Student Guide

Course: Introduction to Information Security

This training course will introduce you to the Information Security Program. Five topics are covered in the following lessons. They include: Information Security Policy, Classification, Declassification, and Safeguarding of classified information, as well as Security Briefings.

Lesson 1: Information Security Overview

Lesson Introduction

This lesson will take a look at what Information Security is, why we need it, and how it is implemented in the Department of Defense. This lesson will look into both the purpose and the history of Information Security, the Executive documents that govern the policies, and the DoD community's policy documents, and Information Security roles and responsibilities.

Information Security Overview

1. Purpose of Information Security

The purpose of the Department of Defense Information Security Program is to promote the proper and effective way to classify, protect, and downgrade official information requiring protection in the interest of national security.

It also promotes the declassification of information no longer requiring such protection. It is vital for our National Security to have a uniform program to govern the classification of information and to provide guidance on how to classify, store, transport, or destroy information. And the program must not only determine the guidance, but also oversee the application of that guidance.

2. History of Information Security

The United States has had a need for protection of sensitive information since George Washington and the Constitutional Convention. However, a formal classification system was not established until President Roosevelt issued the first Information Security Executive Order, 8381. The modern-day Information Security Program has been evolving since the 1950s and is based on a series of presidential executive orders and presidential decision directives that have established uniform information security requirements for the Executive Branch. Since President Roosevelt's initial order, Presidents Truman, Eisenhower, Kennedy, Nixon, Carter, Reagan, Clinton, and Bush have all developed Executive Orders or effected amendments to Executive Orders that have shaped the Information Security Program over time.

The Executive Orders are affected by significant factors facing U.S. national security as well as the political climate in which the order was developed. For example, our previous Executive Order 12958, as amended, was directly affected by the events of 9/11.

Following the event, provisions were added for the classification of information pertaining to weapons of mass destruction and terrorism.

President Barack Obama implements our current guidance through Executive Order 13526.

3. Timeline

If you are a history buff, you can read this table to see how information security has evolved through the past years.

1775	Articles of War – Prohibiting any unauthorized correspondence by soldiers, this limited communication with the enemy.
1776	Legislation was passed that forbade spying by civilians in time of war.
1787	During the Constitutional Convention, which opened in Philadelphia, rules were quickly adopted to insure its proceeding would be held in secrecy. All attendees had to sign an agreement before attending.
1800s	The Chief of Artillery brought to the attention of the Adjutant General the fact that the word "Confidential" was being used indiscriminately. He pointed out in one instance the fact that a paper was marked "Confidential" and contained merely formulas for making whitewash. We're still struggling with the over classification problem today. The Adjutant General, acting on the recommendations of the Chief of Artillery, issued a circular which prohibited further indiscriminate use of "Confidential" on communications from the War Department and permitted its use only on such communications "where the subject matter is intended for the sole information of the person to whom addressed." Internal issuances were to have a statement indicating the class or classes of individuals to whom the contents should be disclosed. It further stated that documents marked "Confidential" were for the use of Army officers, enlisted men and government employees "when necessary in connection with their work." This circular may well have been the first written policy on the "need-to-know" principle.
1820	Statutes were enacted to remove those restrictions and simultaneously provide for the publication of the Convention records.
1912	The War Department established the first complete system for the protection of national defense information.

1940 **Executive Order 8381**	President Franklin Roosevelt signed the first Executive Order, E.O. 8381, which formalized and provided a basis for existing classification systems then being used by both the Army and Navy. Very broad definitions on what could be classified were specified. In essence, all information pertaining to the military, its facilities, or plans could be classified. It also expanded upon the initial regulations and allowed the classification of commercial production facilities. Any information that could endanger national security could be classified. This war-time regulation affected all information whether or not it dealt with defense. For example, information developed during the Manhattan Project was classified under this E.O. This Order provided for three levels of classified material: Secret, Confidential, and Restricted. Top Secret was established at a later date.
1947 **National Security Act**	The National Security Act was created, which saw the birth of the Department of Defense, the Department of the Air Force, the Central Intelligence Agency, and the National Security Council.
1950 **Executive Order 10104**	President Harry Truman issued Executive Order 10104, which limited classification authority to the DoD. It essentially continued the policies of E.O. 8381 and added the classification level of Top Secret to the existing three levels of Restricted, Confidential, and Secret.
1951 **Executive Order 10290**	President Harry Truman issued Executive Order 10290, which extended the Information Security Program to all executive branch agencies not just the DoD. This E.O. was the first to recognize and define Restricted Data (RD) and exempt it from E.O. provisions. It also stated that information was to be protected at its lowest level consistent with the National Security and provided for downgrading and declassifying said data either automatically or upon review. Because classification authority was granted to so many agencies, both Congress and the press quickly attacked this E.O. as being overly broad.
1953 **Executive Order 10501**	In Executive Order 10501, President Dwight Eisenhower reduced the number of original classification authorities, eliminated “restricted” as a classification level, defined the classification markings and limited the application of the classification to only that information which protected our National Defense. Under this order, only experienced persons were to coordinate the classification programs of the various agencies and they were to maintain active training and orientation programs. There were also provisions for downgrading and declassifying data as warranted and automatic declassification was predicated on a date or event specified by the initial classifier.

1961 **Executive Order 10964**	President John Kennedy issued Executive Order 10964 which amended Executive Order 10501. It did not drastically change the content of the previous E.O., but amended it to include the first automatic downgrading/declassification program. It did establish four groups of information, of which one group was to be declassified automatically at 12 year intervals, the second group would be downgraded every three years until declassified; and the third and forth group were exempt from declassification. The Kennedy E.O. also added a new section specifying that any individual who knowingly revealed classified information was subject to administrative sanctions. During the 1960's, the basic rule for classification was, "If it moves, classify it Secret," and "If it move fast, classify it Top Secret." That was fine until the "information explosion". With the Vietnam War, new high tech military weapons were developed, and more and more information was classified.
1972 **Executive Order 11652**	President Richard Nixon issued Executive Order 11652, which further limited the number of classification authorities, shortened the period for downgrading, and established systematic review, establishing a 30-year date for declassification excluding certain information. He said you should take a look at the information before you decide to classify it, but "when in doubt, classify it". Other key factors were the discovery of the Pentagon Papers, due to misclassification. This E.O. also reduced the number of agencies that could classify information. It established mandatory review provisions on classified information, established automatic declassification time tables. It identified specific types of information which could not be classified and identified the need to portion mark documents. Finally, the three classification levels (Confidential, Secret, and Top Secret) were reaffirmed. President Nixon further refined information security guidance by issuing Executive Order 11714 which amended Executive Order 11652. President Ford later amended Executive Order 11652 with Executive Order 11862.
1978 **Executive Order 12065**	President Jimmy Carter continued relaxing classification requirements with the signing of E.O. 12065, on June 28, 1978. His philosophy at the time of "openness in government" influenced this Order. He limited information to a 6-year period unless the classification authority decided that there was a specific reason to continue the classification beyond that time. He also stated that "basic scientific research" could not be classified unless it was a "significant advancement beyond the state-of-the-art." Information could not be considered for classification unless it fell into a specific category. The systematic review was lowered from 30 years to 20 years for declassification. A balancing test, classification vs. the public's right-to-know, was required when information was considered for classification. When there was a doubt, the rule was in favor of release to the public. Thus, this Order advocated, "When in doubt, don't classify."

1982 **Executive Order 12356**	There were concerns under previous Executive Orders that premature declassification of national security information and public release of information occurred without consideration of our national security. This prompted a change in mindset when making changes. A new philosophy evolved that looked towards keeping some principles well established in prior orders, modifying others, and establishing a few new ones. When President Reagan signed E.O. 12356 in 1982, he recognized that we needed a more realistic system concerning declassification. The 20-year systematic review could not be done without unacceptable resource cost. The previous Order made classification "sinful." This Order recognized the need for an informed public but not at the expense of our national security. So, arbitrary dates for declassification were eliminated. When information was originally classified, the Original Classification Authority (OCA) was responsible for determining declassification instructions. A specific date or event for declassification was to be assigned. If a specific date or event could not be determined, then the notation "Originating Agency's Determination Required" (OADR) could be applied. The intent of E.O. 12356 was that classification should only be applied when information should be protected in the interest of national security, at the lowest level required and for only as long as necessary. National security includes both our national defense and foreign relations.
1995 **Executive Order 12958**	With a change of administration and a change in philosophy, President Clinton signed the first post-Cold War Executive Order 12958 on April 17, 1995. The Order was implemented on October 14, 1995. President Clinton stated that our democratic principles require that the American people be informed of the activities of their government. The Order emphasizes our commitment to open government, but still recognizes that protecting our nation's security must still remain a priority. At the time of original classification, the OCA shall attempt to establish a specific date or event for declassification based upon the duration of the national security sensitivity of the information. The options, in order of consideration, are: a date or event less than 10 years; if unable to set a date or event less than 10 years, a declassification date that is 10 years from the date of original classification decision normally will be assigned; or if qualified, the OCA may exempt the information from declassification within 10 years if it falls under one of the specific categories listed in Section 1.6(d) of the Order. The Order provides for automatic declassification for information determined to have permanent historical value when it reaches its 25th birthday. At that time, if warranted, continued classification beyond 25 years may be granted if it meets the provisions of Section 3.4 of the Order. Clinton’s philosophy was “when in doubt, don’t classify.” This E.O. prescribes a uniform system for classifying, safeguarding, and declassifying classified national security information within the Executive Branch. The Assistant to the President for National Security Affairs provides policy and program direction to the Information Security Oversight Office (ISOO) for the security classification program.

	ISOO oversees the program for both government and industry and reports annually to the President on the status of those programs. The Director, Office of Management and Budget (OMB) with approval of the President, appoints the Director of ISOO. ISOO implemented Executive Order 12958 and issued ISOO Directive #1, which expands the guidance and issues further requirements than that stated in the Order.
2003 Executive Order 12958, as amended	Many people wanted to know why the Bush administration chose not to issue a brand new Executive Order. While the number of changes presented in the amendment seem numerous enough for a new E.O., it was deemed less disruptive to proceed with changes to the current framework rather than conduct a wholesale rewrite as has been the tradition. President George W. Bush signed the Executive Order 12958, as amended. This Order continued to emphasize our commitment to openness in government, but still recognized that protecting our nation's security must remain a priority. The "ten year rule" still applied in this Order, however, taking away the exemptions. An OCA had several options while determining the duration of classified information. An OCA could choose a date or event within ten years, ten years from the date of creation, or up to 25 years from the date of creation if deemed appropriate. There were several major changes in this Executive Order to include: extending 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; broadened the protection of confidential foreign government information; simplified the process for classifying records for more than 10 years and less than 25 years and made explicit the authority of the Director of Central Intelligence to protect intelligence sources and methods.
2009 Executive Order 13526	President Barack Obama signed Executive Order 13526, proclaiming that our democratic principles require that the American people be informed of the activities of their Government and that our Nation's progress depends on the free flow of information both within the Government and to the American people. In addition, allowing for the protection of information critical to our Nation's security and demonstrating our commitment to open Government through accurate and accountable application of classification and declassification standards which are equally important priorities.

4. Executive Policy Documents

During World War II, it was evident that there were many problems and dangers that resulted from the lack of a standard Information Security system within the Government. In 1951, President Harry Truman issued Executive Order 10290, which established the first umbrella program to protect classified information for all departments and agencies of the Executive Branch. Prior standardization was only implemented for the military departments.

The current Executive Order 13526 was issued by President Barack Obama in 2009. The time had come to revitalize the protection requirements of our classified information. This new executive order directed a review of policy, to include proposals concerning establishment of the National Declassification Center, effective measures to address the problem of over classification, increased accountability for classification decisions, consideration of the electronic environment, and greater openness and transparency while also affording necessary protection for the Government's legitimate interests.

In addition, it strengthens training requirements for OCAs and derivative classifiers. The Executive Order requires derivative classifiers to be identified by name and position, or by personal identifier, mandates use of classified addendums or unclassified versions of documents, requires agencies conduct fundamental classification guidance reviews to ensure that classification guides reflect current conditions, mandates self-inspection programs to include regular reviews of representative samples of original and derivative actions, makes clear that classification challenges from authorized holders are not limited to those within the classifying agency, modifies what was previously known as the "Third Agency Rule," which allows classified information from one agency to be provided to another agency or U.S. entity, without the consent of the originating agency, and allows for declassification exemptions of 50 and 75 years for specific categories of information.

5. Executive Policy Support

The responsibility of the Information Security Oversight Office, or ISOO, is to oversee and manage the information security program, under the guidance of the National Security Council, or NSC.

The NSC provides the overall policy direction for the Information Security Program. It assists the President in developing and issuing National Security Policies, and it guides and directs the implementation and application of the Executive Order. The NSC exercises its guidance primarily through the ISOO. Executive Order 12958, as amended, made the ISOO responsible for the administration and monitoring of the Information Security Program for the NSC. In other words, the ISOO is the operating arm for information security. The ISOO issues the Classified National Security Information Directive, 32 CFR, Parts 2001 and 2003, Final Rule; which implements the Executive Order and further defines what the Executive Branch agencies must do to comply with the Executive Order requirements.

There is a chance that you may find yourself contributing to one of the documents that falls within the ISOO's Annual Report to the President. Each agency and department within the Executive Branch must annually submit a Standard Form 311, or SF-311, to ISOO, titled the "Agency Security Classification Management Program Data." Some examples of information the SF-311 requests are how many original classification authorities are within your activity, and how many original or derivative classification decisions were made during the past year. Every year, the ISOO combines all of this data and reports it to the President.

6. DoD Policy Documents

The Department of Defense has designated a senior official for implementing its Information Security Program. The Under Secretary of Defense for Intelligence has the primary responsibility for providing guidance, oversight, and approval authority of policies and procedures that govern the DoD Information Security Program.

The USD(I) provides guidance by issuing the DoD Instruction 5200.01. This Directive establishes the basic information security policies for the DoD and authorizes the publication of DoDM 5200.01, Volumes 1 through 4, the DoD Information Security Program. This regulation establishes the baseline for security requirements for all of DoD. The DoDM 5200.01, Volumes 1 through 4 provide guidance and direction on classification management, for both original and derivative classification. It also provides marking, protection, and handling requirements for classified information.

It is important to remember that the DoD Components and Defense Agencies add their own requirements to the DoD standards. They do this in order to ensure that security measures are effective for their unique missions and functions. They monitor the Information Security Program within their organizations and designate a senior agency official to oversee the program. Those senior agency officials are responsible for directing and administering the program within their component or agency. They accomplish this through monitoring and reporting on the status of the Information Security Program at all levels of activity under their cognizance. Some activities apply more stringent standards than ones included in the regulation.

Within the DoD Components and Agencies the head of each activity must appoint an official to serve as its Security Manager. The Security Managers are responsible for the administration of effective Information Security Programs within their activities. Some of the important Information Security functions they deal with include: Security Education and Training, Assignment of Proper Classifications, Downgrading and Declassification, Safeguarding, and Program Monitoring.

Review Activity 1

Select True or False for this statement. When you are finished, see the Answer Key at the end of this Student Guide to check your answer.

		True	False
Executive Order 13526 establishes uniform information security requirements for the Executive Branch and the DoD community.		○	○

Review Activity 2

Match each Executive Order to the president who issued it. Check your answers in the Answer Key at the end of this Student Guide.

A. E.O. 10501, as amended (1961) __ Richard Nixon

B. E.O. 10501 (1953) __ Dwight Eisenhower

C. E.O. 10290 (1951)	___	Jimmy Carter
D. E.O. 11652 (1972)	___	Bill Clinton
E. E.O. 12958, as amended (2003)	___	Harry Truman
F. E.O. 12065 (1978)	___	George W. Bush
G. E.O. 8381 (1940)	___	Ronald Regan
H. E.O. 12356 (1982)	___	John Kennedy
I. E.O. 12958 (1995)	___	Franklin Roosevelt

Answer Key

Review Activity 1

		True	False
Executive Order 13526 establishes uniform information security requirements for the Executive Branch and the DoD community.		●	○

Review Activity 2

A. E.O. 10501, as amended (1961)	D	Richard Nixon
B. E.O. 10501 (1953)	B	Dwight Eisenhower
C. E.O. 10290 (1951)	F	Jimmy Carter
D. E.O. 11652 (1972)	I	Bill Clinton
E. E.O. 12958, as amended (2003)	C	Harry Truman
F. E.O. 12065 (1978)	E	George W. Bush
G. E.O. 8381 (1940)	H	Ronald Regan
H. E.O. 12356 (1982)	A	John Kennedy
I. E.O. 12958 (1995)	G	Franklin Roosevelt

Lesson 2: Classification

Lesson Introduction

This lesson will take a look at the classification of information. As a security professional, one of your vital duties is to protect our country's classified information. You can perform this by following the requirements for properly identifying, safeguarding, handling, transmitting, and destroying classified materials. In order to protect this information you will need to identify it as sensitive, classify it, and then ensure that only authorized personnel with a need-to-know gain access to it. This lesson will provide you with an introduction to working with classified materials.

At the end of this lesson, you will be able to identify:

- Levels and types of classified information to include: Top Secret, Secret, and Confidential
- The definition of original classification
- What information is found in a Security Classification Guide
- The definition of compilation
- The definition of derivative classification

Classification Levels and Types

1. Overview

Classified materials contain information that requires protection against unauthorized disclosure in order to protect our national security. What is National Security? National Security concerns the national defense or foreign relations of the United States. Let's take a second and break down this definition a bit more.

First of all, it is important to remember that classified information requires protection from unauthorized disclosure. Disclosure of the information could inhibit our national defense capabilities or adversely affect our foreign relations.

The second factor to remember is that in order for the information to be eligible for classification, it must be official government information that is owned by, produced by, produced for, or under the strict control of the U.S. government. When dealing with classified information, control means, "the authority to regulate access to the information," so that the information is under the jurisdiction of the U.S. government. So, if materials are controlled by the U.S. government and disclosure of the information could cause damage to the national security, then it may be classified.

Once the determination is made that the information must be classified, then the next step is to designate the level of classification. What are these designations, how are they

assigned, and how do you handle these materials? These questions will be answered in this lesson.

2. Marking and Designating Classified Information

Marking and designating classified information are the specific responsibilities of original and derivative classifiers. Markings and designations serve to alert holders to the presence of classified information, information protected under the Freedom of Information Act, and technical information with restrictions on its dissemination; identify, as specifically as possible, the exact information needing protection; indicate the level of classification assigned to the information; provide guidance on downgrading and declassification; give information on the source or sources and reason or reasons for classification or other restrictions; and finally warn holders of special access, control, or safeguarding requirements.

3. Top Secret, Secret, and Confidential

The three levels of classification that can be designated are Top Secret, Secret, and Confidential, which are delineated by Executive Order 13526. As part of the executive branch, the Department of Defense utilizes these designations for sensitive national security information.

Let's take a moment to define these levels. Top Secret is applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

Let's compare that to Secret information. Secret is applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

Finally, Confidential is applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Always remember that ALL classified information can cause damage to the national security if it is disclosed without the proper authorization. The difference between the designations is the severity of the damage that could be caused.

Because all three levels of classification designate information that has the potential to damage national security, all classified information must be properly protected from unauthorized disclosure. In addition, there are special rules applied to other types of information that, due to their nature, require additional handling and protection. Some of these include Communications Security, or COMSEC, atomic energy information, and Sensitive Compartmented Information, or SCI, among others.

4. Original Classification Overview

Now, after you have an understanding of what classified information is, and what levels are assigned to it, you will need to take a look at how information is classified in the first place.

Original classification is defined as an initial determination that information requires protection against unauthorized disclosure in the interest of national security. This determination can only be made by a designated Original Classification Authority, also known as an OCA. The President has delegated original classification authority to a few positions within the DoD, and those individuals have delegated original classification authority to other officials who need it.

Within the DoD, original classification authority is delegated to the occupant of a position, not to an individual by name. This means that if someone moves to another position, or is on leave, the person occupying the OCA position holds the authority. The delegation of authority will specify the highest level the OCA can classify a piece of information. This means, if the OCA delegates authority to an official at the Secret level, then that official will only be able to classify information at a Secret level, or below.

Because of the importance of their responsibilities, OCAs must go through training prior to exercising their authority. The DoD Information Security Program Manual DoDM 5200.01, Volumes 1 through 4, stresses that OCAs must be aware of their responsibilities and it also makes the management of classified information a critical element of their performance evaluations.

5. Original Classification Process

Original Classification Authorities apply a process to making classification determinations.

Step 1: Determine if the information is official government information

The OCA must ensure that the information is official government information and not already classified. Remember, for information to be classified, the U.S. Government must own, have proprietary interest in, or control the information. During this step, the OCA must ensure that the information was not already classified by another OCA. If the information was already classified, the OCA would use the prior classification decision.

Step 2: Determine if the information is eligible to be classified

The OCA will determine whether the information is eligible to be classified by first examining the categories of information, which E. O. 13526 authorizes for classification. The second part of determining eligibility is to ensure that the information is not specifically prohibited or limited from being classified. In other words, the OCA must ensure that classification is not being considered for some reason other than to protect national security. This means no smokescreens to cover up or promote any wrongdoings. Classification prohibitions and limitations are also spelled out in E.O. 13526.

Step 3: Determine if there is a potential for damage to national security if unauthorized release occurs

The OCA must exercise good judgment for this step. They must determine if unauthorized disclosure of the information could reasonably be expected to cause damage to the national security, which includes defense against transnational terrorism. The determination is much more than a hunch. E.O. 13526 requires that the damage can be identified or described by the OCA.

Step 4: Assign a level of classification

After identifying the potential for damage and resulting need to classify, the OCA then assigns a level of classification to the information. As a reminder, the levels of classification are based upon the degree of damage the unauthorized disclosure of the information could cause to the national security. Again, the OCA must perform a judgment call for assigning the level of classification. Here is a rule of thumb. If there is a significant doubt about the appropriate level of classification, the information must be classified at the lower level.

Step 5: Make a decision about the duration of classification

At the same time an OCA determines that information should be classified, they also must make the decision on how long the classification should last. Once again, E. O. 13526 provides guidance regarding the duration of classification.

Step 6: Communicate the decision

The final step is where the OCA communicates the decision. There are two methods for communicating the decision: the security classification guide and properly marked source documents.

6. Security Classification Guides

A security classification guide, also known as an SCG, is a document issued by an OCA that provides derivative classification instructions. It describes the elements of information that must be protected, as well as the level and duration of classification.

Security classification guides are issued for programs, projects, plans, and systems and spell out the guidelines that must be followed by individuals working with classified information associated with these activities. Derivative classifiers (anyone who applies markings for a new document or material conveying classified information or based on already classified information) use the information from an SCG to determine if something is classified, its classification level, downgrading instructions, declassification instructions, special control notices, or other information pertinent to the proper classification and dissemination of the items in question.

Finally, the SCGs provide contact information for the OCA so that anyone using classified information regarding the system, plan, program, or project can contact them for clarification or review if necessary.

7. Compilation

Another important factor affecting classification is the concept of compilation. In some circumstances, combining elements of information that are individually unclassified may be classified if the compiled information reveals an additional association or relationship that qualifies for classification under DoD policy, and the information is not otherwise revealed when standing alone. Types of information that are commonly classified through compilation are budgets and tables of distribution; staffing and equipment allowances; and mission and geographic location.

For instance, classification by compilation involves combining two or more pieces of unclassified information that, by virtue of being combined or associated, warrant protection as classified information. The resulting classification may range from Confidential up to Top Secret.

OCAs designate when and what types of information are classified through compilation. This concept also applies to elements of information classified at a lower level which when put together reveal an additional factor that warrants classifying the information at a higher level when combined. The OCA will include a clear explanation of the basis for classification by compilation.

Let's take a look at a sample SCG about the 327th Infantry Division. According to the guide, both unit strength and unit location are to be marked as unclassified if used individually. Note the guide also states that when combined, these items require classification at the Secret level. Now, if you were to write a memo that includes information on both of these items, it would need to be designated as classified at the Secret level and your document must be marked to reflect this.

Security Classification Guide				
	U	**C**	**S**	**TS**
Unit Strengths	x			
Unit Location	x			
Compilation of the unit strength with unit location, within the same document			x	

8. Derivative Classification Overview

Earlier you learned that only the OCA has the authority to declare original classification of information, but the rest of us can perform something called derivative classification. Derivative classification is not an authority, but is more of an assumed responsibility of an individual. This responsibility pertains to anyone who applies markings for a new document or material conveying classified information.

Derivative classification means the incorporating, paraphrasing, restating, or generating in new form any information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information.

Derivative classification includes classifying information based on classification guidance. The duplication or reproduction of existing classified information is not derivative classification.

9. Derivative Classification Process

Now that you have an idea of what derivative classification is, let's concentrate on the five requirements you should be aware of when performing derivative classification. Performing derivative classification is much harder than it sounds, but if you follow these requirements, your job will be much easier.

First, observe and respect the OCA's original classification determinations. Don't second-guess the OCA. There are situations where you may want to consult with the OCA to determine whether the classification is warranted, but these are special occasions.

Second, be sure to apply required markings. The primary purpose of marking is to alert the holder of the presence of classified information. Marking also informs holders about specific protection requirements. This means that derivative classifiers must take special care in transferring and accurately applying the appropriate markings for classified information.

Next, use only authorized sources. Authorized sources are considered Security Classification Guides and properly marked source documents. When there is a conflict between a source document and a Security Classification Guide, the SCG takes precedence.

Then, use caution when paraphrasing or restating classified information extracted from a classified source document. Derivative classification requires subject matter knowledge, analytical ability, and an understanding of classification management techniques. Derivative Classifiers must be aware of circumstances which, when paraphrasing or restating, can change the classification.

Finally, always take the appropriate steps to resolve any doubts you have. If you have problems applying classification guidance or suspect the markings on source documents are incorrect, you should contact your security manager or the originator of the information.

Review Activity 1

Try this derivative classification activity. Select the appropriate classification level, as described on the sample SCGs, for each scenario. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Sample SGC:

S – Existence of Sarin
TS – Location of Sarin
TS – Quantities of Sarin

Scenario	S – Existence of Sarin	TS – Location of Sarin	TS – Quantities of Sarin
On-site inspection agency has reported mass quantities of Sarin.	○	○	○
Ugottabekidn Army Depot has found traces of Sarin just outside the post.	○	○	○
They found 1500 full oil drums.	○	○	○

Sample SGC:

C – Maximum altitude pressure
S – Chamber capacity
TS – Chamber size

Scenario	C – Maximum altitude pressure	S – Chamber capacity	TS – Chamber size
With staff members serving as inside observers, the chamber is taken to a maximum altitude pressure of 43K feet (FL 430).	○	○	○

Sample SGC:

S – Vulnerabilities
C – Limitations

Scenario	S – Vulnerabilities	C – Limitations
The hairline surface cracks, which are less than an inch long, were discovered in a lower area where 140 bolts attach a 190-pound transparency to the canopy frame, and aren't visible to a pilot sitting in the cockpit.	○	○

Review Activity 2

Select the correct word from each group to complete the sentence. Check your answers in the Answer Key at the end of this Student Guide.

Group 1:

A. Top Secret
B. Secret
C. Confidential

1. Unauthorized disclosure of _____ information could reasonably be expected to cause serious damage to our national security.
2. Unauthorized disclosure of _____ information could reasonably be expected to cause exceptionally grave damage to our national security.
3. Unauthorized disclosure of _____ information could reasonably be expected to cause damage to our national security.

Group 2:

A. Original Classification
B. Compilation
C. Derivative Classification

4. _____ is defined as the incorporating, paraphrasing, restating, or generating in new form any information that is already classified.
5. _____ is defined as an INITIAL determination that information requires, in the interest of national security, protection against unauthorized disclosure.
6. _____ is defined as unclassified information or classified information (at a lower level) that when the information is combined or associated reveals additional factors that qualifies for classification.

Group 3:

A. Original Classification Process
B. Security Classification Guides (SCG)
C. Original Classification Authority

7. _____ is the term used to identify individuals specifically authorized in writing to make initial classification decisions.
8. _____ contain classification levels, special requirements and duration instructions for programs, projects, plans, etc.
9. _____ is the six step process an OCA applies in making classification determinations.

Answer Key

Review Activity 1

Sample SGC:

S – Existence of Sarin
TS – Location of Sarin
TS – Quantities of Sarin

Scenario	S – Existence of Sarin	TS – Location of Sarin	TS – Quantities of Sarin
1. On-site inspection agency has reported mass quantities of Sarin.	●	○	○
2. Ugottabekidn Army Depot has found traces of Sarin just outside the post.	○	●	○
3. They found 1500 full oil drums.	○	○	●

Sample SGC:

C – Maximum altitude pressure
S – Chamber capacity
TS – Chamber size

Scenario	C – Maximum altitude pressure	S – Chamber capacity	TS – Chamber size
With staff members serving as inside observers, the chamber is taken to a maximum altitude pressure of 43K feet (FL 430).	●	○	○

Sample SGC:

S – Vulnerabilities
C – Limitations

Scenario	S – Vulnerabilities	C – Limitations
The hairline surface cracks, which are less than an inch long, were discovered in a lower area where 140 bolts attach a 190-pound transparency to the canopy frame, and aren't visible to a pilot sitting in the cockpit.	●	○

Review Activity 2

Group 1:

A. Top Secret

B. Secret

C. Confidential

1. Unauthorized disclosure of ____B____ information could reasonably be expected to cause serious damage to our national security.
2. Unauthorized disclosure of ____A____ information could reasonably be expected to cause exceptionally grave damage to our national security.
3. Unauthorized disclosure of ____C____ information could reasonably be expected to cause damage to our national security.

Group 2:

A. Original Classification

B. Compilation

C. Derivative Classification

4. _____C_____ is defined as the incorporating, paraphrasing, restating, or generating in new form any information that is already classified.
5. _____A_____ is defined as an INITIAL determination that information requires, in the interest of national security, protection against unauthorized disclosure.
6. _____B_____ is defined as unclassified information or classified information (at a lower level) that when the information is combined or associated reveals additional factors that qualifies for classification.

Group 3:

A. Original Classification Process
B. Security Classification Guides (SCG)
C. Original Classification Authority

7. ____C____ is the term used to identify individuals specifically authorized in writing to make initial classification decisions.
8. ____B____ contain classification levels, special requirements and duration instructions for programs, projects, plans, etc.
9. ____A____ is the six step process an OCA applies in making classification determinations.

Lesson 3: Declassification

Lesson Introduction

This lesson will take a look at the declassification of information. We will discuss what declassification is, and how it works.

Declassification is the authorized change in the status of information, from classified to unclassified. As you will remember, when an Original Classification Authority, or OCA, determines the level of classification for information, they must also determine the duration of the classification and when the information can be declassified.

This lesson will provide an introduction to the declassification of materials. On its completion, you will be able to define the processes and systems of declassification and the requirements of declassification.

Processes and Systems

1. Overview

One of the foundational characteristics of Executive Order 13526 is its promotion of declassification and public access to information as soon as national security considerations permit. This reinforces the concept of openness within government, but also recognizes the government's duty to protect information that could reasonably damage our national security.

A classification designation for information can end one of two ways, either through downgrading or declassification. Downgrading of information to a lower level of classification is appropriate when the information no longer requires protection in the interest of national security, at the originally assigned level, and can now be properly protected at a lower level. An example of this would be to downgrade a Secret document to Confidential. In contrast, declassification occurs when an authorized change in the status of information changes from classified information to unclassified information. Declassifying information means that it no longer requires protection in the interest of national security at any level.

This section will cover the four declassification systems: scheduled, automatic, mandatory, and systematic. Other special circumstances may arise that could warrant declassification actions. These include classification challenges and reevaluation of classified information.

2. Scheduled

One of the methods by which information can be declassified is through Scheduled declassification. Scheduled declassification occurs when the instructions assigned by the OCA, at the time the information is originally classified, are followed to declassify it.

Scheduled declassification instructions consist of either a date or event for declassification. So, for example, if on January 15, 2006, an OCA determines that

information is to be declassified on January 14, 2016, then, on that date, the information is declassified. It's that simple.

3. Automatic

Another way information is declassified is through automatic declassification. Executive Order 13526 has set up a system where all classified records that have been determined to have permanent historical value under title 44 of the United States Code, will be automatically declassified on December 31st of the year that is 25 years from the date of its original classification.

Now naturally, there are a few categories of information that may require protection beyond 25 years. The Executive Order has established 9 categories of information that may be classified beyond 25 years. You can easily identify this information by the use of a 25X instruction for declassification. The exemptions are annotated as 25X with the category number following the X, for example, 25X1 or 25X9. We will cover this topic in depth in another course.

4. Mandatory Declassification Review (MDR)

Mandatory review is another method of declassifying information. Let's say that an agency is working on a classified project, and John Q. Public from Boise, Idaho sends a letter requesting information about the project. Mr. Public knows that the information is classified, but he wants it reviewed to see if it can be declassified and made available to the public. This is called a request for mandatory declassification review. When such a request is made, the originating agency must respond in a timely manner.

5. Systematic

Let's talk for a moment about Systematic Review. Information which is generated within the Department of Defense and declared permanently valuable is provided to the National Archives and Records Administration or another archiving facility. Some of that information is classified, so that is when the systematic review for declassification program comes into play.

Under this program, permanently valuable classified records are reviewed for declassification after they reach a specific age. Within the DoD, Component Heads have established systematic review programs for declassifying information in the custody of the Component that is contained in permanently valuable historical records, and exempt from automatic declassification.

Review Activity 1

Find the correct answer for each question. Check your answers in the Answer Key at the end of this Student Guide.

1. What is declassification? ___

2. What is Automatic Declassification? ___

3. What is Systematic Declassification Review? ___

4. Who are all known holders of the information? ___

5. What is Mandatory Declassification Review (MDR)? ___

6. What is Scheduled Declassification? ___

A. The individuals who need to be notified if the duration of classification has been changed

B. The declassification system where the public can ask for classified information be review for declassification and public release

C. The declassification system where information exempted from automatic declassification is reviewed for possible declassification

D. The declassification system where an OCA, at the time the information is originally classified, sets a date or event for declassification

E. The declassification system where Permanently Valuable Historical records are declassified when they are 25 years old

F. The authorized change in the status of information goes from classified information to unclassified information

Requirements

1. Overview

Why do we want to declassify information? Why not keep it classified forever?

As a tax payer, we have a right to know what our money is supporting. Executive Order 13526 promotes a government of openness. Imagine how much classified information we would have if we never declassified it. The Information Security Oversight Office (ISOO) Report for Fiscal Year 2011, as required by Executive Order 13525, states that almost 1.5 billion pages of information have been declassified as if 2011. Think of all the money we are saving in security containers, vaults, manpower, and alarms when we no longer classify information.

How long information should remain classified is always a good question. Information shall remain classified as long as it is in the best interest of national security to keep it protected, and that its continued classification is in accordance with Executive Order 13526.

This declassification section will cover general information about approved markings and instructions, the 25 year rule and exemptions.

2. Markings and Instructions

It is important to recognize the required and approved declassification markings for classified information. As you may recall, when information is originally classified, the OCA must determine when that information will be declassified. Declassification instructions are placed on the front of a document and usually appear as declassify on, and the date, or declassify on, and the event.

As with many rules there are exceptions, and this is also true for declassification. For example, declassification instructions are not applied to Restricted Data (RD) and Formerly Restricted Data (FRD). The Department of Energy (DOE) determines when Restricted Data will be declassified. Declassification of Formerly Restricted Data takes a joint determination by DOE and DoD. Documents containing Restricted Data or Formerly Restricted Data should not have declassification instructions.

3. OCA Declassification Options

When OCAs originally classify information they must also make declassification determinations for the information they classify. OCAs base their decisions on predictions about the loss of the information's sensitivity, as well as observing the requirements for declassification within Executive Order 13526. The OCA's declassification options are a specific date or event at 25 years or less, or by 50X1 HUM or 50X2-WMD exemption with no event or date of declassification.

So, this means that declassification instructions on a document which was created on June 12, 2006 could appear as declassify on 20260412, which is a specific date, declassify on completion of operational testing, which is an event, declassify on 50X1-HUM, or declassify on 50X2-WMD. The 50X1-HUM exemption is applied when the OCA is classifying information that could be expected to reveal the identity of a confidential human source, or human intelligence source. The 50X2-WMD exemption is applied to information that could reveal key design concepts of weapons of mass destruction. OCAs having jurisdiction over such information may utilize these last two options without prior ISCAP approval.

4. Exemptions

Executive Order 13526 has set up a system to declassify information when the records become 25 years old. This is called automatic declassification. Records are automatically declassified when they become 25 years old, unless an agency head designates them to be kept classified for more than 25 years.

Documents exempted by an agency head from automatic declassification will be marked 25X, 50X, or 75X plus a brief reference to the pertinent exemption category or number that corresponds to the category in section 3.3(b) of Executive Order 13526. In the Order, there is a list of categories eligible for exemption from automatic declassification for your review. Information exempted from automatic declassification remains subject to the mandatory and systematic declassification review provisions of DoDM 5200.01.

Review Activity 1

Find the correct answer for each question. Check your answers in the Answer Key at the end of this Student Guide.

1. What is declassification?	___	**A.** The individuals who need to be notified if the duration of classification has been changed
2. What is Automatic Declassification?	___	**B.** The declassification system where the public can ask for classified information be review for declassification and public release
3. What is Systematic Declassification Review?	___	**C.** The declassification system where information exempted from automatic declassification is reviewed for possible declassification
4. Who are all known holders of the information?	___	**D.** The declassification system where an OCA, at the time the information is originally classified, sets a date or event for declassification
5. What is Mandatory Declassification Review (MDR)?	___	**E.** The declassification system where Permanently Valuable Historical records are declassified when they are 25 years old
6. What is Scheduled Declassification?	___	**F.** The authorized change in the status of information goes from classified information to unclassified information

Review Activity 2

Find the correct answer for each question. Check your answers in the Answer Key at the end of this Student Guide.

1. What are the options an OCA has when determining declassification?	___	**A.** Restricted Data and Formerly Restricted Data
2. What is the 25-year rule?	___	**B.** Specific Date, Specific Event, or by the 50X1-HUM Exemption
3. For how long should information be classified?	___	**C.** As long as it is in the best interest of National Security to keep it protected
4. What type of information does not provide declassification instructions?	___	**D.** The process where records automatically become declassified after 25 years

Answer Key

Review Activity 1

1. What is declassification?	F	**A.** The individuals who need to be notified if the duration of classification has been changed
2. What is Automatic Declassification?	E	**B.** The declassification system where the public can ask for classified information be review for declassification and public release
3. What is Systematic Declassification Review?	C	**C.** The declassification system where information exempted from automatic declassification is reviewed for possible declassification
4. Who are all known holders of the information?	A	**D.** The declassification system where an OCA, at the time the information is originally classified, sets a date or event for declassification
5. What is Mandatory Declassification Review (MDR)?	B	**E.** The declassification system where Permanently Valuable Historical records are declassified when they are 25 years old
6. What is Scheduled Declassification?	D	**F.** The authorized change in the status of information goes from classified information to unclassified information

Review Activity 2

1. What are the options an OCA has when determining declassification?	B	**A.** Restricted Data and Formerly Restricted Data
2. What is the 25-year rule?	D	**B.** Specific Date, Specific Event, or by the 50X1-HUM Exemption
3. For how long should information be classified?	C	**C.** As long as it is in the best interest of National Security to keep it protected
4. What type of information does not provide declassification instructions?	A	**D.** The process where records automatically become declassified after 25 years

Lesson 4: Safeguarding

Lesson Introduction

This lesson will take a look at how we can protect our classified information with effective safeguarding practices. After you complete this safeguarding lesson, you will have an understanding of the procedures put in place for protecting information, dealing with incidents of potential and actual compromise, the reproduction and transmission of materials, transporting classified materials, the disposition and destruction of materials, and handling special types of information.

Responsibilities

1. Overview

If your workplace handles classified information, you must have established procedures in place to avoid any unauthorized disclosure of classified materials, and to deter anyone from removing classified information without authorization. In this lesson, you will learn about handling classified information in the workplace.

The first basic component of safeguarding information is custodial responsibilities. Custodians are people who are in possession of, or who are otherwise charged with safeguarding classified information. As a custodian, you have important responsibilities that include providing protection for information at all times. The custodian is also charged with ensuring that classified information is locked in an approved storage container or facility whenever it is not in use or under the direct supervision of authorized persons. Custodians must verify a person's need-to-know and access before providing that individual with any classified information. Finally, the custodian must follow all established procedures to ensure that unauthorized persons do not gain access to classified information.

Who could be a custodian? If your supervisor presents you with confidential documents while you are working on a project, you become the custodian for that information. Security of classified materials is a responsibility that all custodians must take seriously.

Now that you have an understanding of what custodians do, let's look at the procedures that custodians must follow. At the end of this section, you will have an understanding of the storage and open storage requirements, access control, and the operating procedures for a classified working environment. You will also learn about the various forms you will need to use.

2. Storage

It is a fact that classified information spends far more time not being used than being used. That is why the safekeeping and the storage of classified material is so very important.

Where do you store this information when you are not actively working with it? There are three authorized places in which you can store classified information. They are your

head, your hands, and an approved container. The head and hands are pretty self explanatory, but the container needs a bit more discussion.

The most commonly used containers are the General Services Administration, or GSA, approved security containers. They come in a variety of configurations including one-drawer, field safe, two-drawer, five-drawer, five individual locking drawers, or modular vault. In addition to GSA approved security containers, we also use secure rooms and vaults. But, we MUST remember the bottom line. An approved security container MUST be used whenever the classified material is not under supervision by a custodian.

For all security containers, other than secure rooms and vaults, GSA writes the specifications for the containers, and then the container manufacturers submit their products for testing against these standards. If the product meets the specifications, GSA certifies it. When you see this GSA approval label, you know that the cabinet has been certified.

You should also know that each level of classification has its own minimum storage requirements.

3. Open Storage Requirements

Open Storage is a term used to describe the ability to store classified information openly in an area that has been designated for this purpose. Open Storage areas are designed to meet the safeguarding requirements of a vault or secure working space. This topic will be explored in more depth in the Introduction to Physical Security Course.

4. Access Control

Our first responsibility is to ensure that only authorized personnel have access to classified information. Access means the ability and opportunity to obtain knowledge of classified information. We are concerned with any loss that may happen to our information.

We must be concerned with our access control measures which will deter deliberate attempts to gain unauthorized access. To do this, we implement security countermeasures such as fences, badges, guards, security containers, and other measures.

As security professionals we know the final responsibility for determining an individual’s access to information rests with the individual who has authorized possession, knowledge, or control of the information, and not on the prospective recipient.

There is a formula for granting access to classified information. First, verify the individual’s clearance eligibility. Second, determine the individual’s need-to-know. Need-to-know is a determination made by an authorized holder of classified information that a prospective recipient requires access to specific classified information in order to perform or assist in a lawful and authorized governmental function. Finally, acknowledge that the SF-312 has been completed. The SF-312 is a contractual agreement between

the U.S. Government and a cleared employee that must be executed as condition of access to classified information. By signing the SF-312, the cleared employee agrees never to disclose classified information to an unauthorized person.

In addition to the basic formula for access, there are also special access requirements for a variety of special personnel or special situations. For example, we have special procedures for granting access to classified information for foreign nationals. We cover more about access in the Introduction to Personnel Security course.

5. Procedures in a Classified Workplace

As we discussed earlier, classified information custodians are charged with providing protection of the information at all times, whether it is locked up in an appropriate storage container or under supervision by authorized persons. They will need to verify a person's need-to-know and access prior to providing that person with any information. They also need to follow procedures to ensure that unauthorized persons do not gain access to the classified information. This section will discuss some of the practices and procedures a custodian will need to make part of their daily life.

a. Coversheets for Classified Information

The first practice we need to talk about is the use of classified information cover sheets. Be sure to use cover sheets! Cover sheets block classified information from view so no one can read it. You should immediately cover the classified document when someone who is not authorized to access the information is present.

Cover sheets also remind the person working with the document that they have classified materials in their work area. There are three cover sheets that you will need to use. The SF-703 is used for Top Secret documents, the SF-704 is used for Secret documents, and the SF-705 is used for Confidential documents. Check with your activity or component to identify other cover sheets that may be appropriate for other types of special or sensitive information.

b. Other Items Containing Classified Information

In addition to protecting classified documents, you must also remember to protect other items in the office that contain classified information such as any preliminary drafts, worksheets, and other materials. Be sure to properly destroy these items after they have served their purpose. Otherwise they need to be given the same secure handling as the classified information itself. For instance, a "post-it" note placed on a classified document may pick up the imprint of the information on the adhesive. The note would need to be properly destroyed or protected as classified as quickly as possible.

c. Classified Discussions

One other reminder about the office concerns classified discussions over the telephone. Discuss classified information only over phones with approved secure communications circuits. Know how to use your Secure Telephone Equipment, or STE. Remember just because you are on an STE does not mean that someone can't hear your end of the conversation. Always know who is nearby when using this telephone.

d. Reproduction of Classified Information

Another important workplace responsibility is following proper procedures when it comes to copying classified information. Each office that reproduces classified information must have procedures in place to ensure that both the originals and copies are properly protected.

The first thing you should check is if the document has a reproduction control notice. If the information is marked with a statement such as, "Reproduction requires approval of originator or higher DoD authority," then you MUST contact those individuals prior to reproducing the document. You can contact the authority by phone, letter, or fax.

Individuals who receive copies need to remember that all copies of classified documents, reproduced for any purpose, including those incorporated in a working paper are subject to the same controls prescribed for the original document. In other words, if the original needed to be accounted for, so does the copy.

e. Forms for Security Checks

Let's take a look at a few more important forms used during your workday. Each activity that processes or stores classified information must establish a system of security checks at the close of each working day. The SF 701, or the Activity Security Checklist, is used to record these checks. The list involves verifying that the security container is properly locked. In addition to checking your container, you should check around your entire work area, including your desk, desktop, trash can, copier, and any other place that classified material might inadvertently be left. The form is also used to remind personnel to properly lock work areas and, if applicable, to activate security alarms. The form is also frequently used for safety purposes in addition to security purposes. The blank spaces can be utilized for additional warranted security and safety items, such as a block to remind personnel to complete tasks, such as turning off coffee pots. The idea of this checklist is to verify that you did not accidentally leave classified materials unsecured, as well as, to ensure the area is safe and secure.

Another form you should be familiar with is the SF 702, or the Security Container Check Sheet, which is used to record the opening and closing of your security container. It is a good practice to fill out the SF 702 every time you open, lock, and check the container. The SF 702 serves as a record of what actions have been taken with the container. If there is an open container violation, the form

helps to narrow the scope of inquiry. This form also gives you a snapshot of the types of uses for the container. The form serves as a reminder to take certain actions with the container. So each time you perform an action, you fill out the form. Before long, the behavior will become a habit, and your actions will be recorded for the benefit of everyone.

Review Activity 1

Select the best answer for each of the following questions. Check your answers in the Answer Key at the end of this Student Guide.

1. The people who are in possession of, or who are otherwise charged with safeguarding classified information.
   - ☐ Custodians
   - ☐ Handlers
   - ☐ Escorts
   - ☐ Officers

2. Which agency is responsible for approving security containers for the storage of classified material?
   - ☐ GAO
   - ☐ GSA
   - ☐ NGA
   - ☐ SGA

3. What is the basic formula for granting access to classified information for individuals?
   - ☐ Verify the individual's clearance eligibility
   - ☐ Determine the individual's need-to-know
   - ☐ Acknowledge that the SF 312 has been completed
   - ☐ All of the above

4. What practices should be followed when handling classified information in the workplace?
   - ☐ Properly destroy preliminary drafts, worksheets, and other material after they have served their purpose
   - ☐ Use approved secure communications circuits for telephone conversations to discuss classified information
   - ☐ Follow proper procedures when copying classified information
   - ☐ Be sure to use security forms, such as the SF 701 and SF 702
   - ☐ All of the above

Security Incidents

A. Overview

This section will discuss the various types of security incidents and the proper actions to take if information has been compromised. The compromise of classified information could have a devastating impact on our national security. Depending on what information or materials have been compromised, it could affect lives or cause severe harm to our nation. If safeguarding fails, we need to react swiftly to the situation, and commit to not having the same incident happen in the future.

Before we learn about how to react to a security incident, we first need to understand the types of incidents that could occur. We will look first at security violations.

a. Security Violations

What specifically is a security violation? Executive Order 13526 provides a three part definition: A security violation occurs when any knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; any knowing, willful, or negligent action to classify or continue the classification of information contrary to the requirements of the order or its implementing directives; or any knowing, willful, or negligent action to create or continue a special access program contrary to the requirements of the order.

If someone fails to classify information to the proper level, or downgrade or declassify information properly, this is a security violation. If someone establishes a Special Access Program without the proper authority, or fails to shut down a SAP after being instructed to do so, this is a security violation. Security violations can be administrative in nature. It could be as simple as someone failing to mark a document correctly.

Now, here is something else to remember: a security violation may or may not involve a compromise. For instance, you are not an OCA but you originally classify information. The information in question is protected and hasn't been compromised, but your action was still a violation nonetheless.

b. Security Infractions

The other type of security incident that could occur is a security infraction. An infraction is defined as a security incident involving failure to comply with Executive Order 13526, or its implementing directives, which cannot reasonably be expected to and does not result in the loss, suspected compromise, or actual compromise of classified information.

So, failing to double-check your SF 702 or not returning a receipt for a classified document are considered examples of security infractions.

2. Unauthorized Disclosure

Let's quickly look at a few more definitions related to unauthorized disclosure. There is a difference between actual and potential compromise. Actual compromise is an unauthorized disclosure of classified information. In other words, in this case we know for sure that an unauthorized individual had access to the information. On the other hand, potential compromise means that the possibility of compromise could exist, but it is not known with certainty that it has occurred.

Next, let's take a look at what unauthorized disclosure means. This is defined as a communication or physical transfer of classified information to an unauthorized recipient. This means that the information has been compromised or disclosed to an unauthorized individual. There is something called "the neither confirm nor deny principle." If classified information appears in the public media, DoD personnel must be careful not to make any statement or comment that would confirm the accuracy or verify the classified status of the information. The rationale behind neither confirming nor denying the compromised information is the impact it would have on any other sensitive information. If there were confirmation of a compromise, then other related information that has not been compromised might be jeopardized. If nothing is said about the compromise, then other validating assumptions are avoided.

Review Activity 2

Select the correct word from each group to complete the sentence. Check your answers in the Answer Key at the end of this Student Guide.

Group 1:

A. Unauthorized disclosure

1. _____ occurs when there is a knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; action to classify or continue the classification of information contrary to the requirements of E. O. 13526 or its implementing directives; or, action to create or continue a special access program contrary to E. O. 13526.

B. Security violation

2. _____ are security incidents involving failure to comply with E.O. 13526, or its implementing directives, which cannot reasonably be expected to and does not result in the loss, suspected compromise, or actual compromise of classified information.

C. Security infraction

3. _____ is a communication or physical transfer of classified information to an unauthorized recipient.

Group 2:

A. Actual compromise

1. _____ is an unauthorized disclosure of classified information

B. Neither confirm nor deny

2. _____ is the possibility of compromise could exist but it is not known with certainty.

C. Potential compromise

3. _____ means that if classified information appears in the public media, DoD personnel must be careful not to make any statement or comment that would confirm the accuracy or verify the classified status of the information.

Transmission

1. Overview

It is inevitable that sooner or later, we will need to move classified material. Each time classified information is copied or transmitted, the risk of loss or compromise increases. In order to minimize risk, everyone is accountable for following special rules for the reproduction and transmittal of classified information. In this section, you will learn about the proper equipment and procedures that you should be aware of when reproducing and transmitting classified information. You will learn about Information Systems, or IS, equipment, facsimile machines, and secure communications, or COMSEC, equipment.

a. IS Equipment

Information Systems, or IS, refers to a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information.

Information Assurance, or IA, refers to the measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of IS by incorporating protection, detection, and reaction capabilities.

Processing classified information on an information system presents unique and challenging security issues. Some examples you may encounter are: classified information being processed on an information system that has not been specifically accredited to process classified information; spillage of classified information onto an unclassified system; and classified information sent via email over an unclassified network.

b. Facsimile

When using a facsimile machine to transmit classified information, the facsimile system must be connected through the appropriate secure communications equipment, over secure communications circuits approved for transmission of information at the specific level of classification.

The Defense Information Systems Agency, or DISA, Joint Interoperability Test Command, or JITC, maintains a register of certified secure digital facsimiles. As with any other transferring of classified information, always verify that the receiver of the information has the proper security access and need-to-know.

c. COMSEC

Communications Security, or COMSEC, is defined as the protection resulting from all measures designed to deny unauthorized persons, information of value that might be derived from the possession and study of telecommunications, and to ensure the authenticity of such communications.

COMSEC includes crypto security, emission security, transmission security, and physical security of COMSEC material and information. COMSEC requirements affect how we transmit classified information. The most common example of COMSEC requirements involves secure telephonic equipment such as the STE. Additionally, due to its sensitive nature, COMSEC information is subject to special transmission procedures found in the National Telecommunications and Information Systems Security Instruction 4001.

Review Activity 3

Identify the important details to remember when transmitting classified material. Check the box next to the points you should be aware of. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Fax Facts:

Always verify that the receiver has the proper clearance eligibility and need-to-know to handle the material.	☐
Once the materials are faxes, you no longer have custodial responsibilities for the information.	☐
DISA, Joint Interoperability Test Command (JITC) maintains a register of certified secure digital facsimiles.	☐

COMSEC Facts:

Common COMSEC approved telephones include the SME-111 and the ISS.	☐
COMSEC information is subject to special transmission procedures found in the National Telecommunications and Information Systems Security Instruction 4001.	☐
COMSEC is the protection resulting from the measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications.	☐

Transportation

1. Overview

As much as we would like to keep our classified information in the safety of our possession, it is only a matter of time before it needs to be transported to another facility. It is vital to follow the proper procedures that have been put in place to protect the materials during their journey.

In this lesson, we will cover the appropriate methods for packaging classified material for safe transportation, the transportation requirements and limitations for the various modes of transportation for classified information, and the courier responsibilities and requirements. Making sure classified material reaches its destination without compromise is everyone's responsibility. This lesson will provide you with the foundation for fulfilling your duty of protecting this information.

2. Packaging Requirements

Whenever classified information is removed from a work area, the risk of loss or compromise increases. To minimize this risk, we need to follow special rules for packaging the material. Preparing classified information for transportation is an important aspect of trying to prevent unauthorized access to it while it is in transit.

The DoDM 5200.01, Volume 3 outlines the baseline policies and procedures that must be followed to assist in safeguarding the information while it is being transported. Additionally, heads of the DoD components are responsible for establishing procedures for transmission and transportation of classified information and information-bearing material that minimizes risk of compromise while permitting use of the most cost-effective transmission or transportation means.

Classified material needs to be prepared for shipment, packaged, and sealed in ways that minimize risk of accidental exposure and facilitates detection of tampering. But before actually wrapping the material, you need to verify that all of the markings on the document itself are correct, and markings on the letter of transmittal are also accurate. Once you have verified your markings are correct, it its time to look at packaging the material.

a. Inner wrapping requirements for classified material

1. Address the envelope to an official government activity or DoD contractor.

2. Put your office's complete return address on the envelope.

3. Conspicuously mark the envelope with the highest level of classified information it contains.

4. Include any applicable special marking, such as "Restricted Data" on the envelope.

5. Place the material within the inner envelope and carefully seal the envelope to minimize the possibility of access without leaving evidence of tampering.

b. Outer wrapping requirements for classified material

1. Insert the inner envelope within the outer envelope and seal the outer envelope to minimize the possibility of access without leaving evidence of tampering.

2. Address the envelope to an official government activity or DoD contractor. Do NOT address it to an individual's name on the outer envelope.

3. Put your office's full return address on the envelope.

4. Do NOT put any markings or notations on the outer envelope that indicate that its contents are classified.

3. Methods of Transmission

There are different requirements for transporting Confidential, Secret, and Top Secret information. As simple as it might be to just pop classified documents into a post office box, or hand them over to the mail carrier, it can't be done that way. Precautions must be taken to secure classified information at all times.

The following chart is broken down by levels of classification, with helpful information, should you ever be in a position of having to transmit or transport classified information. Safeguarding classified information is the responsibility of everyone in a secure environment.

Transmission Method	Top Secret	Secret	Confidential
Direct contact between appropriately cleared personnel	X	X	X
Cryptographic Systems	X	X	X
Defense courier service	X	X	X
DoD component courier service	X	X	X
Dept of State courier service	X	X	X
Cleared U.S. military, civilian employees, or contractors	X	X	X
GSA contract holders for overnight delivery		X	X
USPS registered mail		X	X
USPS express mail		X	X
Canadian registered mail		X	X
Carriers under National Industrial Security Program (NISP) providing Protective Security Service (PSS)		X	X
Government and government contract vehicles, aircraft, and ships		X	X
Civilian reserve air fleet		X	X
USPS certified mail			X
USPS First Class Mail			X
Commercial carriers providing Constant Surveillance Service (CSS)			X
Custody of U.S. citizen masters of U.S. registered ships			X

Alternative or additional methods of transmission approved by the head of the DoD Component			X

4. Hand Carrying / Escort Procedures

As a security professional, there may be times when you or one of the activity personnel you support, are asked to carry classified documents to someplace outside your building. In this lesson, we are going to discuss the policies for hand carrying classified information.

When hand carrying is used in reference to classified information, it doesn't refer to a designated courier, but rather an appropriately cleared U.S. government or contract employee who has been briefed on the process of hand carrying official documents. In addition, these cleared individuals are personally transporting classified information for which he or she has a need-to-know.

Hand carrying classified information should only be done as a last resort. An appropriate official must be the one to determine the need for hand carrying classified information. If the answers to the following two questions are no, then hand carrying information may be necessary. First, are the materials already available at the destination? And second, can the materials be transmitted to the destination in time by another authorized method?

Written authorization is always required before someone can hand carry classified information. There are different types of authorization based on the type of transportation being utilized. Written statements authorizing hand carry transmission should include identifying information regarding the hand carrier, authorized geographic location for hand carry transport, authorized level of hand carrying authority, etc. This authorization statement may be included in official travel orders.

If you are traveling on a commercial airline, a letter of authorization is required. If you are using any other mode of transportation, a written statement authorizing such transmission, or DD Form 2501, Courier Authorization, is required. A DD Form 2501 is a Courier Authorization card. This card is used to identify appropriately cleared DoD military and civilian personnel who have been approved to hand carry classified information. In this case, need-to-know is satisfied by virtue of the officially assigned duty to escort classified information, although the individual may not otherwise require access to the information.

a. Hand Carrying Procedures

Individuals who hand carry classified information must be informed of and acknowledge their security responsibilities. This is usually satisfied by a briefing or by requiring the individual to read written instructions that contain the following information:

- The carrier is liable and responsible for the material being escorted.
- Classified material is not, under any circumstances, to be left unattended. During overnight stops, U.S. military facilities, embassies,

or cleared U.S. contractor facilities must be used. Classified material cannot be stored in hotel safes.

- Material cannot be opened en route except when situations arise with customs, police, and/or immigration officials of various countries whose border the carrier may cross. There is no assurance of immunity from search by the customs, police, and/or immigration officials; therefore, should such officials inquire into the contents, the carrier shall present their courier orders and ask to speak to the senior customs, police and/or immigration official; this action should normally suffice to pass the material through unopened. However, if the senior official demands to see the actual contents of the package, it may be opened in his or her presence, but should be done in an area out of sight of the general public.
- Classified material is not to be discussed or disclosed in any public place.
- The carrier should not deviate from the authorized travel schedule.
- In cases of emergency, the carrier must take measures to protect the classified material.
- The carrier is responsible for ensuring that personal travel documentation (passport, courier authorization, medical documents, etc.) are complete, valid, and current.

The material being carried must be double wrapped. If carrying a briefcase, it can act as the outer wrapping as long as the briefcase is locked. You may receive additional information on this topic from the DSS Transmission and Transportation for DoD online course.

b. Hand Carrying Procedures on Aircraft

Occasionally it's necessary for a hand carrier to use airline travel in order to transport classified information. There are numerous requirements that cover transporting classified information aboard aircraft. While this course will not cover all of them, some of the noteworthy requirements and procedures are listed here:

- If it is necessary to travel by airline, all airlines involved should be U.S. carriers. If a U.S. carrier is unavailable then a foreign carrier may be used.
- The hand carrier must have a DoD or contractor-issued identification card that includes a photograph, descriptive data, and a signature of the individual. If date of birth, height, weight, and signature are not on ID card, include in authorization letter.
- The hand carrier must have a letter of authorization authorizing that person control of the classified information.
- Advance coordination should be made with airline and departure terminal officials and, when possible, with intermediate transfer terminals to develop mutually satisfactory arrangements within the

terms of DoD requirements, Department of Homeland Security (DHS) requirements, and Federal Aviation Administration (FAA) guidance, to facilitate the hand carrier's processing through airline ticketing, screening, and boarding procedures.

- Classified packages that are being carried on an airline should not have any metal bindings on them so as not to attract attention or be mistaken for contraband when going through x-ray machines.

Being responsible for classified information is a task that must be taken very seriously. If the time comes that you have to carry classified information outside the building, please be very cautious and careful. Be aware of your surroundings as well as all of the precautions that must be adhered to that we discussed during this lesson. If the information you are transporting gets into the wrong hands, it could cause considerable damage to our national security.

Review Activity 4

Complete the following review activities. When you are finished, see the Answer Key at the end of this Student Guide to check your answers. Check whether the statement describes an inner or outer envelope.

	Inner Envelope	Outer Envelope
Envelope is conspicuously marked Secret.	☐	☐
Envelope contains no markings or notations indicating its contents are classified.	☐	☐

Select the best answer to the following questions:

1. When the document has been sealed within a properly marked inner envelope you must:
   - ☐ Prepare the documents to be faxed
   - ☐ Call the courier for pick-up
   - ☐ Insert the envelope into the outer envelope
   - ☐ All of the above

2. DCS stands for:
   - ☐ Defense Candy Service
   - ☐ Department of case standards
   - ☐ Defense Courier Service

3. Secret information can be sent via USPS express main when:
   - ☐ Federal Express is not available
   - ☐ Only when it is the most effective means considering security, time, cost, and accountability
   - ☐ When the document is addressed to an APO address

4. Top Secret information can be sent via USPS when:
   - ☐ DCS are not available
   - ☐ It needs to be signed for
   - ☐ Never

5. Confidential information can be sent via DCS, First Class mail, registered mail and:
   - ☐ pony express
   - ☐ certified mail
   - ☐ military escort

Decide whether the following statements are True or False.

		True	False
Hand carrying classified information should only be done as a last resort		○	○
Anyone can determine the need for hand carrying classified information.		○	○
When someone is carrying classified information, written authorization is always required.		○	○
A DD Form 2501 is a Courier Authorization Card that provides authorization for you to transport classified material within the U.S. and its territories.		○	○
Classified information may NEVER be opened en route.		○	○

Disposition and Destruction

1. Overview

The next section covers the disposition and destruction of classified materials. Sometimes we hang on to classified information a little longer than we need. These reasons include the fact that we are unaware that the item may be disposed of, we think we may need the item in the future, we believe the destruction process is inconvenient, or we don't know how to destroy the information. In addition, we may think we can use the items to justify manning. Or possibly our workplace does not have an established program to dispose of classified material.

Everyone who works in a secure environment is responsible for making sure classified information is always handled correctly, from the time it is originated, to the time it is destroyed. As stated previously, the compromise of classified information can be devastating to our national security, even the compromise of those classified materials awaiting destruction. You are going to learn how to manage records, including historical ones. You will also learn about the procedures for the destruction of classified material and the approved methods for destruction.

2. Destruction Methods and Equipment

Classified items must be destroyed in a way that ensures that the classified information can't be recognized or reconstructed. There are several authorized methods for destruction including burning, shredding, pulverizing, disintegrating, pulping, melting, chemical decomposition, and mutilation to preclude recognition. Whatever destruction method you use, it should not harm or injure anyone.

Just as there are approved methods of destroying classified documents and materials, the actual destruction needs to take place on approved equipment in order to complete the destruction process. The National Security Agency maintains listings of evaluated destruction and degaussing products that have been tested and meet performance requirements. All new shredders procured by the DoD must come from the NSA/CSS Evaluated Products List, or EPL, for High Security Crosscut Paper Shredders.

Next you will learn about the different methods for destroying paper-based products and other materials that contain classified information.

3. Document Destruction

Destroying classified paper-based material is the most common type of classified destruction within the DoD. More frequently shredders are being used as the preferred destruction equipment. They are relatively inexpensive compared to an incinerator, and they are convenient. DoD follows the standards set by the National Security Agency. The current specification requires shredders to have crosscut capability to cut the material into confetti-like bits, not just into long strips, as well as the capability to cut the material into 1mm by 5mm pieces.

You should follow three procedures when using a shredder:

1. Remove all staples and paper clips from the documents. These materials will nick the shredder blades and eventually cause the shredder to "go out of spec."

2. It is highly recommended that you use the secure volume concept which is to shred 20 or more pages at the same time. The greater the volume of the bits produced, the lower the chance that the classified information can be reconstructed.

3. Check the insides of the shredder after you use it. Larger pieces may get stuck on the sides or they may slip through.

Other methods of destruction for paper-based classified documents are: burning, pulverizing, disintegrating, pulping, chemical decomposition, and mutilation to preclude recognition. Whatever process is used to destroy classified information should produce a residue from which classified information cannot be gleaned.

4. Material Destruction

Classified information resides on a variety of material other than paper. Just like paper-based classified material, these non-paper-based items must be properly destroyed when they are no longer required. Certain material can present problems in the destruction process because of their composition. Let's look at different types of material and see how they are destroyed.

Microforms and microfiche may be burned if you have an incinerator designed to handle the toxic emissions created by the items. These materials may also be shredded, but the plastic-like substance can cause the shredder to jam. It is difficult to shred the classified information beyond discerning since it is imprinted on tiny areas that may not always be destroyed even by an authorized crosscut shredder. An alternative method is to use chemicals to decompose the imprints.

Typewriter ribbons can be burned. Prior to placing the ribbon and cartridge into the furnace, you should take the ribbon out of the cartridge and cut it up into several pieces. An alternative method of destruction is to shred the ribbon.

Videotapes can be burned or demagnetized, also known as degaussing. Before you degauss your videotape, you should first check with the NSA for information on suitable equipment to complete this process. If you decide to record unclassified information over classified information, treat the videotape as classified until it is physically destroyed. If you burn your videotapes, you must ensure that the destruction equipment can safely handle any toxic emissions that could occur.

Floppy disks can be destroyed a few different ways to include burning, degaussing, or overwriting. When burning floppy disks, you should be careful of the toxic emission that could be present. When degaussing or overwriting, you

should check with your component headquarters or the NSA to ensure you are using the approved methods.

Compact and digital video disks are considered optical media devices. The NSA has a list of established destruction methods for these devices.

Destruction of any other storage media to include thumb drives or zip disks should be coordinated with your local information systems personnel and must conform to the applicable DoD and Component guidance. Refer to the NSA/CSS Storage Device Declassification Manual for additional information on IS storage devices. Be safe and security conscious at the same time.

5. Summary

The destruction of all classified information to include paper-based and other materials is a very serious matter. If the material is not properly disposed of then the information could be reconstructed by an individual who intends to the use the compromised information in a way that causes damage to our national security. As a member of the cleared community, you should always be aware of your surroundings to include classified information. You have an important responsibility for properly safeguarding classified information until it is properly destroyed.

Review Activity 5

Select the appropriate method or methods for the destruction of the items listed below. When you are finished, see the Answer Key at the end of this Student Guide to check your answers.

Item	Incinerator	Shredder	Computer	Degausser
Microfiche *Microfiche must be burned or shredded to be destroyed. It can also be destroyed with chemicals that destroy the imprints.*	☐	☐	☐	☐
Typewriter ribbon *Typewriter ribbons must be burned or shredded.*	☐	☐	☐	☐
Floppy disk *Floppy disks must be burned, overwritten, or demagnetized.*	☐	☐	☐	☐
Document *Documents must be burned, shredded, or chemically decomposed of.*	☐	☐	☐	☐
Videotape *Videotapes must be burned, shredded, or demagnetized.*	☐	☐	☐	☐

Handling Special Types of Information

1. Overview

In this topic, you will learn about some of the most common special types of information and control notices. As a security professional you may have access to many different types of documents. It is imperative that you know how to decipher between not only the classification markings, but also other special markings and control notices.

2. Atomic Energy Information (RD/FRD)

Atomic Energy Information includes documents that have control markings such as Restricted Data and Formerly Restricted Data. These documents are marked per a directive from the Atomic Energy Act of 1954, as amended. These documents shall be stored, protected, and destroyed as required by the DoD Information Security Program Manual.

3. Sensitive Compartmented Information (SCI)

SCI stands for Sensitive Compartmented Information. This is classified information concerned with or derived from intelligence sources, methods, or analytical processes, that is required to be handled within formal access control systems established by the Director of National Intelligence.

4. Communications Security (COMSEC)

COMSEC stands for Communications Security. COMSEC is the protection resulting from all measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications. COMSEC includes cryptosecurity, emission security, transmission security, and physical security of COMSEC material and information.

5. Special Access Programs (SAP)

Special Access Programs, or SAPs, are established in accordance with DoDM 5200.01, DoD Information Security Program. SAPs are created only when absolutely necessary to protect the nation’s most sensitive and critical information or when required by statutes. Establishment must be consistent with law, policy, and regulations, and be based on a determination that the threat and/or vulnerability, for example, sensitivity or value of the information, warrants enhanced protection.

Any DoD program or activity employing enhanced security measures exceeding those normally required for information at the same classification level must be established, approved, and managed as a DoD SAP. Examples of such enhanced security measures include: use of any special terminology, including code words, other than an unclassified nickname, to identify or control information dissemination; personnel security investigative or adjudicative requirements more stringent than those required for a comparable level of classified information; specialized non-disclosure agreements;

exclusion of a classified contract (use of a carve-out), or; a central billet system to control the number of personnel authorized access. DoD SAPs may only be approved by the Secretary of Defense or the Deputy Secretary of Defense.

6. North Atlantic Treaty Organization (NATO)

The North Atlantic Treaty Organization, or NATO, is an alliance of 28 countries from North America and Europe, committed to fulfilling the goals of the North Atlantic Treaty signed on April 4, 1949. The United States is a member of NATO, and as such, has access to NATO classified documents. NATO classified information, or documents prepared by or for NATO, and NATO member nation documents that have been released into the NATO security system, and that bear a NATO classification marking, needs to be safeguarded and marked in compliance with United States Security Authority for NATO, or USSAN.

7. Patent Secrecy Act of 1952

The Patent Secrecy Act of 1952 states that the Secretary of Defense, among others, may determine that disclosure of an invention by granting of a patent would be detrimental to national security. As a result of this determination, the information may be subjected to secrecy orders.

8. Foreign Government and Specialized Treaty Information

Due to their sensitivity and potential impact on our national security, Foreign Government and Specialized Treaty Information may require special safeguarding and dissemination controls.

9. FOIA / FOUO (FOIA Exemptions)

DoD policy is to conduct its activities in an open manner and provide the public with a maximum amount of accurate and timely information concerning its activities, consistent with the legitimate public and private interests of the American people. While openness in government is a DoD goal, we also have to ensure that the information made available to the public is consistent with the need for security, and adherence to other requirements of law and regulation.

The Freedom of Information Act, or FOIA, recognizes the need to withhold certain types of information from public release and, therefore, establishes the guidance and framework for evaluating information for release to the public. The FOIA provides that, for information to be exempt from mandatory release, it must first fit into one of nine qualifying categories and there must be a legitimate Government purpose served by withholding it.

For Official Use Only, or FOUO, is a designation that is applied to unclassified information that may be exempt from mandatory release to the public under the FOIA. Simply because information is marked FOUO does not mean it automatically qualifies for exemption. If a request for a record is received, the information must be reviewed to see if it meets the dual test. On the other hand, the absence of the FOUO marking does not automatically mean the information must be released. Some types of records, for

example, personnel records, are not normally marked FOUO, but may still qualify for withholding.

Information that has been determined for FOUO status should be indicated by markings when the information is included in documents and similar material beginning at the time documents are drafted, whenever possible, to promote proper protection of the information.

FOUO information may be disseminated within the DoD Components, and between officials of the DoD Components and DoD contractors, consultants, and grantees as necessary in the conduct of official business. FOUO information may also be released to officials in other Departments and Agencies of the Executive and Judicial Branches in performance of a valid Government function. Special restrictions may apply to information covered by the Privacy Act.

The following table lists FOIA exemption categories:

FOIA Exemptions:	
Exemption 1	Information that is currently and properly classified.
Exemption 2	Information that pertains solely to the internal rules and practices of the Agency. (This exemption has two profiles, "high" and "low." The "high" profile permits withholding of a document that, if released, would allow circumvention of an Agency rule, policy, or statute, thereby impeding the agency in the conduct of its mission. DoD Components shall not invoke the low profile.)
Exemption 3	Information specifically exempted by a statute establishing particular criteria for withholding. The language of the statute must clearly state that the information will not be disclosed.
Exemption 4	Information such as trade secrets and commercial or financial information obtained from a company on a privileged or confidential basis that, if released, would result in competitive harm to the company, impair the Government's ability to obtain like information in the future, or protect the Government's interest in compliance with program effectiveness.
Exemption 5	Inter-Agency memoranda that are deliberative in nature; this exemption is appropriate for internal documents that are part of the decision making process and contain subjective evaluations, opinions and recommendations.
Exemption 6	Information, the release of which could reasonably be expected to constitute a clearly unwarranted invasion of the personal privacy of individuals.
Exemption 7	Records or information compiled for law enforcement purposes that: • Could reasonably be expected to interfere with law enforcement proceedings; • Would deprive a person of a right to a fair trial or impartial adjudication; • Could reasonably be expected to constitute an unwarranted invasion of the personal privacy of others; • Disclose the identity of a confidential source; • Disclose investigative techniques and procedures; or • Could reasonably be expected to endanger the life or physical safety of any individual.
Exemption 8	Certain records of Agencies responsible for supervision of financial institutions.

Exemption 9	Geological and geophysical information concerning wells.

10. Intelligence Information

In addition to Executive Order 13526, classified intelligence information is also protected under provisions of the National Security Act of 1947, as amended, and Executive Order 12333. As a result, the Director of National Intelligence, or DNI, establishes the policies, controls, and procedures for the dissemination and use of intelligence information.

11. DoD Scientific and Technical Information Program (STIP)

STIP stands for the DoD Scientific and Technical Information Program. STIP is not actually a control marking, but rather a program that implements distribution control statements on scientific and technical information.

STIP was established to improve and enhance the acquisition of data sources to prevent redundant research to disseminate technical information efficiently to prevent the loss of technical information to U.S. adversaries and competitors and last, but no less important, STIP was established to aid the transfer of technical information to qualified researchers in U.S industry and government agencies.

Answer Key

Review Activity 1

1. The people who are in possession of, or who are otherwise charged with safeguarding classified information.
   - ☒ Custodians
   - ☐ Handlers
   - ☐ Escorts
   - ☐ Officers

2. Which agency is responsible for approving security containers for the storage of classified material?
   - ☐ GAO
   - ☒ GSA
   - ☐ NGA
   - ☐ SGA

3. What is the basic formula for granting access to classified information for individuals?
   - ☐ Verify the individual's clearance eligibility
   - ☐ Determine the individual's need-to-know
   - ☐ Acknowledge that the SF 312 has been completed
   - ☒ All of the above

4. What practices should be followed when handling classified information in the workplace?
   - ☐ Properly destroy preliminary drafts, worksheets, and other material after they have served their purpose
   - ☐ Use approved secure communications circuits for telephone conversations to discuss classified information
   - ☐ Follow proper procedures when copying classified information
   - ☐ Be sure to use security forms, such as the SF 701 and SF 702
   - ☒ All of the above

Review Activity 2

Group 1:

A. Unauthorized disclosure

B. Security violation

C. Security infraction

1. ___B_____ occurs when there is a knowing, willful, or negligent action that could reasonably be expected to result in an unauthorized disclosure of classified information; action to classify or continue the classification of information contrary to the requirements of E. O. 12958, as amended, or its implementing directives; or, action to create or continue a special access program contrary to E. O. 12958, as amended.
2. ____C____ occurs as the knowing, willful, or negligent action that contradicts E. O. 12958, as amended, or its implementing directives that does not comprise a violation.
3. ___A_____ is a communication or physical transfer of classified information to an unauthorized recipient.

Group 2:

A. Actual compromise

B. Neither confirm nor deny

C. Potential compromise

1. ____A____ an unauthorized disclosure of classified information
2. ___C_____ the possibility of compromise could exist but it is not known with certainty
3. ___B_____ if classified information appears in the public media, DoD personnel must be careful not to make any statement or comment that would confirm the accuracy or verify the classified status of the information

Review Activity 3

Fax Facts:

Always verify that the receiver has the proper clearance eligibility and need-to-know to handle the material.	☑
Once the materials are faxed, you no longer have custodial responsibilities for the information.	☐
DISA, Joint Interoperability Test Command (JITC) maintains a register of certified secure digital facsimiles.	☑

COMSEC Facts:

Common COMSEC approved telephones include the SME-111 and the ISS.	☐
COMSEC information is subject to special transmission procedures found in the National Telecommunications and Information Systems Security Instruction 4001.	☑
COMSEC is the protection resulting from the measures designed to deny unauthorized persons information of value that might be derived from the possession and study of telecommunications and to ensure the authenticity of such communications.	☑

Review Activity 4

Check whether the statement describes an inner or outer envelope.

	Inner Envelope	Outer Envelope
Envelope is conspicuously marked Secret.	☒	☐
Envelope contains no markings or notations indicating its contents are classified.	☐	☒

Select the best answer to the following questions:

1. When the document has been sealed within a properly marked inner envelope you must:

- ☐ Prepare the documents to be faxed
- ☐ Call the courier for pick-up
- ☒ Insert the envelope into the outer envelope
- ☐ All of the above

2. DCS stands for:

- ☐ Defense Candy Service
- ☐ Department of case standards
- ☒ Defense Courier Service

3. Secret information can be sent via USPS express main when:
   - ☐ Federal Express is not available
   - ☒ Only when it is the most effective means considering security, time, cost, and accountability
   - ☐ When the document is addressed to an APO address

4. Top Secret information can be sent via USPS when:
   - ☐ DCS are not available
   - ☐ It needs to be signed for
   - ☒ Never

5. Confidential information can be sent via DCS, First Class mail, registered mail and:
   - ☐ pony express
   - ☒ certified mail
   - ☐ military escort

Decide whether the following statements are True or False.

		True	False
Hand carrying classified information should only be done as a last resort. *True. Hand carrying classified information should only be done as a last resort because it puts the information at a higher level of risk than other means of transmission or transportation.*		●	○
Anyone can determine the need for hand carrying classified information. *False. An appropriate official must be the one to determine that hand carrying classified information is necessary.*		○	●
When someone is carrying classified information, written authorization is always required. *True. Written authorization is always required before someone can hand carry classified information. If you are traveling on a commercial airline, a latter of authorization is required. If you are using any other mode of transportation, a written statement authorizing such transmission, or a DD Form 2501 "Courier Authorization" is required.*		●	○
A DD Form 2501 is a Courier Authorization Card that provides authorization for you to transport classified material within the U.S. and its territories. *False. Geographic limitations are determined by the authority issuing the card. Note: Rules governing hand carrying classified information aboard commercial passenger aircraft require an authorization letter in lieu of a DD Form 2501.*		○	●
Classified information may NEVER be opened en route. *False. The material cannot be opened en route except when situations arise with customs, police, and/or immigration officials of various countries whose border the carrier may cross. There is no assurance of immunity from search by the customs, police, and/or immigration officials; therefore, should such officials inquire into the contents, the carrier shall present the courier orders and ask to speak to the senior customs, police and/or immigration official; this action should normally suffice to pass the material through unopened. However, if the senior official demands to see the actual contents of the package, it may be opened in his or her presence, but should be done in an area out of sight of the general public.*		○	●

Review Activity 5

Item	Incinerator	Shredder	Computer	Degausser
Microfiche *Microfiche must be burned or shredded to be destroyed. It can also be destroyed with chemicals that destroy the imprints.*	☑	☑	☐	☐
Typewriter ribbon *Typewriter ribbons must be burned or shredded.*	☑	☑	☐	☐
Floppy disk *Floppy disks must be burned, overwritten, or demagnetized.*	☑	☐	☑	☑
Document *Documents must be burned, shredded, or chemically decomposed of.*	☑	☑	☐	☐
Videotape *Videotapes must be burned, shredded, or demagnetized.*	☑	☑	☐	☑

Lesson 5: Briefings

Lesson Introduction

As a security professional, you will see your share of security related briefings and may even be responsible at some point for giving security briefings to other individuals. This lesson will provide you with an introduction to 10 of the most common security briefings used within the DoD that you may encounter. Each of these briefings are designed to enhance security education and awareness, and ultimately to protect our national security.

Common Security Briefings

1. Initial Orientation Briefings

All personnel in the organization, including DoD civilians, military members, and on-site support contractors shall receive an initial orientation to the DoD Information Security Program. Before any personnel are allowed access to any classified information, they must be briefed on various aspects of the information security program. This initial orientation is intended to: define classified information and Controlled Unclassified Information, or CUI, and explain the importance of protecting such information; provide a basic understanding of security policies and principles; notify personnel of their responsibilities within the security program, and inform them of the administrative, civil, and/or criminal sanctions that can be applied when appropriate; provide individuals enough information to ensure the proper protection of classified information and CUI in their possession, including actions to be taken if such information is discovered unsecured, a security vulnerability is noted, or a person has been seeking unauthorized access to such information; and inform personnel of the need for review of ALL unclassified DoD information prior to its release to the public.

In the initial orientation or in the training required by DoDM 5200.01, Volume 3, educators should include who the DoD Component senior agency official and activity security management personnel are, a description of their responsibilities, and whether they are involved in the protection of classified or controlled unclassified information.

2. Indoctrination Briefings

Briefings provided for all cleared personnel are referred to as initial orientation briefings, but they are also called indoctrination briefings by some activities. Indoctrination briefings can also refer to the briefings provided to individuals who are authorized access to special types of classified information. We will focus on this aspect.

Much like accessing collateral classified information, accessing Special Compartmented Information, or SCI, or any Special Access Program, or SAP, information, you must receive an indoctrination briefing. This briefing provides information about how to protect the classified information within these special programs, and how to determine to whom you can disclose this information.

3. Annual Refresher Briefings

Cleared personnel are required to receive annual refresher briefings that reinforce the policies, principles, and procedures covered during the initial orientation or indoctrination briefings, as well as any specialized briefings. The refresher briefings also address the threat and techniques employed by foreign intelligence activities who are attempting to obtain classified information. During refresher briefings, personnel are reminded of the penalties for engaging in espionage activities. Additionally, refresher briefings provide a great opportunity to address local security issues or concerns. These may include issues identified during organizational self-inspections, common issues that resulted in security violations, or recent or upcoming changes to local security procedures.

Each Original Classification Authority, or OCA, is required to receive annual training as specified in section 5, enclosure 5 of DoD Manual 5200.01, Volume 3. The OCA must certify receipt of the training in writing. For OCAs who do not receive the specified training at least once within a calendar year, the DoD Component Head or the senior agency official who delegated the authority will suspend their classification until the training has taken place, unless a waiver is granted.

Derivative classifiers, or those who create now classified documents, including emails, based on existing classification guidance, must receive training in derivative classification with an emphasis on avoiding over-classification, as required by paragraph 3.c. of this enclosure.

Training may, at the DoD Component's discretion, be included in the training required by paragraph 7.a. of this section. Derivative classifiers who do not receive training at least once every 2 years will not be authorized or allowed to derivatively classify information until they have received training, unless a waiver is granted.

As you can see, Refresher Briefings are a valuable education and awareness tool, used to remind cleared personnel of their continued security responsibilities, and ensure they are aware of security threats they may face.

4. Debriefings / Termination Briefings

Debriefings are also known as Termination Briefings. When a cleared person no longer needs access to classified information, they will receive a debriefing. This briefing emphasizes an individual's continued responsibility to protect classified information to which they have had access. They are also provided instructions for reporting any unauthorized attempt to gain access to such information. The person leaving is also advised on the prohibition against retaining material once they depart the organization. In addition, retired personnel, former DoD employees, and non-active duty members of the Reserve Components must submit their writings and other materials intended for public release to the DoD security review process. Perhaps most importantly, they are reminded of the potential civil and criminal penalties for the failure to fulfill their continuing security responsibilities.

5. Courier Briefings

Courier briefings are provided to cleared personnel who will be escorting, hand carrying, or serving as a courier for classified material. During this briefing, the individual will be informed of procedures for handling classified information while in transit. They will also be informed about points of contact in case of an emergency while performing courier responsibilities.

6. NATO Briefings

Now, we are going to learn about the special NATO briefing. NATO briefings are only provided to personnel who have a validated need to work with NATO classified information. Access to NATO classified information requires a final security clearance at the same level as the NATO information that you are required to access. The one exception to this rule is that you do not need a security clearance to access information designated as NATO RESTRICTED.

Government employees, as well as military personnel, will be given a NATO briefing by their security manager or their security manager's designee. The NATO briefing will cover security requirements for handling classified NATO information and the consequences of negligent handling of this information. Annual refresher briefings will be conducted to reinforce the importance of proper handling and protection of classified NATO information.

When access to NATO information is no longer required a debriefing is conducted. The debriefing covers the individual's continued responsibility for safeguarding classified NATO information. This briefing does not have to be in a specific format. It can be accomplished by requiring the person to read a document or listen to a presentation, and then sign their name to verify they understand their continued responsibilities.

7. Non-Disclosure Briefings

The next special type of briefing we will learn about is the Non-Disclosure Briefing. In some organizations, this briefing means the same thing as the Initial Orientation Briefing or the Indoctrination Briefing. But for most DoD organizations this briefing refers to something else. Specifically, this briefing is provided to individuals who have had unauthorized access to classified information.

Determining when this special briefing should be given is based on several factors which include the individual's clearance status and their need-to-know. If a situation warrants this briefing then the recipient of the briefing will be advised of their responsibility to prevent further dissemination of the information and of the administrative sanctions and criminal penalties that might follow if they fail to do so. The debriefing in this situation will be designed to ensure that the individual who has had unauthorized access understands what classified information is, why its protection is important, and knows what to do should someone try to obtain the information from them.

8. Foreign Travel Briefings

Another type of special security briefing you may encounter is the Foreign Travel Briefing. Foreign travel briefings are provided to personnel who will be traveling to foreign countries. This briefing is usually required for all personnel with SCI or SAP access. Cleared personnel who are traveling to areas where there are concerns about possible foreign intelligence exploitation are also required to receive a foreign travel briefing. Lastly, this briefing is required for cleared personnel who will be attending professional meetings or conferences where foreign attendance is likely. Check with your component, agency, or local requirements to determine your specific foreign travel briefing policies.

Foreign Travel Briefings provide important information, not only about the potential security risks at a given destination, but they also provide important information about points of contact if a problem arises. In addition to security warnings, the security travel briefings also provide valuable information about any applicable safety or criminal issues about which travelers should be aware.

9. Attestation Briefings

The Attestation briefing is for contractors who require indoctrination into a Special Access Program, or SAP. During this briefing, individuals have to orally attest to understanding their responsibility to protect national security information by reciting the following statement.

I accept the responsibilities associated with being granted access to classified national security information. I am aware of my obligation to protect classified national security information through proper safeguarding and limiting access to individuals with the proper security clearance and/or access and official need-to-know. I further understand that, in being granted access to classified SAP information, a special confidence and trust has been placed in me by the United States Government.

Immediately following this attestation all personnel will sign a document that applies to them and their work location. The document must be signed in the presence of a witness.

10. Antiterrorism/Force Protection (AT/FP) Briefings

The next briefing you are going to learn about is the Antiterrorism/Force Protection, or AT/FP, briefing. Several groups assisted the Chairman of the Joint Chiefs of Staff in establishing requirements and minimum standards for antiterrorism training. The standards that are currently in place address personnel responsible for managing antiterrorist training programs. They also address training requirements for individuals, commanders, senior executive officers, high risk personnel, those assigned to high risk billets, and units preparing to deploy.

There are four levels of training. Level one is for individual personal protection awareness. Level two is for unit antiterrorism advisors. Level three is a commander's course. And level four is an executive seminar.