order 13292, which amended EO 12958. Some of the major changes to EO 12958 include the following:

- Extended the automatic declassification deadline by three years to allow agencies to complete reviewing the backlog of classified historical records more than 25 years old.
- Broadened the authority of agencies to reclassify information that has not been disseminated publicly, but only under strictly controlled circumstances.
- Broadened the protection of confidential foreign government information while ensuring that such information remains subject to automatic declassification.
- Simplified the process for classifying records for more than 10 years and less than 25 years.
- Makes explicit the authority of the Director of Central Intelligence to protect intelligence sources and methods

One of the issues that arose in the wake of 9/11 was awareness of the limitations imposed by the lack of authority under EO 12958 to pass classified information to persons not otherwise eligible (e.g. local and state authorities) in an emergency. As a result, EO 13292 added a section specifically authorizing an agency head or designated person to share classified information with individuals not otherwise eligible to receive it, and specifying procedures to be followed. This is especially important in the context of homeland security.

Resolution of doubts

You now know what authority you have to classify information. What would you do if you had information that you felt could be classified but you could not find a source? There is an interim measure to use until you can either find a classification source document or query the appropriate classification authority; you can protect the information as if it were classified CONFIDENTIAL. You use similar logic when you have reasonable doubt about an appropriate classification level. For example, if you have information marked CONFIDENTIAL, but believe it to be SECRET, then safeguard it at the higher level pending determination by a classification authority.

Unclassified information of possible intelligence value

Not all of the material we work with in the intelligence field is classified. We also deal with unclassified information on a daily basis. For example, you may use regulations, access and recall rosters, military orders, and other materials when accomplishing your job. You probably handle such material very casually without a second thought. Now place yourself in the position of an enemy intelligence specialist. Would any of this material benefit you in the processing of intelligence? You're answer should be a definite yes. All of this information may be harmless separately, but when compiled, it may become valuable intelligence for our enemy. The protection of this type of material and unclassified information of possible intelligence value falls under the OPSEC program. See your OPSEC manager or representative for more information. This form of information is in direct support of or is otherwise directly associated with classified information. It contributes to the knowledge of the classified aspects of the program or operation. It also includes unclassified information, which when combined with other unclassified information, reveals insight or aspects of classified plans, programs, operations, or information. Generally speaking, information of this nature falls into one of the two following categories:

Essential Elements of Friendly Information (EEFI)

EEFI includes information concerning a plan, project, or activity that, if acquired by the hostile intelligence threat, may jeopardize the successful execution of the mission. All major commands (MAJCOM) and separate operating agencies (SOA) are required to develop EEFI to meet their own operational requirement. EEFI parallel the key questions about friendly operations, capabilities, intentions, or activities likely to be asked by an opposing commander and are found in the OPSEC annex of an operations plan (OPLAN). An awareness of your unit's EEFI should make you think twice before releasing information outside official military channels. The bottom line is that EEFI represent unclassified questions that an opposing commander may ask. The answers to those questions may constitute classified information. Some of the typical EEFI you may encounter include the following:

- Changes to unit mission.
- Changes to organization.
- Introduction of new equipment.
- Security clearances of individuals.
- Equipment shortages effecting readiness or efficiency.
- Equipment or system performance.
- Mapping requirements that indicate operational intent.
- The classification of operations or programs.

For Official Use Only (FOUO)

FOUO is designed to protect information that must be withheld from widespread distribution to the public. The primary use for FOUO within the USAF is to protect personal information. It can also be used in other cases where the release of information may reveal operational capabilities or deficiencies that the enemy could exploit to its advantage. Reasonable measures must be taken to safeguard FOUO information; e.g., placing it in a locked room, filing cabinet, or desk if the area is open to non-government personnel. The following is some material that would be considered FOUO:

- Security access rosters.
- Personal Air Force records.
- Unclassified portions of CDCs.
- Unclassified inspector general (IG) reports.

Declassification

At the time of original classification, the original classifying authority (OCA) attempts to establish a specific date or event for declassification, based upon the duration of the national security sensitivity of the information. If the original classification authority cannot determine an earlier specific date or event for declassification, information is marked for declassification 10 years from the date of the original decision. However, the OCA may apply an automatic declassification exemption code to specific information, if it can reasonably be expected that the unauthorized disclosure of the information would cause damage to national security for a period of greater than 10 years. Which of the eight exemption codes the OCA applies depends on what might happen if the information was disclosed. The following codes apply if the release of the information could reasonably be expected to:

- X1 - Reveal an intelligence source, method, or activity, or a cryptologic system or activity.
- X2 - Reveal information that would assist in the development or use of weapons of mass destruction (WMD).
- X3 - Reveal information that would impair the development or use of technology within a United States weapon system.

- X4 - Reveal United States military plans or national security emergency preparedness plans.
- X5 - Reveal foreign government information.
- X6 - Damage relations between the United States and a foreign government, reveal a confidential source, or seriously undermine diplomatic activities that are reasonably expected to be ongoing for a period greater than 10 years.
- X7 - Impair the ability of responsible United States Government officials to protect the President, the Vice President, and the other individuals for whom protection services, in the interest of national security, are authorized.
- X8 - Violate a statute, treaty, or international agreement.

026. Using special handling instructions

Based on the type of information, an originating department or agency will sometimes provide special controls for classified information. They may provide additional protection for the sources and methods used to obtain the information. These special handling instructions or control markings are called *caveats*.

Caveats

Caveats are used as additional warnings to restrict the distribution of classified material. Some caveats identify who may view the material, while others identify who may not be provided the material. There are hundreds of caveats in use today and I will not attempt to list them all. The following is just a *sample* of the most common ones.

Not Releasable to Foreign Nationals (NOFORN)

This caveat is used to identify classified intelligence that may not be released in any form to foreign governments, foreign nationals, or non-US citizens without the originator's permission. It is also used on intelligence that, if released to a foreign government or national, could jeopardize intelligence sources or methods. The caveat NOFORN is also used to control who receives foreign intelligence or related material requiring SCI protection. Mark the individual pages and internal paragraph classifications with the abbreviation NOFORN or NF immediately following the classification; i.e., SECRET-NOFORN or (S-NF).

Release To:

This caveat is used to identify intelligence that an originator has predetermined to be releasable through established foreign disclosure procedures and channels to specific foreign countries. The name of each country the information is releasable to must be specified within the caveat; i.e., "THIS INFORMATION HAS BEEN AUTHORIZED FOR RELEASE TO UNITED KINGDOM, CANANDA, AND AUSTRALIA." This warning notice may be abbreviated as "REL UK/CAN/AUS" for use on individual pages and for internal paragraph markings. Remember that you cannot use both NOFORN and the Release To caveats at the same time. Either indicate the information is not releasable to any country or indicate which specific countries are authorized to receive the information.

Special Category (SPECAT)

This caveat is used on classified messages to identify special projects or subjects. The SPECAT designator identifies a message as requiring special handling beyond that normally given because of its security classification. Only personnel in telecommunications, administration, and user channels, who are properly cleared and authorized access, may handle and view SPECAT-designated messages. The SPECAT caveat is followed by Exclusive for (name) or a specific identification, acronym, or codeword of the project or subject with which identifies.

Limited Distribution (LIMDIS)

The LIMDIS designator is used on classified messages identified with specific projects or subjects that must receive LIMDIS and special accessing in administrative support and user channels. According to AFI 34-401, the Air Force does not authorize use of LIMDIS controls to any material except message distribution.

027. Identifying foreign government information

Intelligence personnel often have access to and are required to maintain foreign government information that is classified. This information is released to the US by foreign governments or international organizations with the understanding that it will be protected from unauthorized disclosure. We must protect this information as we would US classified information. In addition, some foreign classified information is protected within special dissemination or need-to-know access control systems.

Foreign classification

Foreign government information is routinely given a security classification designation by the government or international organization that originated it. Most of these classification designations do not parallel those applied to US Government information. Several countries and organizations also have an additional security classification titled “Restricted.” The host country will designate the control on restricted information; however, if you are not sure of the classification, always control the material as Confidential.

Classifying foreign government information

If the security classification designation of foreign government documents is shown in English, you will not have to apply any other classification markings. However, if the foreign classification designation is not shown in English, the equivalent overall US classification must be applied conspicuously on the document.

Incorporating foreign government classified

On occasion, you may be required to include foreign government information in some of your intelligence products. These products must be identified in a manner that ensures the information is not declassified prematurely or made accessible to persons without the consent of the originator. You can satisfy this requirement by placing the notation “FOREIGN GOVERNMENT INFORMATION” on the face of the document. You must also include any necessary portion or paragraph markings. For instance a paragraph that contains Secret United Kingdom (UK) information should contain the paragraph marking (UK-S) at the beginning.

Foreign restricted or NATO restricted

If you include foreign restricted or NATO restricted information in an otherwise unclassified document, you must give the document the overall classification of Confidential. These documents will also require appropriate portion and paragraph classification markings. (We’ll cover NATO classified material requirements in more detail later in this volume.)

Foreign government “CLASSIFIED BY” line

The “Classified by:” line of DoD documents containing only foreign government information *normally* includes the identity of the foreign government or international organization that originated it. For example, it might appear as “Classified by: Government of Australia” or “Classified by: NATO.

Summary

In the past few units, we’ve covered the directives and levels of classified material, the authority by which it is classified, and special handling instructions. We also looked at how foreign government

information is classified and handled. In the next unit we'll examine how classified information is marked and accounted for.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

024. Identifying classification directives and levels

1. What two regulations provide the basic DoD policy on why we classify information?
2. Why are security classifications applied to information?
3. What type of classified information requires the *highest* degree of protection?
4. What level of classified information would cause *exceptionally* grave damage to national security if compromised?
5. What type of damage would be caused by the disclosure of significant military plans or intelligence operations?
6. Compromise of information classified as Confidential would be expected to cause what to national security?
7. What is required prior to an individual being indoctrinated into SCI?

025. Identifying classification authority

1. What is a classification guide?
2. What is derivative classification?
3. Who decides how long information remains classified?

4. How should a classified document be marked when the original classification authority is unable to determine a specific declassification date?
5. What should you do with information that is marked Secret when you believe it may be Top Secret?
6. What Air Force program protects information of possible intelligence value?
7. List at least four examples of Essential Elements of Friendly Information (EEFI).
8. List at least three examples of material that should be protected as For Official Use Only (FOUO).
9. What is downgrading and declassifying information based on?
10. Which declassification code should be applied to a classified document if the release of the information could reasonably be expected to reveal information that would impair the development or use of technology within a US weapon system?
11. Which declassification code should be applied to a classified document if the release of the information could reasonably be expected to violate a statute, treaty, or international agreement?

026. Using special handling instructions

1. What is a caveat?
2. What caveat is used to identify classified information that may not be released in any form to foreign governments?
3. What caveat would be used to identify information that can be released to Canada?

4. What caveat is used on classified messages to identify special projects or subjects?

027. Identifying foreign government information

1. How should foreign government information that is marked “Restricted” be protected?
2. What should you do if a document containing foreign government information is marked in a foreign language?
3. When would you mark a document “FOREIGN GOVERNMENT INFORMATION”?

028. Marking documents and products

Classified information must be clearly identified. Marking is the primary means of telling the holders of classified information the protection requirements for that information. We discussed earlier the various levels of classifications and the many caveats associated with them. Identifying the information is classified is the first step to safeguarding the material; however, if the material is then improperly marked, the chance of a compromise is increased. The overall classification marking of the document must be conspicuous enough to alert anyone handling the document, that it is classified.

Hand marking documents

Every classified document or product must be marked to show the highest classification of information it contains. This marking must be conspicuous enough to alert anyone handling it that it is classified. When you use or produce items from classified documents or materials; they must be properly classified and marked. To do this, apply the appropriate security markings or announcements, using stamp-in letters larger than the text. These include the following:

1. Overall classification.
2. Classification source (the “Classified by” line).
3. Reason for classification (the “Reason” line).
4. Downgrading or declassification instructions (the “Declassify on” line).
5. Portion markings.

Marking SCI caveats and code words

Mark SCI with the applicable SCI control system caveat at the bottom of all pages of hard copy documents, including any front and back covers. Mark material warranting SCI codeword or operational program designator protection immediately following the security classification on all pages containing such information.

Automated marking of documents

For documents produced by automatic data or word processing equipment, the markings may be in letters the same size as the text, provided they are applied by the printing equipment and highlighted by asterisks and spacing. Some examples are as follows:

SECRET or ***** SECRET *****

Placement of markings on documents

The placement of the markings should follow these steps:

1. The overall highest level of classification of a document must be centered at the top and bottom of the front and back covers, title page, and first page, if there are any. Subjects and titles of classified documents are also marked using parentheses.
2. When possible assign unclassified subjects and titles to documents. If this is not possible, you must include an unclassified short title for reference purposes, transmittal documents, and destruction certificates.
3. You must mark the overall classification at the center top and bottom of any addition; i.e., an endorsement that covers the first page of the document.
4. Classify interior pages of a document at the center top and bottom with the highest classification based on the contents of that page. Interior pages may be marked with the overall classification of the document when such marking is necessary to achieve production efficiency. The information is otherwise sufficiently identified by paragraph classification markings.
5. Handle and mark major components (attachments, units, annexes, etc.) of complex documents and material as separate documents.
6. Each section, part, paragraph, or similar portion of a classified document will be marked to show the level of classification. In most cases, parentheses will be used for portion markings; e.g. (TS) for Top Secret, (S) for Secret, (C) for Confidential, and (U) for Unclassified. When appropriate, the additional warning notices or control markings must also be added.
7. When marking paragraphs of a classified document, you must place the marking immediately before the paragraph. If letters or numbers are used to identify paragraphs, the marking will appear after the letter or number but before the paragraph.
8. If the document contains illustrations, photographs, figures, graphs, drawings, charts, and similar portions, you must clearly mark the unabbreviated classification within, beside, or next to each one. If captions are included, they will be marked on the basis of their content alone by placing the appropriate marking immediately before the caption.

An example of a document containing these markings can be seen in Figure 5-1.

	SECRET//X1 OFFICE OF THE SECRETARY OF DEFENSE WASHINGTON, DC	Date
	<p>MEMORANDUM FOR DASD (I&S)</p> <p>SUBJECT: Classification Markings (U)</p> <p>1. (U) This is an example of a document that contains originally classified information. Standard markings are required for all documents as shown here. These markings include:</p> <ul style="list-style-type: none"> a. (U) Portion marking(s) for each section of a document to reflect the classification of the information. When using subsections such as shown here, individual markings are used. When subsections are not marked, the information is protected at the level of protection shown by the overall section. b. (U) Overall markings - conspicuously annotated using larger font size or bold-face print. c. (U) A "Classified by" line that includes the name or personal identifier and position of the originator. d. (S) A reason for classification. e. (U) A "Declassify on" line that indicates the following: <ul style="list-style-type: none"> (1) The date or event for declassification not to exceed 10 years, or: (2) An extension beyond the initial 10 years, using X-series declassification codes. <p>2. (S) If this paragraph contained "Secret" information, the portion would be marked with the designation "S" in parentheses. If the paragraph contained "Confidential" information, the portion would be marked with the designation "C" in parentheses.</p> <p>Classified by: Buster Keaton ASD(C3I)</p> <p>Reason: 1.5 (a) and (d)</p> <p>Declassify on: December 31, XXXX</p>	
SECRET//X1		

Figure 5-1. Sample classified document.

Classified working papers

These are documents and materials accumulated or created in the preparation of a finished product. As a minimum, they are dated when created and marked with the highest classification of any information contained in them. They are also accounted for, controlled, and marked in the same way as a finished document. Working papers should be destroyed when no longer needed.

Marking products other than documents

Much of the classified material you work with will come in some form other than a document. This material must be marked to identify its classification level. These markings could be in the form of a tag, sticker, decal, or similar device. If the material cannot be marked, written notification of the security classification must be furnished to the recipients. The following procedures for marking various types of material are not all-inclusive and may be varied to accommodate the physical characteristics of the material. Consult your unit classification guide for additional guidance.

Maps, charts, and drawings

You must mark the classification level of the legend, title, or scale blocks in a manner that distinguishes the classification of the legend from the classification of the map, chart, or drawing. The highest classification of information appearing on the product must be inscribed at the top and bottom, front and back. You must also apply additional markings that are clearly visible when the map, chart, or drawing is folded.

Photographs and film

Negative and positive photographs must be marked to ensure that a viewer will know that classified information is involved. Mark the appropriate classification at the beginning and end of each strip for roll negatives and positives. Film containers must also bear classification markings. If possible, the face side of prints and reproductions should contain applicable classification markings, but annotations on the reverse side are also acceptable.

Transparencies and slides

When possible, classification markings must be clearly applied to the image of each transparency or slide. If the markings are not visible until projected on a screen; i.e., 35-millimeter slides, the classification markings must also be placed on the border, holder, or frame. Although not specifically required, it is standard practice to apply the markings on both the imagery and the frames in all cases. If slides and transparencies are being controlled as a set, only the lead slide must be marked with associated markings such as classification authority, declassification instructions, date, etc. All remaining slides in the set must bear their individual classifications. Any classified slide or transparency permanently removed from a set must be marked as a separate document.

Motion picture films and videotapes

Classified motion picture films and videotapes are marked at the beginning and end with the overall classification of the recording and must be visible when projected. Associated markings must appear at the beginning of the film or tape. When not being viewed, they must be kept in containers bearing conspicuous classification and associated markings.

Computer media

The procedures for classifying, controlling, storing, declassifying, and destroying classified computer media are the same as for other forms of material containing classified information. Various forms of computer media are reusable and include hard disks, floppies, ribbons, and tapes. When reusing these media forms, you must be aware of the highest classification previously stored on that media and control it appropriately. Removing the classified and declassifying the medium can eliminate this requirement. Some special security control considerations for most forms of computer media are as follows:

- Removable information storage media used with automated data processing (ADP) equipment such as computers, video disk (VD) players, optical disk (OD) readers, compact disk read only memory (CD ROM) units, word processors, or electronic typewriters require clearly visible external classification and associated markings. The media that you may come in contact with are magnetic tapes, disc packs, compact disks, video disks or diskettes.
- Place a clearly visible external classified marking on the media. Standard Form (SF) 706 will be placed on Top Secret ADP storage media, SF 707 will be placed on Secret ADP storage media; SF 708 will be placed on Confidential ADP storage media, SF 710 will be placed on Unclassified ADP storage media.
- At least one SF 711 ADP media descriptor label will be placed on all ADP storage media regardless of classification. This media also requires internal classification markings to ensure that classified information will bear classification and associated markings if it is reproduced or generated in hard copy.

To prevent inadvertent compromise, storage media must reflect the highest classification ever processed by that machine. If you want to release the storage media at a lower classification, a qualified individual using one of many diagnostic programs to ascertain proper classification level must first check it.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

028. Marking documents and products

1. Where is the highest overall classification of a document marked?
2. How should interior pages of a document be marked?
3. Where do you place the classified markings for a paragraph?
4. What are the two minimum markings required for working papers?
5. Where is the overall classification of a map or chart placed?
6. What is the classification of a Secret slide within a set of slides with an overall classification of Top Secret?
7. What form is placed on all unclassified automated data processing storage media?

029. Documenting receipt and transfer of classified material

Because of the nature of our career field, accounting for classified material will become a habit over time. Most of you will handle a considerable amount of classified material that will require you to document its receipt and transfer, and it is very important that you pay close attention to the security requirements involved.

Document procedures

Receiving and transferring classified material means moving it from one place to another by any means. Classified materials are dispatched through the Defense Courier Service (DCS) Armed Forces Courier Service, US Postal Service (USPS), State Department courier, Federal Express (FED-EX) (material must clear the FED-EX accounting system by the weekend), or by hand-carrying methods. Intelligence gathering generates the need to move large volumes of information. Electronically

transmitting all this data is not only impractical, but also impossible. Thus, we have to establish rules and procedures that will protect classified material when it is being dispatched from one place to another. DCS and USPS provide the means and numerous directives describe the rules and procedures. When receiving or sending classified information or material from one point to another, you must follow these basic guidelines:

- Top Secret information and material are moved by escort, courier, or transmitted over electronic means (encrypted or cryptographic) that are protected from exploitation by enemy forces. Top Secret information is transported under a chain of receipts covering each individual who gets custody.
- Secret information and material are moved by registered US mail or the methods used for Top Secret materials.
- Confidential information and material are sent by the same means for sending Secret and Top Secret materials, except between DoD component locations anywhere in the US or its territories. In such cases, certified or first-class mail will be used and the outer envelope will be marked "POSTMASTER: Do Not Forward."

AF Form 310

A receipt between the originator and the intended recipient is used for Secret information. Do not issue receipts for Confidential material unless prescribed by a special access program directive issued by HQ USAF or higher authority. The AF Form 310, *Document Receipt and Destruction Certificate*, is adequate to satisfy most Secret receipt requirements (figure 5-2 illustrates this form). The following is a list of steps when shipping Secret material using AF Form 310:

1. Prepare three copies.
2. Place one copy in a suspense file at the originating location.
3. Two copies are sent in the container along with the material shipped.
4. Upon receipt, the gaining unit signs one copy and returns it to the originating location.
5. Upon receiving the signed receipt, the originating location may destroy the suspense copy, and the signed copy is placed on file for at least two years.
6. Initiate tracer action for receipts that are not returned within 30 days for shipments within the Continental United States, and 45 days for shipments to overseas locations.

DOCUMENT RECEIPT AND DESTRUCTION CERTIFICATE			
1. TO: 30 AINS/DOT 89 OAK RD LANGLEY AFB VA 23665		2. FROM: 315 TRS/DOED 154 Canberra Street Goodfellow AFB TX 76908-4002	
		3. DATE 11 Jan 9__	
		4. CONTAINER NO. DOE-96-011	
5. DESCRIPTION OF DOCUMENT(S): (Indicate overall classification, originator, type (letter, message, plan, etc.), date, unclassified subject title, number of copies, and originator control number and copy number if Top Secret. Also use these data elements for identifying any attachments that would require a receipt if transmitted separately) S/NF, 315 TRS/DOE, BOOKLET, 20 Dec 95, Imagery Manual 001-01, 5 copies LAST ITEM _____			
TO AVOID TRACER ACTION, RETURN SIGNED RECEIPT BY _____ →			6. DATE 11 Feb 9__
DOCUMENT RECEIPT			
I ACKNOWLEDGE RECEIPT OF THE ABOVE DOCUMENTS			
7. DATE RECEIVED 10 Feb 96	8. NAME AND ORGANIZATION MSgt Smith, 30AINS/DOT	9. SIGNATURE OF RECIPIENT <i>[Signature]</i>	
DESTRUCTION CERTIFICATE			
10. THE DOCUMENT(S) LISTED ABOVE WERE <input checked="" type="checkbox"/> DESTROYED <input type="checkbox"/> COMMITTED TO CENTRAL DESTRUCTION FACILITY ON _____ →			11. DATE 20 Mar 9__
12. TYPED OR PRINTED NAME AND SIGNATURE OF WITNESSING OFFICIAL <i>Steve Johnson</i> STEVE JOHNSON, MSgt, USAF		13. TYPED OR PRINTED NAME AND SIGNATURE OF WITNESSING OFFICIAL	

AF FORM 310
NOV 81

PREVIOUS EDITION WILL BE USED

Figure 5-2. Document Receipt and Destruction Certificate.

Packaging classified material

In your job, if you are required to ship classified information to various locations, use the following rules when preparing shipments:

1. Material must be double-wrapped in opaque envelopes or containers.
2. Material used for packaging must be strong and durable enough to provide security while in transit to prevent items from breaking out of the container, and to aid in the detection of any tampering with the container.
3. The inside container will show the address of the receiving activity, conspicuous classification and associated markings.
4. The outside container will conceal all classified characteristics and markings.
5. Address the outside envelope or container to an official government activity.

Hand-carrying classified material

All Air Force personnel escorting or hand carrying classified outside their normal work area require authorization for such action. A verbal approval from your supervisor is sufficient when hand-carrying classified between buildings or areas controlled by your commander or agency chief. If you are escorting or hand-carrying the classified between buildings or areas that are not under the control of your commander or agency chief, you must have written authorization. This written authorization may be in the form of an official letter or wallet-sized card signed by your commander or staff agency chief.

The authorization must contain your full name, the purpose of hand-carrying or escorting the classified material, a telephone number at the issuing activity for verification purposes, and other information that will assist your movement through inspection points such as base gates and other facilities. If your travel does not pass through any inspection points, a verbal approval from your supervisor is adequate.

While hand carrying this material, you must use an envelope, folder, briefcase, or other closed container to prevent loss or observation of the classified material. When the material is carried in private, public, or government conveyance, it must not be placed in any detachable compartment such as a luggage rack or automobile trailer.

If you are tasked to hand-carry or escort classified for any other travel, such as from one base to another, an approved courier letter must be carried. An exemption from inspection notice must be placed on the classified package. Normally, the authorization to hand-carry classified will also be annotated on your travel orders.

In-transit storage

If you are a courier, you may have to store classified material overnight at a base. Storing classified material in your room or hotel safe is *not* authorized and constitutes a security violation. The following are two places you can normally find secure storage:

1. Air Mobility Command (AMC) airfreight terminals.
2. A repository designated by the installation commander. Base operations dispatch personnel, passenger service personnel, and installation entry controllers (gate guards) know the location of the overnight repository.

030. Accounting for classified material

Accountability is maintained for classified information as a means of protecting it from unauthorized disclosure. Maintaining accountability is simply keeping an accurate record of how much classified information you have, where it is, and, in the case of TOP SECRET information, who has seen it.

Even though active accountability records are not required for Secret and Confidential material in most cases, there is a chance you will be responsible for the accountability of this information. Consequently, you should familiarize yourself with the accountability procedures of the various classification levels in your area. Let's look at some specific accountability requirements for each level of classified information.

Top Secret

The security of Top Secret material is paramount and requires strict, mandatory compliance with the Top Secret Control procedures listed below:

1. *Top Secret Control Officer (TSCO)* - The commander of each unit that routinely originates, stores, receives, or dispatches Top Secret information will establish a Top Secret control account (TSCA) headed by a TSCO. The TSCO's duties encompass all matters affecting accountability and control of Top Secret information.
2. *Top Secret Register* - The TSCO maintains a Top Secret register (a complete file of AF Forms 143, *Top Secret Register Pages*). These registers identify the Top Secret document or material to include the title, date of the document, identity of the originator, date the document or material was received, number of copies received or later reproduced, and the disposition of the Top Secret material and all its copies.
3. *Originator Control Number* - The originator of Top Secret information assigns an originator control number to the face of the document. This number consists of the calendar year, originator functional address symbol, and the next consecutive number of the Top Secret documents produced by the originator that calendar year; e.g., 96DOE01.
4. *Disclosure Records* - The TSCO attaches an AF Form 144, Top Secret Access Record and Cover Sheet, to each Top Secret document, which identifies all people given access to the information and the date of the disclosure.
5. *Inventories* - All Top Secret documents and material will be inventoried at least annually or change of the unit TSCO, depending on whichever occurs first. These inventories are done to audit inactive register page entries for proper disposition and to physically check active documents or material.

COMINT restrictions

The dissemination of COMINT is more severely limited than other defense information because of its extreme sensitivity. Only certain authorized communications channels are used to disseminate this information, and the recipient must have COMINT indoctrination and the proper security clearance. Personal recognition is the most desirable way to determine if a person is authorized access to a sensitive, controlled area. Since personal recognition of every individual authorized access to COMINT is impossible, a badge system is used. This identifies personnel who have access to COMINT information or who need to enter a controlled area to perform their duties.

Secret

The control system for Secret material is based on the concept that Secret material originated in or received by the Air Force remains in the Air Force, or a record of its disposition is kept. Receipt records are normally kept using an AF Form 310. AF Form 310's are placed in a file for at least two years. Active accountability records for individual Secret documents are not kept unless prescribed in a special access program directive issued by Headquarters USAF or higher authority.

Confidential

Active accountability records for individual Confidential documents are not kept unless prescribed in a special access program directive issued by Headquarters USAF or higher authority.

Maintenance

Restrict equipment maintenance to authorized and identified vendor maintenance personnel. Ensure that maintenance personnel who must enter areas where classified information is processed have the proper security clearance or are constantly escorted. Do not give classified media, products, etc. to vendor maintenance personnel for testing or use. Also limit operator and user maintenance to normal cleaning and housekeeping activities to protect Air Force rights under warranties.

Summary

As you can see, there are very specific requirements when it comes to properly marking classified information, and most units develop a local guide to assist you in this area. We also discussed the receipt and transfer of classified information, and accounting for what your unit maintains, to include the more stringent controls placed on COMINT materials. In the next several units, we'll look at how classified information is safeguarded, what is required when it is destroyed, and what is involved when classified information is released.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

029. Documenting the receipt and transfer of classified material

1. How may Top Secret material be dispatched?
2. How may Secret material be dispatched?
3. What form is prepared when shipping Secret material?
4. When must a tracer action be initiated for a Secret shipment to an overseas location?
5. What information is placed on the inner wrapping of a Secret package or container?
6. What is required to hand-carry classified material between buildings controlled by your commander or agency chief on your base?
7. What two items are required to hand-carry classified material from one base to another?
8. What two locations may you use to store classified material overnight while in-transit?

030. Accounting for classified material

1. Who at each unit is responsible for the accountability and control of Top Secret information?
2. What form is used to identify Top Secret documents and material?
3. What form is attached to each Top Secret document to identify all people given access to the information?
4. How often is Top Secret material inventoried?
5. Why is dissemination of COMINT severely limited?
6. How long are AF Form 310s maintained?

031. Safeguarding classified material

Safeguarding classified material pertains mostly to the physical measures taken to ensure that the information is protected. One of the best preventions is to destroy outdated and otherwise unneeded classified material. The destruction of unnecessary documents is one of the most neglected principles in safeguarding classified material.

Safeguarding

To perform your duties, you will be handling classified information; therefore, you will be a custodian of classified material. As such, you will be responsible for providing protection and accountability for this information at all times. You must ensure unauthorized people do not gain access to classified information under your control. No one has a right to classified information based only on one's rank, position, or clearance status. Before disclosing classified information, the official who has custody of the classified information must determine if a person's assigned duties require access to classified information and whether the person has a clearance equal to or higher than the material being disclosed. Classified documents removed from storage will be kept under constant surveillance, face down, or covered when not in use. If you plan to remove classified from your designated work area during non-duty hours, you must receive authorization from your commander or designated authority. All rooms, areas, copier machines, computers, and other equipment where classified information is stored, handled, or processed will be included in an end-of-day security check. When performing your end-of-day security checks, ensure the following steps are taken:

1. All classified material is properly stored.
2. Burn bags are properly stored or emptied.
3. Wastebaskets do not contain classified material.
4. Standard Form 702, *Security Container Check Sheet* or other designated forms are used on each secure container to show that it has been properly locked and checked.
5. Record the inspection results of your area on an SF 701, *Activity Security Checklist*.

Storage

Classified material must be in use by or under the direct control of an authorized person who is in the same room as the material. Otherwise, the classified material must be stored in a locked container. AFI 31-401 provides basic guidance on the type of containers to be used for storage. AFMAN 14-304 should be consulted for special storage requirements for SCI material. The following are the basic guidelines for use of safes and storage containers:

- Store Top Secret material in a safe or steel file container having a built-in, three-position, dial-type, changeable combination lock approved by the General Services Administration (GSA). It may also be stored in a class-A vault or vault-type room that meets the standards established by the head of the DoD component concerned or the local commander.
- When Top Secret material is located in buildings, structural enclosures, or other areas not under US Government control, the storage container, vault, or vault-type room must be protected by an alarm system or guarded during non-operating hours.
- Secret and Confidential material can be stored in any manner authorized for Top Secret or in a class-B vault or vault-type room which meets the standards established by the head of the DoD component or local commander.
- Until they are phased out, steel filing cabinets having a built-in, three-position, dial-type combination lock can be used. As a last resort, an existing steel filing cabinet equipped with a steel lock-bar, provided a GSA-approved changeable combination padlock secures it can be used.
- There shall be no external marking on a safe or container that describes the level of classified material within. Do not store money, weapons, controlled drugs, precious metals, or any other items susceptible to theft in the same safe or container used for storing classified material. Figure 5-3 shows examples of authorized storage containers.

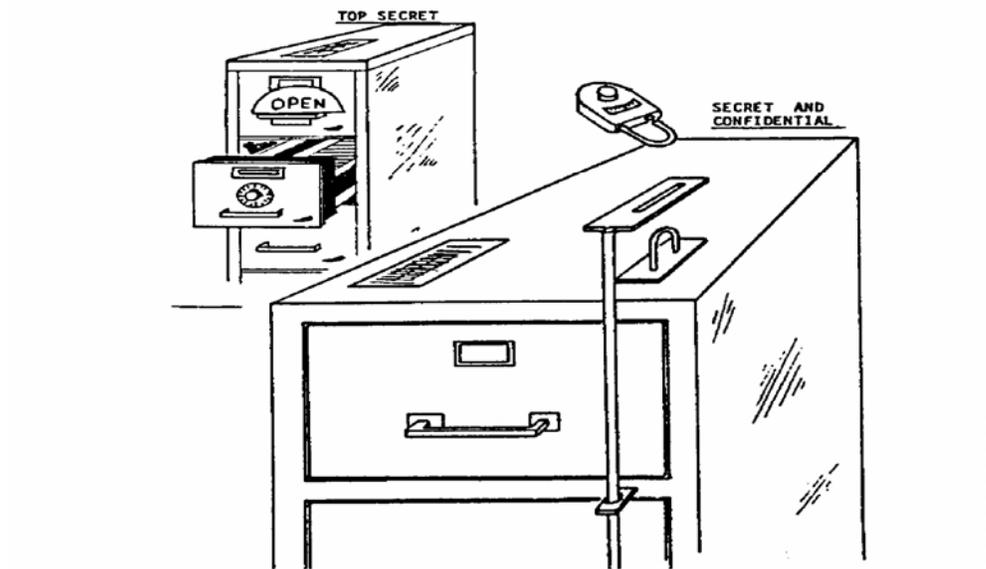


Figure 5-3. Authorized Storage Containers.

Combinations

A safe or padlock combination has a security classification equal to the highest level of material stored within the safe or container. Only persons authorized access to the material stored within a safe or container should be given the combination. The combination must be changed when any of the following conditions exist:

1. When it is first brought into the work-center.
2. After 12 months since the last combination change.
3. When someone with access to the combination no longer requires access to the material.
4. When an unauthorized person has been given the combination.
5. When material normally stored within the safe or container cannot be accounted for.
6. When a safe or container is taken out of service. (Built-in combinations will be reset to 50–25–50 and padlocks will be reset to 10–20–30.)

Sensitive Compartmented Information Facility (SCIF)

A SCIF is a formally accredited area, room, group of rooms, or installation where SCI material may be stored, used, discussed, or electronically processed. A SCIF may be permanent or temporary, mobile or fixed, and vary in construction. Procedures must be established to prevent the free access of persons unless they have been formally indoctrinated for that particular SCI material. SCIFs can be located at government-controlled facilities, contractor plants, or civilian locations. There are two types of SCIFs and they are defined as follows:

- *Open Storage* – This permits the storage of SCI material on shelves or in metal containers (locked or unlocked) within a SCIF, while authorized personnel do not occupy the SCIF. The containers do not have to be GSA-approved containers.
- *Closed Storage* – This allows the storage of SCI in properly secured GSA-approved security containers within a SCIF when authorized personnel do not occupy the SCIF.

The SCIF may be sub-divided into a number of areas. Samples of these areas are as follows:

- *Secure working area* – An area used daily for handling, processing, or discussing SCI material. No SCI material may be stored in this type of secure working area.
- *Secure vault area* - An area under the control of a designated custodian and used to store (open storage) and protect SCI material.
- *Temporary secure working area* – An area, room, or group of rooms (i.e., a briefing or conference room or a processing area) that has been secured against physical and audio penetration for the temporary use of SCI material. A temporary working area will not be used to store SCI material and will not be used in excess of 40 hours per month.
- *Continuous operations area* – An area such as an operations building. Two or more SCI indoctrinated people who can maintain continuous entry control of the facility occupy the area. This area is open and provides protection for SCI material 24 hours a day, 7 days a week.
- *Secure area* – An area in which SCI material can be stored in approved security containers and openly discussed and used.
- *Temporary secure area* – A temporarily accredited facility used for storing, handling, discussing, and processing SCI material. It can be established for a period of 6 months or less and is only approved by HQ AF/INSC.
- *Non-discussion area* – A clearly defined area within a SCIF where classified discussions are not authorized.

Storing and accounting for SCI material

The basic requirement for SCI security is that at all times SCI is in the direct custody or control of SCI indoctrinated persons who are physically capable of providing the required protection. Otherwise, the SCI material must be properly stored in a SCIF. Storage containers within a SCIF are designated, numbered, and inspected. SCI material entering a SCIF is logged, but no further documentation is required unless the material leaves the SCIF.

Storing removable media

Store all removable media (i.e., floppies, hard disk packs, ribbons, etc.) in the appropriate container according to the classification of the material.

032. Destroying classified material

Destruction

There is no reason to retain classified material if it is no longer needed to perform your mission. The proper destruction of classified information completes the life cycle of that information, while continuing security practices that prevent the unauthorized disclosure of the information. Your duties will always include the destruction of classified material or the witnessing of this destruction. The following are some specific requirements that apply to the destruction of classified material:

Basic requirements

Regardless of the classification of the material to be destroyed, the following rules apply:

1. Supervise the destruction.
2. Safeguard the material until it is actually destroyed.
3. Destroy the material completely so that its classified content cannot be restored or revealed through any visual, physical, technical, or chemical process.

Authorized methods of destruction

When possible, destroy classified material by burning. Other destruction methods include melting, chemical decomposition, pulverizing, pulping, shredding, or mutilation sufficient to preclude recognition or reconstruction of the classified information. In each case, completely destroy the material and ensure that the residue of the destruction process is unreadable and cannot be reconstructed in any form.

Records of destruction

Normally, AF Form 145, *Certificate of Destruction*, AF Form 310, *Document Receipt and Destruction Certificate*, and AF Form 1565, *Entry Receipt and Destruction Certificate* are used to record and certify the destruction of classified material. Destruction records are required for Top Secret and Secret information and are maintained for a minimum of 2 years. The record must be dated and signed at the time of destruction. Two witnesses are required for Top Secret information and one for Secret. In the case of information placed in burn bags for central disposal, the witnessing official or officials need only sign the destruction record when the burn bags are delivered. Destruction records are not required for classified waste such as typewriter ribbons or working papers.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

031. Safeguarding classified material

1. What form is used to record the end-of-day inspection?

2. What safeguards must be in place when Top Secret material is located in a building that is not under US Government control?
3. What may not be stored in a safe or container that is also used to store classified material?
4. What is the classification of a safe or container combination when used to store classified material?
5. List three conditions that would require a safe or container combination to be changed?
6. What is a SCIF used for?
7. What type of SCIF requires SCI material to be stored in GSA-approved security containers when unoccupied?
8. What are the limitations on the use of a SCIF temporary secure working area?
9. Where should you store removable media?

032. Destroying classified material

1. What are the three basic requirements for destroying classified material?
2. What are the authorized destruction methods?
3. What three forms may be used to record and certify the destruction of classified material?

033. Releasing and disclosing classified information

Part of your responsibility for safeguarding classified material is preventing the release or disclosure of this information to anyone who does not have the need for that information. You can properly identify, properly mark, and properly store classified material, but if you give it to someone without the need for the information, you've erased all of your hard work.

Access to classified

As part of your everyday duties in intelligence you will possess and control classified information. Therefore, you are personally, morally, and legally responsible for the protection of that information. Every effort must be made to ensure that only authorized persons gain access. There are three general criteria that must be met before you can allow a person access to classified information:

Security clearance

First, the person must possess a security clearance equal to or greater than the classification level of the information being disclosed. There are several ways to determine this. Probably the best method is an automated listing. The system that should be available to you is the secure, web-based Joint Personnel Adjudication System (JPAS), which is new as of June 2003. Previous systems included the Automated Security Clearance Approval System (ASCAS) roster, and Sentinel Key. The thing you need to remember is that your unit has some form of an automated listing with which you can verify an individual's security clearance. Methods other than an automated listing include confirmation (written or verbal) from the requestor's security manager, supervisor, or commander, TDY orders, or your personal knowledge of that person's security clearance. The possession of a security clearance alone does not entitle a person access to classified information.

Need to know

Secondly, the person considered for access must also have a valid need-to-know. This means you must determine that the person has an essential need for access to the classified material for the accomplishment of their official duties. You can establish a person's need-to-know based upon your personal knowledge of the requestor or confirmation (written or verbal) from the person's security manager, supervisor, or commander. In some special access programs, a predetermined need-to-know access list is published according to procedures for the specific program. The need-to-know rule also includes limiting the disclosure to only the specific classified information needed. For example, do not disclose a complete classified Operations Plan when a recipient only needs access to an unclassified portion of it. If there are any doubts about a specific person's need-to-know, you should immediately consult your security manager, supervisor, or commander.

Nondisclosure agreement

The third criteria to be considered is that a person must have executed a Standard Form 189, *Classified Information Nondisclosure Agreement*. This can be verified from JPAS, written or verbal confirmation from the person's security manager, supervisor, or commander, or by your personal knowledge that the requestor has signed the agreement.

Refusal

You should be extremely tactful about refusing to release a classified document to someone, but a simple explanation usually suffices. Most people will understand that you are only conscientiously performing your duty. Do not give-in to pressure by higher-ranking individuals. Get your chain of command involved immediately.

Access by Visitors

Except when a continuing, frequent, working relationship is established through which current security clearance and need-to-know are determined, DoD personnel visiting other DoD activities, its contractors, or other agencies must provide advance notification of the pending visit. Visit requests should include the following essential information:

1. Full name.
2. Rank.
3. Social Security Number.

4. Security clearance of the visitor.
5. Visitor's unit of assignment.
6. Unit to be visited.
7. Date and duration of proposed visit.
8. Purpose of visit sufficient to establish need-to-know.
9. Names of persons to be contacted.

Your unit's security manager usually handles visitor access and the transferring of security clearances (your Special Security Office, or SSO, normally processes the transfer of clearances at the SCI level). It is extremely important that you understand this process in order to reduce the chance of compromise.

Summary

Information Security is probably one of the most important programs within the intelligence field. If we do not protect classified information, we place our country's security in jeopardy. You have been placed in a position of great trust, and it is absolutely vital that you do everything within your means to follow the directives and guidance for the protection of classified information.

034. Handling NATO classified

During your career in intelligence, it is highly likely that you will find yourself assigned to a unit with the North Atlantic Treaty Organization (NATO). Much of the information that you'll handle will be classified, and the security procedures closely resemble those for US classified materials. However, there are differences that you must be aware of. In this lesson, we'll briefly cover NATO's background; the types and control of NATO classified material. For further information, refer to AFI 31-406, *Applying North Atlantic Treaty Organization (NATO) Protection Standards*.

Background

The North Atlantic Treaty was signed in Washington, D.C. on 4 April 1949, initially creating an alliance of 12 independent nations committed to each other's defense. Since that time, the number of NATO members has grown to 19, and by 2004, it is expected to number 26 nations.

The Secretary of Defense is the US National Security Authority for NATO, and is responsible for ensuring that NATO security requirements are implemented throughout the Executive Branch of the US Government.

The "NATO" marking means the information is the property of NATO requiring the NATO originator's consent for dissemination outside of NATO and is subject to the security protection mandated by AFI 31-406.

Types of NATO classified

- *ATOMAL* – Refers to atomic information provided by the governments of the United States or the United Kingdom to NATO under the *Agreement Between the Parties to the North Atlantic Treaty Organization for Co-Operation Regarding Atomic Information*.
- *COSMIC Top Secret (CTS)* – COSMIC is a NATO marking and designation that is synonymous with Top Secret and is applied exclusively to all copies of Top Secret documents prepared for circulation within NATO, however, the term "NATO TOP SECRET" is not used. CTS will be applied only to information that the unauthorized disclosure of which would result in *exceptionally grave damage* to NATO.
- *NATO SECRET (NS)* – NS is applied only to information the unauthorized disclosure of which would result in *serious damage* to NATO.
- *NATO CONFIDENTIAL (NC)* – NC is applied only to information the unauthorized disclosure of which would result in *damage* to NATO.

- *NATO RESTRICTED (NR)* – The United States does not have a security classification equivalent to NATO RESTRICTED. NATO information classified as restricted is safeguarded in a manner that prevents disclosure to non-Governmental personnel. This is similar to our “FOR OFFICIAL USE ONLY” information marking; however, **NATO RESTRICTED is a security classification**. An unauthorized disclosure of this type of information would be *disadvantageous* to the interests of NATO.
- *NATO UNCLASSIFIED (NU)* – NATO unclassified information cannot be released to non-NATO nations, organizations, or individuals without the prior approval of NATO.

Control of NATO classified

Each NATO member nation establishes a central registry, the purpose of which is to ensure proper control and accountability of NATO classified information. The Central US Registry (CUSR), located in the Pentagon, oversees the administration of the US registry system. The CUSR establishes sub-registries to execute the accountability and security management of NATO and ATOMAL material in many locations throughout the world, and control points may also be established to assist in these operations. Within the US Air Force, USAFE is the lead office for the NATO Safeguarding Program.

The marking, safeguarding, storage, and dissemination procedures for NATO classified materials is much the same as US classified materials, and AFI 31-406 provides in-depth coverage of these requirements.

Summary

Classified materials generated from within the NATO infrastructure must be afforded protection, just as we protect our own US-only classified materials. What makes NATO classified unique is the fact that an unauthorized disclosure might prove militarily disastrous, but also has the potential of damaging alliances between member nations. As such, it is imperative that you follow proper security procedures in order to protect NATO classified materials.

Self-Test Questions

After you complete these questions, you may check your answers at the end of the unit.

033. Releasing and disclosing classified information

1. What is the best method to determine if an individual is cleared for classified information before you release it?
2. What is meant by “need-to-know”?
3. What is an SF 189 used for?

034. Handling NATO classified

1. Who is the US National Security Authority for NATO?

2. What NATO classification is given to atomic information provided by the governments of the United States or the United Kingdom to NATO?
3. What NATO classification is synonymous with the US "For Official Use Only" marking?
4. What is the purpose of a central registry?
5. What USAF MAJCOM is the lead office for the NATO Safeguarding Program?

(b)(2) High [redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

(b)(2) High

[Redacted text block]

[Redacted text block]

- [Redacted list item]

[Redacted text block]

[Redacted text block]

[Redacted text block]

(b)(2) High

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

(b)(2) High

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

- [Redacted]
- [Redacted]
- [Redacted]

[Redacted]

[Redacted]

(b)(2) High

[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]

[Redacted text block]

[Redacted text block]

[Redacted text block]

- [Redacted list item]
- [Redacted list item]
- [Redacted list item]
- [Redacted list item]

[Redacted text block]

[Redacted text block]

(b)(2) High

[Redacted text block]

(b)(2) High

[Redacted text block]

(b)(2) High [Redacted]
[Redacted]
[Redacted]

[Redacted]
[Redacted]

[Redacted]
[Redacted]

[Redacted]
[Redacted]

[Redacted]
[Redacted]

[Redacted]
[Redacted]

[Redacted]
[Redacted]

[Redacted]
[Redacted]

Answers to Self-Test Questions

024

1. DoD 5200.1R and AFI 31-401.
2. To protect national security.
3. Top Secret.
4. Top Secret
5. Serious.
6. Damage.

7. A Single Scope Background Investigation (SSBI).

025

1. A classification guide is written guidance of classification and declassification decisions.
2. New material that derives its classification from information already classified.
3. The originator of the classified information.
4. Either 10 years from the date of the original decision, or if deemed necessary, the document should be marked with one of the eight X-series declassification codes.
5. Safeguard it at the higher level pending determination by a classification authority.
6. OPSEC.
7. Changes to unit mission, changes to organization, introduction of new equipment, security clearances of individuals, equipment shortages effecting readiness or efficiency, equipment or system performance, mapping requirements that indicate operational intent, the classification of operations or programs.
8. Security access rosters, personal Air Force records, unclassified portions of CDCs, unclassified inspector general reports.
9. The loss of sensitivity of the information.
10. X3
11. X8

026

1. A special handling instruction or control marking used to identify additional warnings to restrict the distribution.
2. NOFORN.
3. REL to: CAN.
4. SPECAT.

027

1. Confidential.
2. Apply the equivalent US classification conspicuously on the document.
3. When your intelligence product information incorporates foreign government documents.

028

1. Centered at the top and bottom of the front and back covers, title page, and first page, if there are any.
2. Center top and bottom with the highest classification based on the contents of that page. Interior pages may be marked with the overall classification of the document when such marking is necessary to achieve production efficiency. The information is otherwise sufficiently identified by paragraph classification markings.
3. Immediately before the paragraph.
4. Date of creation and highest classification contained.
5. At the top and bottom, front and back.
6. Secret.
7. SF 710.

029

1. By escort, courier, or transmitted over electrical means.
2. By using registered US mail or any means approved for Top Secret.
3. AF Form 310, Document Receipt and Destruction Certificate.
4. When receipts are not returned after 45 days.
5. The receiving address and conspicuous classification and associated markings.
6. A verbal approval from your supervisor.
7. An approved courier letter and an exemption from inspection letter.

8. Air Mobility Command (AMC) airfreight terminals and a repository designated by the installation commander. Base operations dispatch personnel, passenger service personnel, and installation entry controllers (gate guards) know the location of the overnight repository.

030

1. The Top Secret control Officer (TSCO).
2. AF Form 143, Top Secret register.
3. AF Form 144, Top Secret Access Record.
4. At least annually or change of the unit TSCO.
5. Because of its extreme sensitivity.
6. For at least two years.

031

1. SF 701
2. They must be protected by an alarm system or guarded during non-operating hours.
3. Money, weapons, controlled drugs, precious metals, or any other item susceptible to theft.
4. Equal to the highest level of material stored within the safe or container.
5. When it is first brought into the work-center, after 12 months since the last combination change, when someone with access to the combination no longer requires access to the material, when an unauthorized person has been given the combination, when material normally stored within the safe or container cannot be accounted for, and when a safe or container is taken out of service. Built-in combinations will be reset to 50-25-50 and padlocks will be reset to 10-20-30.
6. To store, use, discuss, or electronically process SCI material.
7. Closed storage.
8. It cannot be used in excess of 40 hours per month.
9. In an appropriate container according to its classification.

032

1. Supervise the destruction, safeguard the material until it is actually destroyed, and destroy the material completely so that its classified content cannot be restored or revealed through any visual, physical, technical, or chemical process.
2. Burning, melting, chemical decomposition, pulverizing, pulping, shredding, or mutilation sufficient to preclude recognition or reconstruction of classified information.
3. AFFM 145, Certificate of Destruction, AFFM 310, Document Receipt and Destruction Certificate and AFFM 1565, Entry Receipt and Destruction Certificate.

033

1. By using the secure, web-based Joint Personnel Adjudication System (JPAS).
2. Access to the classified information is needed for the accomplishment of their official duty.
3. To verify that an individual has agreed not to disclose classified information.

034

1. Secretary of Defense.
2. ATOMAL.
3. NATO RESTRICTED (NR).
4. To ensure proper control and accountability of NATO classified information.
5. USAFE.

035

1. This information can provide our adversaries with intelligence indicators about our daily operations, capabilities, intentions, future plans, and activities.

2. Identifying indicators that are tip-offs to impending activities.
3. All DoD members.

036

1. US Government telecommunications.
2. The preparation, transmission, or processing of information by electrical means.
3. Physical security, cryptosecurity, emission security, transmission security.
4.
 - (1) e.
 - (2) d.
 - (3) c.
 - (4) a.
5. Physical security.
6. The information being transmitted, received, handled, or otherwise processed by classified processing equipment.
7. Telephone.
8.
 - (1) Registered mail and secure communications for classified or sensitive unclassified information.
 - (2) Use cryptographically secure STU-III or EMSEC facsimile (FAX).
 - (3) Never attempt to “talk around” classified subjects or use homemade codes to pass classified information by unsecured communications.

037

1. To integrate information systems security policy and practices into the Air Force culture and minimize the possibility of system compromise.
2. AFI 33-204.
3. Follow established equipment protection policies.
4. Illegally copying government-owned software.

Student Notes

Volume Review Exercises

Note to Student: Consider all choices carefully, select the *best* answer to each question, and *circle* the corresponding letter. When you have completed all unit review exercises, transfer your answers to ECI (AFIADL) Form 34, Field Scoring Answer Sheet.

Do not return your answer sheet to AFIADL.

1. (001) According to AFMAN 36-2108, which of the following is not a responsibility of the 1N0X1 AFSC?
 - a. Develops mission planning and execution support materials.
 - b. Debriefs enemy personnel captured by US and allied forces.
 - c. Performs geo-locational mensuration functions.
 - d. Prepares and presents intelligence briefings.

2. (002) At what point in your intelligence career are you enrolled in the 1N051 CDCs?
 - a. Operations Intelligence Specialist.
 - b. Operations Intelligence Craftsman.
 - c. Operations Intelligence Apprentice.
 - d. Operations Intelligence Journeyman.

3. (002) How long must you spend in upgrade training status before being awarded your 7-skill level in the 1N0X1 career field?
 - a. 6 months.
 - b. 12 months.
 - c. 15 months.
 - d. 18 months.

4. (003) Which of the following is a duty you are more likely to perform as a Senior or Chief Master Sergeant in the 1N0X1 AFSC?
 - a. Intelligence analyst.
 - b. Airman assignments.
 - c. Intelligence systems support.
 - d. Aircrew briefing and debriefing.

5. (004) Which intelligence AFSC performs duties as a sensor operator for UAVs?
 - a. 1N0X1.
 - b. 1N1X1.
 - c. 1N4X1.
 - d. 1N5X1.

6. (004) Which intelligence AFSC is responsible for collecting, analyzing, processing, and deriving intelligence information from non-communications electromagnetic transmissions?
- a. 1N1X1.
 - b. 1N2X1.
 - c. 1N5X1.
 - d. 1N6X1.
7. (005) At the tactical level in dedicated intelligence centers afloat, where is naval intelligence conducted?
- a. CIC.
 - b. CVIC.
 - c. FMFPAC.
 - d. NAVCENT.
8. (005) Which US Navy intelligence specialty performs duties that most closely resemble those performed by the 1NOX1 AFSC?
- a. IS-3905.
 - b. IS-3910.
 - c. IS-3912.
 - d. IS-3924.
9. (005) Which US Navy intelligence specialty provides target intelligence support to tactical mission planners, and maintains tactical level targeting folders?
- a. IS-3905.
 - b. IS-3912.
 - c. IS-3923.
 - d. IS-3925.
10. (005) Which US Navy intelligence specialty produces imagery-based products for use by the TLAM Afloat Planning System?
- a. IS-3910.
 - b. IS-3923.
 - c. IS-3925.
 - d. IS-3926.
11. (005) What is the designation assigned to the Marine Corps component intelligence staff officer at the regiment/battalion level?
- a. I-2.
 - b. J-2.
 - c. S-2.
 - d. G-2.

-
-
12. (005) Which Marine Corps intelligence specialty performs duties that correlate closely to the 1N0X1 AFSC?
- MOS 0231.
 - MOS 0241.
 - MOS 0251.
 - MOS 0261.
13. (005) Which Marine Corps intelligence specialty conducts geospatial, geodetic, hydrographic, and satellite analysis and surveys?
- MOS 0231.
 - MOS 0241.
 - MOS 0251.
 - MOS 0261.
14. (005) Which US Army intelligence MOS is considered the “quarterback” of all Army enlisted intelligence specialties?
- MOS 96B.
 - MOS 96D.
 - MOS 98B.
 - MOS 98D.
15. (005) Which US Army intelligence MOS fuses intelligence information collected by the 98G, and disseminates it to higher headquarters?
- MOS 96B.
 - MOS 98B.
 - MOS 96C.
 - MOS 98C.
16. (006) What Executive Order outlines the goals of the US intelligence effort and the structure of the US Intelligence Community?
- EO 12332.
 - EO 12333.
 - EO 12334.
 - EO 12863.
17. (007) The President is at the top of the US intelligence pyramid, and is responsible for directing all national intelligence activities through which agency?
- DCI.
 - IOB.
 - NSC.
 - SecDef.
18. (007) What national level organization is responsible for approving all National Intelligence Estimates?
- National Intelligence Council.

- b. Community Management Staff.
- c. National Foreign Intelligence Board.
- d. Intelligence Community Principal's Committee.

19. (007) What national level organization is responsible to the President through the DCI, and accountable to the American people through the intelligence oversight committees of the US Congress?

- a. CIA.
- b. NIC.
- c. CMS.
- d. NFIB.

20. (007) What CIA directorate produces quick-reaction papers, and supports diplomatic negotiations and military operations?

- a. Operations.
- b. Intelligence.
- c. Science and Technology.
- d. Intelligence and Research.

21. (008) Within the Executive Branch, what organization is considered the lead US foreign affairs agency?

- a. Department of State.
- b. Department of Justice.
- c. Office of the Attorney General.
- d. Office of Intelligence Liaison and Policy.

22. (008) What organization serves as the US Government's focal point for threat assessment, warning, investigation, and response for threats or attacks against telecommunications, energy, banking and finance, water systems, government operations, and emergency services?

- a. OIS.
- b. EPIC.
- c. NIPC.
- d. NDPO.

23. (008) What directorate within the Department of Homeland Security maps the vulnerabilities of the nation's critical infrastructure against a comprehensive analysis of intelligence and public source information to protect the nation against terrorist attack?

- a. IAIP.
- b. ICPC.
- c. NIPC.
- d. DS&T.

-
-
24. (008) What Department of Homeland Defense entity makes full use of all terrorist threat-related information and expertise available to the US Government, and provides comprehensive all-source threat analysis to the President, the DHS, and to other Federal agencies?
- NIC.
 - EPIC.
 - NIPC.
 - TTIC.
25. (009) Which of the following is *not* a tenet of intelligence, according to Joint Publication 2-02, *National Intelligence Support to Joint Operations*?
- Usability.
 - Feasibility.
 - Relevance.
 - Completeness.
26. (009) What organization's primary functional national responsibility is to coordinate (not control) the intelligence activities performed by the military components?
- CIA.
 - DIA.
 - JCS.
 - NSC.
27. (009) What DOD-level organization serves as the OPR for airborne reconnaissance?
- DIA.
 - NRO.
 - NGA.
 - DARO.
28. (009) What MAJCOM is tasked specifically to provide homeland defense and civil support?
- USJFCOM.
 - USSTRATCOM.
 - USNORTHCOM.
 - USSOUTHCOM.
29. (009) What organization processes, analyzes, and consolidates data to produce fused intelligence information focused on USEUCOM's area of responsibility, and is the principal element for ensuring effective intelligence support for combatant commanders and theater forces?
- JAC.
 - ACE.
 - NATO.
 - USAFE.

30. (010) Who is responsible for ensuring timely intelligence is provided to DOD entities, including the Joint Staff, the services, combatant commands, other defense entities, and applicable agencies and departments outside the DOD?

- a. Director, National Security Agency.
- b. Director, Defense Intelligence Agency.
- c. Chairman of the Joint Chiefs of Staff.
- d. Joint Staff Directorate for Intelligence/J-2.

31. (011) In multinational operations, who retains overall command authority over US forces, but may place appropriate forces under the operational control of a foreign commander to achieve specific military objectives?

- a. President.
- b. Secretary of Defense.
- c. Joint Force Commander.
- d. Combined Force Commander.

32. (012) What unit manages ACC's overall intelligence combat readiness, unit advocacy, and is the focal point for targeting, geospatial issues and collection management?

- a. 70th Intelligence Wing.
- b. Air Intelligence Agency.
- c. ACC Intelligence Squadron.
- d. 609th Air Intelligence Squadron.

33. (012) What unit provides time-sensitive reporting of strategic indications of enemy bomber and naval deployments and movements that pose a potential threat to North America and the US?

- a. 1st AF, CONR.
- b. 8th AF, 608th AIS.
- c. 9th AF, 609th AIS.
- d. 12th AF, 612th AIS.

34. (012) What USAFE unit is the focal point for multi-source intelligence to support the execution of operational requirements during peace, contingencies, and war, and forms the core of the Combined/Joint Air Operations Center?

- a. 24th IS.
- b. 32nd AIS.
- c. UTASC.
- d. DCAOC.

35. (012) What PACAF unit forms the Commander, Pacific Air Forces, and USPACOM air component commander's combat intelligence staff?

- a. KCOIC.
- b. 607th AIS.
- c. 607th AIG.
- d. PACAF AIS.

-
-
36. (012) What AF MAJCOM provides threat assessments and defines the intelligence infrastructure support required by new weapons systems?
- ACC.
 - AFMC.
 - AFSPC.
 - AFSOC.
37. (013) What type of intelligence information deals with an enemy's combat plans, strength, and tactics, as applied to combat operations?
- Basic intelligence.
 - Critical intelligence.
 - Tactical intelligence.
 - Strategic intelligence.
38. (013) What source of intelligence is information comprised either individually or in combination with COMINT, FISINT, and ELINT?
- SIGINT.
 - MASINT.
 - RADINT.
 - TECHINT.
39. (013) What type of intelligence is derived from the collection and analysis of non-information bearing elements, extracted from the electromagnetic energy unintentionally emanated by foreign devices, equipment, and systems (excluding atomic and nuclear detonations)?
- ELINT.
 - FISINT.
 - RADINT.
 - TECHINT.
40. (013) What ELINT requirements include the data necessary to determine an emitter's function, capability, vulnerability, and technical characteristics?
- EOB requirements.
 - ELTEC requirements.
 - OPELINT requirements.
 - TELINT requirements.
41. (014) What intelligence requirement is developed to answer very specific questions, and normally involves time-dominant information and high perishability?
- Spot.
 - Crisis.
 - Standing.
 - Emergency.

42. (014) Responsibility for the overall efficient management and guidance of the intelligence cycle begins in which phase of the process?

- a. Direction.
- b. Collection.
- c. Processing.
- d. Production.

43. (015) What type of collection method is conducted openly and may be acknowledged by and attributed to its sponsor and participants?

- a. Overt.
- b. Covert.
- c. Discreet.
- d. Clandestine.

44. (015) What type of collection method is planned and executed to conceal the identity of the sponsor, and allows for plausible denial?

- a. Overt.
- b. Covert.
- c. Discreet.
- d. Clandestine.

45. (015) What arrangement allows for the efficient use of resources within the theater, and eliminates shortfalls, duplication of effort, and confusion during collection activities?

- a. Decentralized production.
- b. Combined production.
- c. All-source analysis.
- d. Critical analysis.

46. (016) Almost all intelligence information should be screened _____ for priority action?

- a. once.
- b. twice.
- c. at regular intervals.
- d. when the source is not in doubt.

47. (017) What intelligence reference document provides an up-to-date summary of essential information on military forces, with emphasis on *characteristics and performance* of major items of military equipment?

- a. Modernized Integrated Database.
- b. Tables of Organization and Equipment.
- c. Geographic Installation Intelligence Production Specifications.
- d. AFTTP 3-1, Vol. 2, Threat Reference Guide and Countertactics.

-
-
48. (017) What is the objective of interpretation?
- determine the truthfulness of collected information.
 - form a logical picture or hypothesis of enemy activities.
 - satisfy the EEI that originally set the intelligence process in motion.
 - coordinate with all concerned agencies for effective resource programming.
49. (018) What type of intelligence information reporting is in response to specific, validated requirements?
- Periodic.
 - Initiative.
 - Controlled.
 - Evaluation.
50. (018) The value of intelligence is based on its usefulness to the commander and staff, not it's _____?
- source.
 - quality.
 - quantity.
 - urgency.
51. (018) What method of intelligence report writing tells the commander what resources and capabilities are available to the enemy, and aids in planning?
- Intelligence digest.
 - Intelligence synopsis.
 - Intelligence summary.
 - Intelligence estimate of the situation.
52. (019) What is the principal benefit of the Shared Production Program?
- Validating all requirements through DIA.
 - Ensuring customer satisfaction with the program.
 - Using available intelligence resources effectively.
 - Placing all collection efforts under one organization.
53. (019) What is the assignment of production responsibilities under the SPP based on?
- national interests.
 - command policies.
 - mission requirements.
 - primary production center locations.
54. (019) Which of the following represents an example of federated production in ISR operations?
- Collection units are geographically separated from, and not subordinate to, the COMAFFOR.
 - Collection units are not geographically separated from, and not subordinate to, the COMAFFOR.
 - Collection units are geographically separated from, and subordinate to, the COMAFFOR.
 - Collection units are not geographically separated from, and subordinate to, the COMAFFOR.

55. (020) What AFI outlines the scope of the Air Force Intelligence Oversight Program?
- AFI 14-401.
 - AFI 10-104.
 - AFI 14-104.
 - AFI 10-401.
56. (020) Select the statement that *best* describes the purpose of the Intelligence Oversight program?
- Ensure intelligence related products are disseminated in accordance with AF instructions.
 - Enable intelligence personnel to perform their duties while preserving US citizen's rights.
 - Encourage compliance with intelligence collection procedures and established instructions.
 - Provide collection instructions for intelligence personnel performing counterdrug operations.
57. (020) What Executive Order established the Intelligence Oversight Board as a standing committee of the President's Foreign Intelligence Advisory Board?
- EO 12333.
 - EO 12863.
 - EO 12334.
 - EO 12864.
58. (020) In the context of your responsibilities concerning Intelligence Oversight, a unit authorized to collect, process, retain, or disseminate intelligence information for foreign intelligence, counterintelligence, terrorism, or narcotics activities, what are you involved with?
- processing site.
 - collection agency.
 - production facility.
 - intelligence activity.
59. (021) Which of the following is not included in typical MIDB products and outputs?
- Equipment list by force and primary function.
 - Facility and unit threat evaluation data and remarks.
 - Facility location list with vulnerabilities and remarks.
 - Equipment on-hand, quantities by facility and unit name.
60. (022) What intelligence architecture provides automated air campaign planning, execution monitoring, and intelligence capabilities for force-level air operations?
- PC-I3.
 - DCGS.
 - TBMCS-I3.
 - MIIDS/IDB.

61. (022) What TBMCS-I3 resident application provides a near-real time correlated view of land, sea, air, and Theater Missile Defense tracks?

- a. Intelligence Data Management (IDM).
- b. Situational Awareness/Assessment (SAA).
- c. Order of Battle Management/Threat Assessment (OBMTA).
- d. Collection Requirements/Monitoring Management (CRMM).

62. (022) What intelligence architecture is currently the Combat Air Force's primary unit-level intelligence system for automated receipt, correlation, and dissemination of intelligence in direct support of air operations?

- a. MIDB.
- b. IMOM.
- c. DCGS.
- d. TBMCS-UL.

63. (022) What ADOCS function provides a near real time depiction of the artillery battle?

- a. Counterfire Common Operational Picture (CF-COP).
- b. Fire Support Coordination Measures Analysis.
- c. Improved Many on Many.
- d. Joint Battlespace Display.

64. (022) Which of the following is *not* a key function within the ADOCS suite of applications?

- a. Battlespace Visualization.
- b. Improved Many on Many.
- c. Coalition Coordination and Integration.
- d. Air Interdiction Planning and Execution.

65. (022) What TBMCS-UL application allows users the ability to perform imagery exploitation, analysis, and change detection?

- a. ELT.
- b. IMOM.
- c. AFTRS.
- d. ADOCS.

66. (022) What application provides the capability to extract highly precise, mensurated coordinates for use by precision-guided munitions?

- a. IMOM.
- b. AFTRS.
- c. ADOCS.
- d. RAINDROP.

67. (022) What system provides near-real time global surveillance information from UHF satellite communications intelligence networks for sensor cueing?

- a. JDISS.
- b. DCGS.
- c. JWICS.
- d. AFTRS.

68. (023) What intelligence system is both an architectural framework and an integrated intelligence dissemination and collaboration service that provides uniform methods for exchanging information among intelligence providers and users?

- a. PC-I3.
- b. JWICS.
- c. INTELINK.
- d. TBMCS-UL.

69. (023) What intelligence system(s) comprise the joint standard and foundation for commonality among intelligence support systems?

- a. TBMCS-I3 only.
- b. JWICS and JDISS.
- c. JDISS and TBMCS-I3.
- d. JWICS and TBMCS-I3.

70. (023) When raw imagery intelligence data is converted into a more usable intelligence product, what form does the product *generally* take?

- a. Imagery Exploitation Report.
- b. Reconnaissance Exploitation Report.
- c. Imagery Interpretation Report.
- d. Reconnaissance Interpretation Report.

71. (023) What intelligence system serves as the authoritative source for targets for the entire imagery and geospatial community, and provides RMS exploitation feedback?

- a. NES.
- b. DCGS.
- c. MIDB.
- d. COLISEUM.

72. (023) What intelligence system provides a database designed to support the national intelligence community for registration, validation, tracking and management of Production Requirements?

- a. NES.
- b. RMS.
- c. MIDB.
- d. COLISEUM.

-
-
73. (023) Which of the following is *not* a system capability of the Distributed Common Ground System?
- Dynamic sensor retasking during both LOS and BLOS operations.
 - Calculation and display of threat modeling, lethality data, and probability of detection.
 - Scalable deployments tailored to meet specific intelligence needs and theater requirements.
 - All-weather, all-light, all-source intelligence receipt processing, exploitation, and dissemination.
74. (023) What DCGS component permits the DGS to remain in garrison while supporting forward deployed aircraft?
- SSS.
 - APS.
 - SYERS.
 - MOBSTR.
75. (024) The basic DOD policies on why we classify information and the different levels of classification can be found in DOD 5200.1R and what other directive?
- AFM 1-1.
 - AFI 31-401.
 - DOD 5240.1.
 - AFMAN 14-304.
76. (024) What Executive Order established a process to identify information that must be protected as national security information?
- EO 12333.
 - EO 12334.
 - EO 12863.
 - EO 12958.
77. (024) What category of classification identifies national security information or material that requires *some* protection?
- Secret.
 - Top Secret.
 - Confidential.
 - For Official Use Only.
78. (024) What category of classification would apply if the unauthorized disclosure of information could result in significant impairment of a program or policy directly related to national security?
- Secret.
 - Top Secret.
 - Confidential.
 - For Official Use Only.

79. (025) What should be done if information that might be classified is encountered, but a source cannot be readily found to verify whether it is or isn't classified?

- a. Protect it as CONFIDENTIAL at a minimum until the actual classification level is determined.
- b. Protect it as FOR OFFICIAL USE ONLY until the actual classification level is determined.
- c. Protect it as UNCLASSIFIED information of possible intelligence value only.
- d. Do nothing unless you possess original classification authority.

80. (025) Under what program does the protection of unclassified information of possible intelligence value fall?

- a. SAP.
- b. FOUO.
- c. OPSEC.
- d. LIMDIS.

81. (025) Which of the following is *not* considered an EEFI?

- a. Security clearances of individuals.
- b. Threats in the unit's area of interest.
- c. Introduction of new equipment to the unit.
- d. Classification level of operations or programs.

82. (026) Which of the following is *not* considered an additional warning/caveat to restrict the distribution of classified material?

- a. Release To:.
- b. Restricted To:.
- c. Special Category.
- d. Limited Distribution.

83. (026) According to AFI 34-401, in which of the following does the AF authorize the use of LIMDIS controls?

- a. classified messages.
- b. sensitive foreign government materials.
- c. classified materials handled by couriers.
- d. unclassified foreign government materials.

84. (027) How is a document marked that contains sensitive information provided by a foreign government?

- a. FOREIGN LIMDIS INFORMATION.
- b. SENSITIVE FOREIGN INFORMATION.
- c. FOREIGN CLASSIFIED INFORMATION.
- d. FOREIGN GOVERNMENT INFORMATION.

-
-
85. (028) What Standard Form is used to mark computer media classified as Secret?
- SF 707.
 - SF 708.
 - SF 709.
 - SF 710.
86. (029) Which method of transporting classified information can be used for Secret material, but is not authorized for Top Secret material?
- Escort.
 - Courier.
 - Registered US mail.
 - Encrypted electronic means.
87. (030) What is used to identify Top Secret material that includes the title, date of the document, identity of the originator, date the document was received, number of copies received or later reproduced, and final disposition?
- Top Secret Register.
 - Originator Control Register.
 - Top Secret Control Officer Log.
 - Originator Accountability Log.
88. (030) How often must Top Secret documents and materials be inventoried?
- At least annually.
 - At least quarterly.
 - At least biennially.
 - At least bi-annually.
89. (031) What form is used to show that a secure container has been properly locked and checked?
- SF Form 701.
 - SF Form 702.
 - SF Form 710.
 - SF Form 711.
90. (031) What Air Force source document should be consulted for special storage requirements for SCI material?
- AFI 14-304.
 - AFI 31-401.
 - AFMAN 14-304.
 - AFMAN 31-401.

91. (031) When a temporarily accredited facility is required for the storage, handling, and processing of SCI material, for how long may it be established, and who is the approving authority?

- a. Six months or less; HQ AF/INSC.
- b. Six months or less; owning Command's SSO.
- c. Twelve months or less; HQ AF/INSC.
- d. Twelve months or less; owning Command's SSO.

92. (031) In which of the following areas is the storage of SCI material authorized?

- a. Non-discussion area.
- b. Secure working area.
- c. Temporary secure area.
- d. Temporary secure working area.

93. (032) Which of the following forms are *normally* used to record and certify the destruction of classified material?

- a. AFFMS 144, 310, and 1565.
- b. AFFMS 144 and 310 only.
- c. AFFMS 145, 310, and 1565.
- d. AFFMS 145 and 310 only.

94. (033) Which of the following is *not* one of the three general criteria that must be met before allowing an individual access to classified information?

- a. A verifiable need-to-know.
- b. An emergency situation that dictates immediate access.
- c. A valid security clearance, verified through an automated listing.
- d. Verification of a signed classified information non-disclosure agreement.

95. (034) What NATO security classification marking is comparable to our FOR OFFICIAL USE ONLY information marking?

- a. NATO RESTRICTED.
- b. NATO UNCLASSIFIED.
- c. NATO OFFICIAL USE ONLY.
- d. NATO APPROVAL REQUIRED.

96. (034) What Air Force source document provides in-depth coverage of the requirements for the marking, safeguarding, storage and dissemination of NATO classified materials?

- a. AFM 1-1.
- b. AFI 31-401.
- c. AFI 31-406.
- d. AFMAN 14-304.

97. (035) OPSEC is the process of denying our adversaries information about our capabilities and intentions by identifying, controlling, and protecting which of the following?
- special compartmented information.
 - your unit's aircraft limitations and capabilities.
 - classified information transmitted over secure telephones.
 - indicators about planning and conducting military operations.
98. (035) What are other OPSEC indicators that might disclose our vulnerabilities to our adversaries besides communications?
- operations, intelligence, and administrative indicators.
 - operations and intelligence indicators only.
 - intelligence and administrative indicators.
 - operations and administrative indicators.
99. (036) Which of the following is *not* a protective measure that falls under COMSEC?
- Cryptosecurity.
 - Physical security.
 - Emission security.
 - Information security.
100. (037) What causes the majority of all security problems involving COMSEC?
- The user's ignorance of established procedures.
 - Faulty computer systems and software.
 - Unintentional carelessness.
 - Lack of clear guidance.