**NONRESIDENT TRAINING COURSE**

**January 2000**


# Introduction to the Department of the Navy Information and Personnel Security Program

## NAVEDTRA 14210

**Although the words "he," "him," and "his" are used sparingly in this course to enhance communication, they are not intended to be gender driven or to affront or discriminate against anyone.**

# PREFACE

By enrolling in this self-study course, you have demonstrated a desire to improve yourself and the Navy. Remember, however, this self-study course is only one part of the total Navy training program. Practical experience, schools, selected reading, and your desire to succeed are also necessary to successfully round out a fully meaningful training program.

**TEXT**: The texts for this course, Department of the Navy Personnel Security Program Regulation, SECNAVINST 5510.30A, and Department of the Navy Information Security Program Regulation, SECNAVINST 5510.36, are NOT supplied and must be obtained by the student. Available at: http://neds.nebt.daps.mil

**COURSE OVERVIEW**: In completing this nonresident training course, you will demonstrate a knowledge of the subject matter by correctly answering questions on the following subjects:

(Assignments 1-5*) The Department of the Navy Personnel Security Program Regulation*, SECNAVINST 5510.30A: basic program policy and authorities, command security management, counterintelligence matters, security education, national security positions, personnel security investigations and determinations, clearance, access to classified information, continuous evaluation and visitor access to classified information.

(Assignments 6-11) *Department of the Navy Information Security Program Regulation*, SECNAVINST 5510.36: introduction to the information security program, command security management, security education, classification management, security classification guides, marking; safeguarding, storage and destruction, dissemination, transmission and transportation, loss or compromise of classified information, and industrial security program.

**THE COURSE**: This self-study course is organized into subject matter areas, each containing learning objectives to help you determine what you should learn along with text and illustrations to help you understand the information. The subject matter reflects day-to-day requirements and experiences of personnel in the rating or skill area. It also reflects guidance provided by Enlisted Community Managers (ECMs) and other senior personnel, technical references, instructions, etc., and either the occupational or naval standards, which are listed in the *Manual of Navy Enlisted Manpower Personnel Classifications and Occupational Standards*, NAVPERS 18068.

**THE QUESTIONS**: The questions that appear in this course are designed to help you understand the material in the text.

**VALUE**: In completing this course, you will improve your military and professional knowledge. Importantly, it can also help you study for the Navy-wide advancement in rate examination. If you are studying and discover a reference in the text to another publication for further information, look it up.

*2000 Edition*

Published by
NAVAL EDUCATION AND TRAINING
PROFESSIONAL DEVELOPMENT
AND TECHNOLOGY CENTER

**NAVSUP Logistics Tracking Number**
**0504-LP-026-8550**

## Sailor's Creed

"I am a United States Sailor.

I will support and defend the Constitution of the United States of America and I will obey the orders of those appointed over me.

I represent the fighting spirit of the Navy and those who have gone before me to defend freedom and democracy around the world.

I proudly serve my country's Navy combat team with honor, courage and commitment.

I am committed to excellence and the fair treatment of all."

# INSTRUCTIONS FOR TAKING THE COURSE

## ASSIGNMENTS

The text pages that you are to study are listed at the beginning of each assignment. Study these pages carefully before attempting to answer the questions. Pay close attention to tables and illustrations and read the learning objectives. The learning objectives state what you should be able to do after studying the material. Answering the questions correctly helps you accomplish the objectives.

## SELECTING YOUR ANSWERS

Read each question carefully, then select the BEST answer. You may refer freely to the text. The answers must be the result of your own work and decisions. You are prohibited from referring to or copying the answers of others and from giving answers to anyone else taking the course.

## SUBMITTING YOUR ASSIGNMENTS

To have your assignments graded, you must be enrolled in the course with the Nonresident Training Course Administration Branch at the Naval Education and Training Professional Development and Technology Center (NETPDTC). Following enrollment, there are two ways of having your assignments graded: (1) use the Internet to submit your assignments as you complete them, or (2) send all the assignments at one time by mail to NETPDTC.

**Grading on the Internet:** Advantages to Internet grading are:

- you may submit your answers as soon as you complete an assignment, and
- you get your results faster; usually by the next working day (approximately 24 hours).

In addition to receiving grade results for each assignment, you will receive course completion confirmation once you have completed all the assignments. To submit your assignment answers via the Internet, go to:

**http://courses.cnet.navy.mil**

**Grading by Mail:** When you submit answer sheets by mail, send all of your assignments at one time. Do NOT submit individual answer sheets for grading. Mail all of your assignments in an envelope, which you either provide yourself or obtain from your nearest Educational Services Officer (ESO). Submit answer sheets to:

COMMANDING OFFICER
NETPDTC N331
6490 SAUFLEY FIELD ROAD
PENSACOLA FL 32559-5000

**Answer Sheets:** All courses include one "scannable" answer sheet for each assignment. These answer sheets are preprinted with your SSN, name, assignment number, and course number. Explanations for completing the answer sheets are on the answer sheet.

**Do not use answer sheet reproductions:** Use only the original answer sheets that we provide—reproductions will not work with our scanning equipment and cannot be processed.

Follow the instructions for marking your answers on the answer sheet. Be sure that blocks 1, 2, and 3 are filled in correctly. This information is necessary for your course to be properly processed and for you to receive credit for your work.

## COMPLETION TIME

Courses must be completed within 12 months from the date of enrollment. This includes time required to resubmit failed assignments.

## PASS/FAIL ASSIGNMENT PROCEDURES

If your overall course score is 3.2 or higher, you will pass the course and will not be required to resubmit assignments. Once your assignments have been graded you will receive course completion confirmation.

If you receive less than a 3.2 on any assignment and your overall course score is below 3.2, you will be given the opportunity to resubmit failed assignments. **You may resubmit failed assignments only once.** Internet students will receive notification when they have failed an assignment--they may then resubmit failed assignments on the web site. Internet students may view and print results for failed assignments from the web site. Students who submit by mail will receive a failing result letter and a new answer sheet for resubmission of each failed assignment.

## COMPLETION CONFIRMATION

After successfully completing this course, you will receive a letter of completion.

## ERRATA

Errata are used to correct minor errors or delete obsolete information in a course. Errata may also be used to provide instructions to the student. If a course has an errata, it will be included as the first page(s) after the front cover. Errata for all courses can be accessed and viewed/downloaded at:

**http://www.advancement.cnet.navy.mil**

## STUDENT FEEDBACK QUESTIONS

We value your suggestions, questions, and criticisms on our courses. If you would like to communicate with us regarding this course, we encourage you, if possible, to use e-mail. If you write or fax, please use a copy of the Student Comment form that follows this page.

**For subject matter questions:**

E-mail: n311.products@cnet.navy.mil
Phone: Comm: (850) 452-1355
DSN: 922-1355
FAX: (850) 452-1370
(Do not fax answer sheets.)
Address: COMMANDING OFFICER
NETPDTC N311
6490 SAUFLEY FIELD ROAD
PENSACOLA FL 32509-5237

**For enrollment, shipping, grading, or completion letter questions**

E-mail: fleetservices@cnet.navy.mil
Phone: Toll Free: 877-264-8583
Comm: (850) 452-1511/1181/1859
DSN: 922-1511/1181/1859
FAX: (850) 452-1370
(Do not fax answer sheets.)
Address: COMMANDING OFFICER
NETPDTC N331
6490 SAUFLEY FIELD ROAD
PENSACOLA FL 32559-5000

## NAVAL RESERVE RETIREMENT CREDIT

If you are a member of the Naval Reserve, you may earn retirement points for successfully completing this course, if authorized under current directives governing retirement of Naval Reserve personnel. For Naval Reserve retirement, this course is divided into two units evaluated at 17 points: 12 points upon satisfactory completion of unit 1, assignments 1 through 8; and 5 points upon satisfactory completion of unit 2, assignments 9 through 11. (Refer to *Administrative Procedures for Naval Reservists on Inactive Duty,* BUPERSINST 1001.39, for more information about retirement points.)

# Student Comments

**Course Title:** *Introduction to the Department of the Navy Information and Personnel Security Program*

**NAVEDTRA:** 14210 **Date**: _____

**We need some information about you**:

Rate/Rank and Name: _____ SSN: _____ Command/Unit _____

Street Address: _____ City: _____ State/FPO: _____ Zip _____

**Your comments, suggestions, etc**.:

**Privacy Act Statement:** Under authority of Title 5, USC 301, information regarding your military status is requested in processing your comments and in preparing a reply. This information will not be divulged without written authorization to anyone other than those within DOD for official use in determining performance.

NETPDTC 1550/41 (Rev 4-00

# ASSIGNMENT 1

Textbook Assignment: ***Department of the Navy Personnel Security Program Regulation,* SECNAVINST 5510.30A**, "Basic Program Policy and Authorities," chapter 1, pages 1-1 through 1-8; "Command Security Management," chapter 2, pages 2-1 through 2-7; "Counterintelligence Matters," chapter 3, pages 3-1 through 3-3; "Security Education," chapter 4, pages 4-1 through 4A-1; and "National Security Positions," chapter 5, pages 5-1 through 5A-1.

---

***LEARNING OBJECTIVE*: *Describe the Navy Personnel Security Program policy and identify responsibilities of designated authorities*.**

1-1. Which of the following is a purpose for establishing the Navy Personnel Security Program?

1. To authorize initial and continued access to classified information
2. To authorize initial and continued assignment to sensitive duties
3. To ensure that no final unfavorable personnel security determination will be made without compliance with all procedural requirements
4. All of the above

1-2. For the Department of the Navy, who is ultimately responsible for ensuring that there is an effective Personnel Security Program and that it complies with all directives issued by higher authority?

1. Secretary of Defense
2. Secretary of the Navy
3. Chief of Naval Operations
4. Director of Naval Intelligence

1-3. Which of the following National Authorities for Security Matters is responsible for oversight and implementation of E.O. 10450 which prescribes security requirements for federal government employment?

1. Attorney General of the United States
2. Secretary of the Navy
3. Federal Bureau of Investigation
4. Office of Personnel Management

1-4. Which Department of Defense agency conducts personnel security investigations for the DoD and also administers the National Industrial Security Program?

1. National Security Agency
2. Defense Security Service
3. Security Research Center
4. Defense Intelligence Agency

1-5. What official is responsible to the SECNAV for establishing, directing and overseeing an effective Department of the Navy (DON) Personnel Security Program (PSP)?

1. Chief of Naval Operations (N09N)
2. Chief of Naval Personnel
3. Director, DON Central Adjudication Facility (CAF)
4. Commander, Naval Security Group

1-6. Which of the following statements concerning special programs is NOT correct?

1. Require additional security protection
2. May require special reporting procedures or formal access lists
3. May require additional handling measures
4. Must be authorized by DoD in accordance with DoD Directive 0-5205.7

1-7. Which of the following statements concerning Special Access Programs (SAPs) is/are correct?

1. Require security measures in addition to those requirements for the protection of Top Secret, Secret or Confidential classified information
2. Are authorized by the Secretary of Defense or Deputy Secretary of Defense
3. Are governed by DoD Directive 0-5205.7
4. All of the above

1-8. Within the Navy, what is the controlling regulation for implementation and maintenance of the Personnel Security Program?

1. OPNAVINST 5520.2E
2. SECNAVINST 5510.30A
3. OPNAVINST 5510.1H
4. OPNAVNOTE 5510 Series

1-9. Which of the following individuals are responsible for compliance with the Personnel Security Regulation?

1. Navy and Marine Corps members
2. Civilians employed by the Navy
3. Commanding officers
4. All of the above

1-10. When a commanding officer seeks permission to waive a personnel security requirement, the request for waiver must be submitted to what official?

1. Secretary of the Navy
2. Chief of Naval Operations (N09N2)
3. Commander, Naval Intelligence Command
4. Commander, Naval Personnel Command

1-11. The title "commanding officer" as used in SECNAVINST 5510.30A may be interpreted as including which of the following individuals?

1. Officer in charge of a naval activity
2. Commander of a naval vessel
3. Head of any naval organizational activity
4. All of the above

1-12. If your command has difficulty interpreting SECNAVINST 5510.30A, a request for guidance or clarification should be sent to what official?

1. Chief of Naval Education and Training
2. Deputy Chief of Naval Operations (CNO (N89))
3. Chief of Naval Operations (N09N2)
4. Director, Department of the Navy Central Adjudication Facility

1-13. Who is responsible for the security and administration of the Sensitive Compartmented Information program for the cryptologic community?

1. Director, Department of the Navy Central Adjudication Facility
2. Commander, Naval Security Group Command
3. Director, Navy International Programs Office
4. Deputy Chief of Naval Operations (CN0 (N89))

***LEARNING OBJECTIVE***: *Identify the key officials involved in command security management and describe their duties.*

1-14. Which of the following commands must appoint a security manager in writing?

1. Commands handling Top Secret material only
2. Commands handling Top Secret and Secret materials only
3. Any command eligible to receive classified information
4. Commands handling Critical Nuclear Weapon Design Information (CNWDI) only

1-15. At the command level who is ultimately responsible for compliance with and implementation of the DON Information and Personnel Security Program?

1. The security officer
2. The executive officer
3. The administrative officer
4. The commanding officer

1-16. Which of the following functions is/are the responsibility of the security manager?

1. Coordinates the command program for continuous evaluation of eligibility for access to classified information or assignment to sensitive duties
2. Ensures all personnel execute a Classified Information Nondisclosure Agreement (SF 312) prior to granting initial access to classified information
3. Maintains liaison with the command Special Security Officer (SSO) concerning information and personnel security policies and procedures
4. All of the above

1-17. Which of the following statements does NOT accurately reflect security manager requirements?

1. Must be designated in writing
2. Must relieve the commanding officer of his/her responsibility for the command's information and personnel security program
3. Must have a favorably adjudicated SSBI completed within the previous 5 years
4. Must be a U. S. citizen

1-18. Which of the following requirements must be met by individuals before they can be considered eligible to serve as an assistant security manager?

1. Must be an officer, warrant officer, or U.S. civilian employee GS-9 or above
2. Must be proven reliable and of mature judgment as determined by an investigative board convened by the command
3. Must be subjected to a National Agency Check (NAC)
4. Must be a U.S. citizen and designated in writing

1-19. Who within a command is responsible to the commanding officer for the implementation of the command's INFOSEC program?

1. The Contracting Officer's Representative (COR)
2. The Special Security Officer (SSO)
3. The Top Secret Control Officer (TSCO)
4. The Information Systems Security Manager (ISSM)

1-20. The SSO has which of the following functions?

1. Serves as the principal advisor in the command on the Sensitive Compartmented Information security program
2. Is responsible for the operation of the Sensitive Compartmented Information Facility (SCIF)
3. Must cooperate and coordinate with the command security manager
4. All of the above

1-21. Security Servicing Agreements (SSAs) will be specific and must clearly define where the security responsibilities of each participant begin and end. The SSA will include requirements for advising the commanding officer of any matters which may directly affect the security posture of the command.

1. True
2. False

***LEARNING OBJECTIVE***: *Identify reporting responsibilities related to counterintelligence matters and describe the requirements of the command security education program.*

1-22. Which of the following matters must always be reported to the Director, Naval Criminal Investigative Service (DIRNCIS)?

1. Sabotage, espionage, international terrorism or deliberate compromise
2. Foreign connections
3. Both 1 and 2 above
4. Foreign travel

1-23. A command security education program must accomplish which of the following goals?

1. Familiarize personnel with the security requirements for their particular assignments and identify restrictions
2. Familiarize personnel with procedures for challenging classification decisions
3. Advise personnel of the adverse effects to the national security which could result from unauthorized disclosure of classified information and of their personal, moral and legal responsibility to protect classified information within their knowledge, possession or control
4. All of the above

1-24. Which of the following requirements should be included in a security education program?

1. Indoctrination of personnel upon employment by the DON in the basic principles of security
2. Orientation of personnel who will have access to classified information at the time of assignment regarding command security requirements
3. Annual refresher briefings for personnel who have access to classified information
4. All of the above

1-25. Counterintelligence briefings must be given once every two years.

1. True
2. False

1-26. Which of the following will be given as soon as possible to an individual who reports to a command for duties that involve access to classified information?

1. Orientation briefing
2. On-the-job training
3. Indoctrination briefing
4. Refresher briefing

1-27. Whenever security policies or procedures change, personnel whose duties would be impacted by these changes must be briefed as soon as possible.

1. True
2. False

1-28. What type of briefing will be given annually to personnel who have access to classified information?

1. Orientation
2. New requirements
3. Refresher
4. Indoctrination

1-29. A command debriefing will be given to individuals who no longer require access to classified information due to which of the following situations?

1. Transfer from one command to another
2. Terminating active military service or civilian employment
3. Expiration of a Limited Access Authorization (LAA)
4. All of the above

1-30. As part of the command debriefing, individuals will be required to read the provisions of the Espionage act and other criminal statutes. If individuals are retiring from active service and will be entitled to receive retirement pay, they must be advised that they remain subject to the Uniform Code of Military Justice (UCMJ).

1. True
2. False

1-31. A Security Termination Statement need NOT be signed if an individual is transferring from one command to another and will continue to require access to classified information.

1. True
2. False

1-32. Which of the following statements apply(ies) to Security Termination Statements?

1. Must be witnessed
2. Must be executed by senior officials (flag and general officers, ES-1 and above, Senior Executive Service and equivalent positions)
3. Both 1 and 2 above
4. Must be filed in the command security folder

***LEARNING OBJECTIVE***: *Identify National Security Positions and describe the suitability determination process used for applicants and appointees to these positions.*

1-33. Which of the following statements apply to National Security Positions?

1. They must be assigned a position sensitivity level
2. The commanding officer is responsible for designating National Security Positions
3. There are three levels of National Security Positions
4. All of the above

1-34. Which of the following statements does NOT accurately describe a Critical-Sensitive Position?

1. Fiduciary, public contact, or other duties demanding the highest degree of public trust
2. Under DCID 1/14 authority
3. Category I AIS
4. Access to Top Secret information

1-35. Which of the following statements do/does NOT accurately reflect a Noncritical-Sensitive Position?

1. Access to Confidential information
2. Duties involving education and orientation of DoD personnel
3. Both 1 and 2 above
4. Investigative duties

1-36. What official is responsible for maintaining a record of position designation decisions?

1. The commanding officer
2. The security manager
3. The personnel officer
4. The top secret control officer

1-37. What Government entity has been charged with establishing the program for investigating and adjudicating the suitability of government applicants for and appointees to the Federal civil service?

1. U.S. Investigative Service
2. Defense Security Service
3. National Security Agency
4. Office of Personnel Management

1-38. Personnel security investigations are conducted to gather information for two purposes: to meet OPM requirements for accomplishing employment suitability determinations and to satisfy requirements for security determinations.

1. True
2. False

1-39. Security determinations are made before suitability determinations.

1. True
2. False

1-40. Personnel security determinations are based on criteria found in what regulation?

1. SECNAVINST 5510.30A
2. SECNAVINST 5510.35
3. SECNAVINST 5510.36
4. OPNAVINST 5510.1H

1-41. Investigations completed for non-sensitive positions are forwarded to the command for the suitability determination.

1. True
2. False

1-42. Which of the following statements concerning investigations for sensitive positions is NOT correct?

1. A favorable security determination on a "No Actionable Issue" case from OPM will include an automatic favorable suitability determination
2. The Department of the Navy Central Adjudication Facility (DON CAF) will make a suitability determination on "No Action Issue" cases
3. Cases with "Actionable Issues" are forwarded to the requesting command for the suitability determination
4. The DON CAF will make suitability determinations on cases with "Actionable issues"

1-43. The DON CAF will adjudicate investigations on non-U.S. citizens occupying sensitive positions.

1. True
2. False

1-44. Which of the following statements apply(ies) to assignment of non-U.S. citizens to sensitive positions?

1. Non-U.S. citizens cannot be appointed to a civilian Federal service position without approval from OPM
2. OPM's approval of a non-U.S. citizen to a federal service appointment does not authorize assignment to sensitive duties or access to classified information
3. If the position for which OPM's approval is sought is a sensitive position, CNO (N09N2) must first approve it to insure that assignment or access would not be prohibited or restricted
4. All of the above

1-45. Sensitive positions are either Special-Sensitive, Critical-Sensitive, or Noncritical- Sensitive.

1. True
2. False

1-46. Which of the following statements is/are NOT applicable to suitability determinations?

1. DON CAF adjudicates all investigations for suitability determinations.
2. The DON CAF has been delegated the authority to make de facto suitability determinations only on investigations closed without actionable issues
3. An unfavorable suitability determination made by the command requires no DON CAF action
4. Both 2 and 3 above

1-47. Suitability adjudications are normally a command responsibility and are based on standards and criteria established by OPM and contained in Title 5 CFR 731.

1. True
2. False

1-48. Which of the following statements pertain(s) to personnel security determinations?

1. The focus is whether the employment of the individual can reasonably be expected to promote the efficiency of the Federal Service
2. Security determinations are based on criteria found in SECNAVINST 5510.30A
3. The focus is whether the assignment of the individual can reasonably be expected to be clearly consistent with the nation's security interests
4. Both 2 and 3 above

1-49. An individual hired under emergency appointment procedures may not be considered for assignment to sensitive duties.

1. True
2. False

1-50. Security determinations are based on criteria found in SECNAVINST 5510.30A and are in most cases adjudicated by the DON CAF.

1. True
2. False

# ASSIGNMENT 2

Textbook Assignment: ***Department of the Navy Personnel Security Program Regulation,* SECNAVINST 5510.30A,** "Personnel Security Investigations," chapter 6, pages 6-1 through 6C-1; and "Personnel Security Determinations," chapter 7, pages 7-1 through 7-15.

---

***LEARNING OBJECTIVE***: *Identify the types of personnel security investigations and investigative procedures and requirements for personnel security clearances.*

2-1. Which of the following pertain(s) to Personnel Security Investigations (PSIs)?

1. Conducted on individuals who will be given access to classified information
2. Conducted on individuals who will be assigned sensitive duties
3. Both 1 and 2 above
4. Conducted on individuals transferring to another command

2-2. Which of the following officials is/are authorized to request PSIs on individuals under their jurisdiction?

1. Commanding officers of organizations and activities listed on the Standard Navy Distribution List and Marine Corps List of Activities
2. Director, DON Central Adjudication Facility (CAF)
3. Chiefs of recruiting stations
4. All of the above

2-3. The sole purpose of a personnel security investigation is to prevent unqualified applicants from being accepted for employment within the Department of the Navy.

1. True
2. False

2-4. Which of the following statements describe(s) personnel security investigative policy?

1. Only the minimum investigation to satisfy a requirement will be requested
2. The investigation requested and conducted will be commensurate with the level of sensitivity of the access required or the position occupied
3. CNO (N09N2) must give prior approval to establish investigative requirements in addition to, or at variance with, those established in SECNAVINST 5510.30A
4. All of the above

2-5. The Defense Security Service (DSS) and the U.S. Investigative Service (USIS) conduct all PSIs for the DON within the Continental United States.

1. True
2. False

2-6. Which of the following investigations, if any, is conducted by USIS and meets the minimum investigative requirements for appointment to a non-critical sensitive position with access to classified information?

1. ENTNAC
2. ANACI
3. SSBI
4. None of the above

2-7. What investigation is conducted to support Top Secret clearance and SCI access eligibility determinations?

1. SSBI
2. NACI
3. NAC
4. CPR

2-8. An NAC includes a search of the DCII, FBI files and files of other appropriate government agencies.

1. True
2. False

2-9. Which of the following investigative elements is/are included in a PR for continued Top Secret access?

1. NAC
2. Subject interview
3. Ex-spouse interview
4. All of the above

2-10. A reinvestigation updates a previous investigation and is authorized only for specific duties and access.

1. True
2. False

2-11. Of the following investigations, which is conducted to resolve personnel security issues which arise after a PSI is conducted, evaluated or adjudicated?

1. SPR
2. NACI
3. SSBI
4. SII

2-12. Under what circumstances is a prenomination interview conducted?

1. Before nomination for SCI access
2. Before granting TS access
3. Before requesting a PSI
4. Both 2 and 3 above

2-13. Only U.S. citizens are eligible for security clearance.

1. True
2. False

2-14. Which of the following is the minimum investigative basis for Secret or Confidential clearance eligibility determinations?

1. NACLC
2. ANACI
3. Either 1 or 2 above, depending upon military or civilian status
4. ENTNAC

2-15. Deleted

2-16. A new investigation is required upon reentry of officers and enlisted members if there has been a break in active service of over 24 months.

1. True
2. False

2-17. Which of the following investigations, if any, is required for a civilian employee who requires access to information classified Secret in performance of duties?

1. ANACI
2. NACI
3. NAC
4. None of the above

2-18. With the exception of loyalty reasons, who within the Navy and Marine Corps has authority to deny acceptance and retention in the DON?

1. CHNAVPERS and CMC
2. DON CAF
3. CNO (N09N2)
4. Both 2 and 3 above

2-19. For the purpose of partial or full mobilization under provisions of Title 10, U.S.C. (Title 14 pertaining to the U.S. Coast Guard as an element of the DON), the requirement for a NAC upon reentry may be waived.

1. True
2. False

2-20. Deleted

2-21. Emergency appointees may NOT be considered for positions requiring access to classified information.

1. True
2. False

2-22. Which of the following governs the management of the investigative requirements for DON contractor personnel?

1. DISCR
2. DSS
3. NISP
4. FAD

2-23. Which of the following is the minimum investigative requirement for assignment as a security manager?

1. ANACI
2. NAC
3. SPR within 10 years
4. SSBI or PR within 5 years

2-24. Deleted

2-25. Contract guards require a favorably adjudicated SSBI.

1. True
2. False

2-26. Which of the following is the governing regulation for the Personnel Reliability Program (PRP)?

1. SECNAVINST 5510.35
2. SECNAVINST 5510.30A
3. SECNAVINST 5510.36
4. OPNAVINST 5510.162

2-27. Which of the following programs has/have Special Investigative Requirements?

1. SIOP-ESI
2. NATO
3. PSA
4. All of the above

2-28. Investigations will not be duplicated when a previously conducted investigation meets the scope and standards for the level required.

1. True
2. False

2-29. Reciprocity requires that Federal Government agencies accept each other's investigations and consequent favorable personnel security determinations without re-adjudication. Under what circumstances is reciprocity NOT appropriate or necessary?

1. Potentially disqualifying information is developed since the last favorable adjudication
2. The individual is being considered for a higher level clearance eligibility
3. The most recent clearance or access authorization was conditional or based on a waiver
4. All of the above

2-30. Before requesting an investigation, activities must determine that the individual does NOT have an investigation which satisfies the requirements.

1. True
2. False

2-31. Requests for PSIs will NOT normally be submitted on any civilian or military personnel who will be retired, resigned, or separated with less than nine months of service remaining.

1. True
2. False

2-32. Prior personnel security investigations may only be requested by commands for review in support of an official requirement. All requests for prior investigations must be fully justified and forwarded to which of the following?

1. DON CAF
2. Naval Criminal Investigative Service
3. Defense Security Service
4. Bureau of Naval Personnel

2-33. Which of the following functions is/are command responsibility(ies) performed in conjunction with personnel security investigation requests?

1. Verification of prior investigation
2. Local records check
3. Verification of date and place of birth
4. All of the above

2-34. Commands are required to validate the citizenship of individuals prior to submitting a request for a PSI.

1. True
2. False

2-35. What type of investigation is required for DON civilian employees in non-critical sensitive positions and those who will require access to Confidential and Secret classified information?

1. ANACI
2. ENTNAC
3. SSBI
4. SII

2-36. What type of investigation is required to support trustworthiness determinations?

1. SPR
2. NAC
3. SSBI
4. NACLC

2-37. What type of investigation is required to support security and suitability determinations for civilian employees and military members requiring access to Top Secret and/or SCI and assignment to special-sensitive and/or critical-sensitive positions?

1. SII
2. PR
3. SSBI
4. NAC

2-38. An individual who refuses to provide relevant information for investigative purposes may be considered eligible for access to classified information.

1. True
2. False

2-39. When an investigation is in a pending status and the subject is released from active duty, discharged, resigns, or circumstances change and the investigation is no longer required, the command must notify what agency?

1. NCIS
2. DSS
3. BUPERS
4. DON CAF

2-40. When the investigation request is rejected by the investigative agency because the request package was not properly completed, commands must take corrective action immediately and resubmit the request.

1. True
2. False

2-41. Commands must submit tracer requests regarding overdue DSS investigations to DON CAF.

1. True
2. False

2-42. Commands may obtain the status of DSS investigations by calling DSS customer service.

1. True
2. False

2-43. Where are all PSIs conducted for DON activities forwarded to upon completion?

1. Requesting activity
2. NCIS
3. DON CAF
4. BUPERS

2-44. Investigations requested to support trustworthiness determinations and non-sensitive positions are NOT adjudicated by the DON CAF.

1. True
2. False

2-45. Reports of investigation may only be shown or released to the subject of the investigation.

1. True
2. False

***LEARNING OBJECTIVE***: *Recognize the basic policy and procedures for personnel security determinations and identify personnel security program authorities and their responsibilities.*

2-46. What Executive Orders establish the standards for personnel security determinations?

1. E.O. 11690 and E.O. 10450
2. E.O. 10450 and E.O. 12968
3. E.O. 10450 and E.O 12958
4. E.O. 12958 and E.O. 12968

2-47. Who is responsible for ensuring the security information in the military personnel database is accurately updated from the DON CAF database and reported to commands via the EDVR and ODCR?

1. Director, NCIS
2. CNO (N09N2)
3. Chief, NAVPERS
4. DSS

2-48. Who is responsible for ensuring the security information in the Defense Civilian Personnel Data System (DCPDS) is accurately updated from the DON CAF database and reported to commands?

1. Chief, NAVPERS
2. CNO (N09N2)
3. SECNAV
4. DASN (CP/EEO)

2-49. What command documents personnel security determinations in the Navy Joint Adjudication and Clearance System (NJACS) and the Defense Clearance and Investigations Index (DCII)?

1. DON CAF
2. CNO (N09N2)
3. DSS
4. NAVPERS

2-50. Commanding officers are responsible for granting interim personnel security clearances.

1. True
2. False

2-51. Commanding officers will maintain a personnel security record on all assigned personnel, to include records of briefings, clearance determinations, and access determinations.

1. True
2. False

2-52. Which of the following situations require(s) a personnel security determination?

1. Access to classified information or assignment to sensitive duties is necessary under interim conditions
2. Questionable or unfavorable information becomes available about an individual in a sensitive position or a position requiring access to classified information
3. A personnel security investigation on a nominee for a security clearance or assignment to sensitive duties has been completed
4. All of the above

2-53. Trustworthiness NACs will be requested using the SF 85P, forwarded to DSS for investigation and adjudicated by the DON CAF.

1. True
2. False

2-54. The DON Facility Access Determination (FAD) Program applies to contractor employees and was established to support commanding officers in their responsibilities under the Internal Security Act of 1950 to protect persons and property under their command against the actions of untrustworthy persons.

1. True
2. False

2-55. The DON CAF issues a Letter of Intent (LOI) to revoke or deny which of the following eligibilities?

1. Security clearance
2. Assignment to a sensitive position
3. Access to Sensitive Compartmented Information
4. All of the above

2-56. The recipient of a Letter of Intent from the DON CAF has what maximum number of calendar days to respond in writing?

1. 15
2. 30
3. 45
4. 90

2-57. The ultimate appellate authority for unfavorable DON CAF personnel security determinations is what entity?

1. CNO (N09N2)
2. DOHA
3. DON CAF
4. PSAB

2-58. A personal appearance before an administrative judge of the Defense Office of Hearing and Appeals (DOHA) must be requested within what maximum number of days after receipt of a Letter of Notification?

1. 10
2. 15
3. 30
4. 45

2-59. Written appeals to the PSAB must be submitted within what maximum number of days after receipt of a Letter of Notification?

1. 15
2. 30
3. 60
4. 90

# ASSIGNMENT 3

Textbook Assignment: ***Department of the Navy Personnel Security Program Regulation*, SECNAVINST 5510.30A,** "Clearance," chapter 8, pages 8-1 through 8A-3.

---

***LEARNING OBJECTIVE***: *Describe the security clearance adjudication process guidelines and identify responsibilities and requirements for granting, recording, withdrawing, denying, and revoking security clearances.*

3-1. What agency is designated by the Secretary of the Navy as the single clearance granting authority for the Department of the Navy?

1. OPM
2. SECNAV Security
3. DON CAF
4. CNO (N09N2)

3-2. Once issued, a security clearance remains valid provided the cleared individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months.

1. True
2. False

3-3. Which of the following issues will the DON CAF adjudicator consider when making a security clearance determination?

1. Loyalty
2. Reliability
3. Trustworthiness
4. All of the above

3-4. Security clearance eligibility is established by DON CAF at the highest level supportable by the prerequisite security investigation.

1. True
2. False

3-5. A security clearance is initially issued upon adjudication of the prerequisite security investigation. When is it reestablished?

1. With each transfer
2. After adjudication of each subsequent investigation
3. Whenever an individual's rating changes
4. Annually

3-6. Security clearance determinations will be mutually and reciprocally accepted by the DON when made by which of the following Federal agencies?

1. Department of Agriculture
2. Department of Transportation
3. Central Intelligence Agency
4. All of the above

3-7. In order to mutually and reciprocally accept another Federal Government agency's clearance determination, which of the following conditions must be met?

1. There has not been a break in continuous service greater than 24 months.
2. The investigative basis is adequate for the clearance granted
3. There has been no new derogatory information
4. All of the above

3-8. Revocation of security clearance eligibility may be reciprocally accepted by agencies of the Federal Government.

1. True
2. False

3-9. For security clearance eligibility purposes, continuous service applies to which of the following conditions?

1. Active duty military service or active status in military reserve or Individual Ready Reserves (IRR)
2. Active status in the National Guard or NROTC
3. Civilian employment in the Federal Government
4. All of the above

3-10. For security clearance eligibility purposes, continuous service terminates when an individual transfers to a new command and no longer requires a security clearance.

1. True
2. False

3-11. Retired status qualifies as continuous service for security clearance purposes.

1. True
2. False

3-12. A DoD security clearance is invalid for access to DOE Restricted Data.

1. True
2. False

3-13. For security clearance purposes, U.S. citizens can be defined as those born in the U.S., those who are U.S. nationals, those who have derived U.S. citizenship or those who acquire it through naturalization.

1. True
2. False

3-14. Citizens of the Federated States of Micronesia (FSM) and the Republic of the Marshall Islands are NOT U.S. citizens.

1. True
2. False

3-15. The Facility Access Determination program may be used for trustworthiness determinations for contractor personnel when no access to classified information is required.

1. True
2. False

3-16. Security clearance will NOT be granted for which of the following individuals?

1. Civilians in non-sensitive positions
2. Persons such as guards and emergency service personnel, maintenance, food services, and cleaning personnel
3. Vendors and other commercial sales or service personnel
4. All of the above

3-17. Elected members of Congress who require access to classified information in the performance of their duties will be processed for security clearance eligibility.

1. True
2. False

3-18. Congressional staff members are granted security clearance, as necessary, by what Federal entity?

1. WHS
2. DON CAF
3. The White House
4. Congress

3-19. State governors are not processed for security clearance eligibility. CO's may grant them access to specifically designated classified information, on a need to know basis, when approved by CNO (N09N2).

1. True
2. False

3-20. Staff personnel of the governor's office who require access to DON classified information are granted a security clearance by the DON CAF.

1. True
2. False

3-21. Members of the Supreme Court, the Federal judiciary and the Supreme Courts of the individual states are NOT processed for security clearance eligibility. They may, nonetheless, be granted access to classified information to the extent necessary to adjudicate cases.

1. True
2. False

3-22. The Navy Joint Adjudication and Clearance System (NJACS) is the official repository for DON personnel security determination records and includes which of the following data elements?

1. Clearance determination
2. Initial access
3. Personnel security investigative
4. All of the above

3-23. The DON CAF security clearance determination certification must be maintained in the individual's local service record or official personnel file until the individual transfers.

1. True
2. False

3-24. Once issued, the DON CAF clearance certification remains valid provided the individual continues compliance with personnel security standards and has no subsequent break in service exceeding 24 months.

1. True
2. False

3-25. Copies of the DON CAF certification may NOT be maintained in the local personnel security file.

1. True
2. False

3-26. The EDVR, ODCR, MCTFS, or the DCPDS are sources of NJACS data which may be used temporarily to support local access determinations when the DON CAF security clearance certification is not found in the individual's service record or OPF, pending receipt of a replacement certification.

1. True
2. False

3-27. Commands with DCII access may NOT use DCII data records in lieu of the DON CAF certification records to support local access determinations.

1. True
2. False

3-28. The CO may issue an interim Secret/Confidential clearance as long as there is a favorable review of local records, a favorable review of the PSI request questionnaire and submission of the PSI request to the appropriate investigative agency.

1. True
2. False

3-29. The CO may issue an interim Top Secret clearance as long as the investigative paperwork for a Single Scope Background Investigation has been submitted to DSS.

1. True
2. False

3-30. Which of the following forms will be used by the CO or his/her designee to record interim security clearance determinations?

1. OPNAV 5510/413
2. OPNAV 5520/20
3. OPNAV 5510/21
4. SF 710

3-31. At what point after granting an interim security clearance is follow-up action necessary?

1. 30 days
2. 90 days
3. 120 days
4. 180 days

3-32. The interim clearance may not be continued in excess of one year without confirmation from the DON CAF that the investigation contains no disqualifying information.

1. True
2. False

3-33. When the command receives a Letter of Intent ( LOI) to deny security clearance of an individual who has been granted interim clearance, it must withdraw interim clearance and suspend any associated access.

1. True
2. False

3-34. Every commanding officer must have a favorably adjudicated SSBI whether or not access to classified information is required.

1. True
2. False

3-35. Navy and Marine Corps reserve personnel in an "active status" are considered to have continuous service and may be granted access to classified information as necessary and supportable.

1. True
2. False

3-36. To maintain mobility and operational readiness, the Chief of Naval Personnel or Headquarters Marine Corps may require individuals in specified ratings/MOS to have security clearance eligibility established by DON CAF to support assignments.

1. True
2. False

3-37. A consultant hired by a Government Contracting Activity (GCA) who will only require access to classified information at the GCA activity or in connection with authorized visits to the GCA is adjudicated for security clearance by which of the following agencies?

1. NISP
2. DISCO
3. The employing GCA
4. DON CAF

3-38. Contractors may grant Confidential clearances to qualified employees.

1. True
2. False

3-39. Commanding officers are required to report to the Defense Security Service (DSS) Operations Center Columbus (OCC) any adverse information which comes to their attention concerning a cleared contractor employee assigned to a worksite under their control. What other office must be advised of the adverse information?

1. DSS Operating Location Office identified on the DD Form 254
2. NISP Program Office
3. CNO (N09N2)
4. Command security manager

3-40. What must a command do when a member's duties change to no longer require access to classified information?

1. Debrief the member
2. Execute a Security Termination Statement
3. Notify the DON CAF that clearance and access are no longer required
4. All of the above

3-41. The command suspends access on an individual that the command received derogatory information on and provides a report of suspension to the DON CAF. After receiving additional information, the command determines that the individual's access should be restored immediately. The command may grant the access.

1. True
2. False

3-42. Transfer in Status (TIS) is a process by which an individual may be transferred from one DoD component, command or activity to another DoD component, command or activity in an SCI indoctrinated status.

1. True
2. False

3-43. Once the DON CAF grants a security clearance, it remains valid provided which of the following factors have been met?

1. The individual continues compliance with personnel security standards
2. The individual has no break in service exceeding 24 months
3. Both 1 and 2 above
4. The individual does not transfer to another command

3-44. Interim security clearances and/or access, and assignment to sensitive civilian positions is NOT authorized for individuals who have received an unfavorable security determination until the DON CAF reestablishes the security clearance.

1. True
2. False

3-45. After DON CAF makes an unfavorable decision concerning the individual's security clearance, commands must remove all access. However, in cases when the command determines it is necessary, an individual may maintain access until final appeal procedures are exhausted.

1. True
2. False

3-46. Which of the following statements pertaining to security clearance is true?

1. Non-U.S. citizens are eligible for security clearances.
2. Naturalized U.S. citizens may not be considered for Limited Access Authorization
3. Non-U.S. citizens are not eligible for security clearances
4. U. S. citizens born in communist countries are not eligible for security clearances

3-47. Commands are ultimately responsible for ensuring that the DON CAF is apprised when an individual fails to comply with personnel security standards. To satisfy this requirement, commands must institute which of the following programs?

1. TIS program
2. Continuous evaluation program
3. SAP program
4. Security policy program

3-48. Contractor personnel security investigations are conducted by the Defense Security Service (DSS). Which office adjudicates the investigative results and establishes security clearance eligibility for contractor personnel?

1. DON CAF
2. WHS
3. DSS OCC
4. DoD

3-49. A Department of Energy "L" clearance is the same as a DoD Top Secret clearance.

1. True
2. False

3-50 An Interim Secret or Confidential security clearance for contractors may be granted by the command.

1. True
2. False

# ASSIGNMENT 4

Textbook Assignment: ***Department of the Navy Personnel Security Program Regulation,* SECNAVINST 5510.30A,** "Access To Classified Information," chapter 9, pages 9-1 through 9A-2.

---

***LEARNING OBJECTIVE***: *Recognize the basic policy and procedures governing access to classified information, including Sensitive Compartmented Information and Restricted Data.*

4-1. Access to classified information may be granted if allowing access will promote the DON mission while preserving the interests of national security.

1. True
2. False

4-2. The level of access to classified information authorized will NOT be limited to the minimum level required to perform assigned duties.

1. True
2. False

4-3. What form must be executed by all persons prior to gaining initial access to classified information?

1. OPNAV 5520/20
2. OPNAV 5510/413
3. SF 312
4. SF 86

4-4. Access to classified information will be limited to the minimum number of individuals necessary to accomplish the mission and will be based on the need to know.

1. True
2. False

4-5. Within the command, who has the ultimate authority over who may have access to classified information under command control?

1. Security manager
2. Special Security officer
3. Department head
4. Commanding officer

4-6. Commanding officers may grant access to classified information to any individual, provided the individual has met which of the following requirements?

1. Has an official need to know
2. Has an established security clearance
3. Is not the subject of unadjudicated disqualifying information
4. All of the above

4-7. For individuals who have NOT been determined eligible for security clearance, access authorization may be allowed in certain circumstances.

1. True
2. False

4-8. What is the DON regulation governing the Sensitive Compartmented Information program?

1. SECNAVINST 5510.36
2. NAVSUPP to DoD S5105.21.M-1
3. DCID 1/14
4. DoD 5200.2R

4-9. Limiting access to classified information is the responsibility of each individual possessing classified information. Before permitting others access to classified information, what determination must the possessor make?

1. Access is justified based on the person's security clearance eligibility
2. The date of the person's last investigation
3. Access is justified based on the person's security clearance and need to know
4. Access is justified based on the supervisor's approval

4-10. Who is delegated sole responsibility for granting, denying, revoking and verifying SCI access for DON personnel?

1. COMNAVSECGRU
2. SSO NAVY
3. Director, DON CAF
4. DNI

4-11. Who has the authority to adjudicate DON contractor personnel requiring SCI access eligibility?

1. DSS OCC
2. Director, DON CAF
3. NISP
4. SSO NAVY

4-12. Which of the following statements regarding SCI access is correct?

1. A valid requirement or certification of need to know must be established prior to requesting an adjudication of SCI access eligibility
2. A Single Scope Background Investigation request must be forwarded with an OPNAV 5510/413 requesting SCI access
3. SCI access, like security clearance eligibility, is a right, not a privilege
4. Before requesting SCI access, DCID 1/14 exception requirements will be prepared in accordance with SECNAVINST 5510.30A

4-13. What form is used to request SCI access?

1. OPNAV 5510/413
2. OPNAV 5520/20
3. DD 1879
4. SF 86

4-14. Upon favorable adjudication of the completed SSBI, DON CAF will forward a final clearance/SCI access eligibility certificate to the requesting command. The command will ensure the SSO receives a copy of the message or letter to indoctrinate the individual to SCI and the security manager will maintain a command record of the clearance and access granted.

1. True
2. False

4-15. Commanding officers are NOT responsible for establishing and administering a program for continuous evaluation of all personnel with SCI access eligibility.

1. True
2. False

4-16. Information that could potentially affect an individual's eligibility for SCI access must be reported to DON CAF.

1. True
2. False

4-17. Commanding officers may NOT suspend SCI access, as this is the sole perogative of the DON CAF.

1. True
2. False

4-18. The final review authority for appeals of SCI access eligibility determinations is delegated to which of the following entities?

1. SECNAV
2. DNI
3. PSAB
4. DON CAF

4-19. A Periodic Reinvestigation is NOT required every 5 years for continued SCI access eligibility.

1. True
2. False

4-20. What form must be executed by all personnel as a condition of access to classified information?

1. SF 86
2. SF 312
3. OPNAV 5520/20
4. OPNAV 5510/413

4-21. A new SF-312 must be executed every time an individual transfers and access requirements change.

1. True
2. False

4-22. Personnel who have signed other non-disclosure agreements for specific access (such as Form 1847-1, Sensitive Compartmented Information (SCI) Non-Disclosure Agreement) are NOT required to execute the SF 312.

1. True
2. False

4-23. If an individual refuses to sign an SF 312, what actions must be taken by the command?

1. Deny the individual access and report the refusal to DON CAF
2. Deny the individual access and report the refusal to CNO
3. Immediately contact the Director, NCIS by classified message
4. Document the individual's refusal and forward a copy to CNO (N09N2)

4-24. The SF 312 must be witnessed and the witnessing official must sign and date the SF 312 upon execution. The witnessing official can be any member of the command.

1. True
2. False

4-25. The executed SF 312 must be accepted on behalf of the U.S. The accepting official can be the CO, the XO, the Security Manager or any individual designated in writing by the CO to accept the SF-312 on behalf of the U.S.

1. True
2. False

4-26. Administrative withdrawal of clearance, after execution of an SF 312, and subsequent granting of clearance and access will NOT require re-execution of another SF 312.

1. True
2. False

4-27. What is the NJACS system?

1. Naval Joint Adverse Clarification System
2. Naval and Marine Corp Joint Adjudication Central System
3. Navy Joint Adjudication and Clearance System
4. Naval Justice Adjudication Central System

4-28. The DON CAF is responsible for maintaining a record of all access granted to include temporary accesses, special accesses or other program accesses.

1. True
2. False

4-29. Commands may use which of the following methods to record access determinations?

1. Computerized database
2. Log book
3. A form OPNAV 5520/20
4. All of the above

4-30. What information must be included in the command access record?

1. Name, SSN, citizenship verification
2. Date and level of access authorized
3. The basis for the access determination and the name, title, rank or grade of the individual authorizing the access
4. All of the above

4-31. Interim security clearances are recorded on the OPNAV 5510/413.

1. True
2. False

4-32. One-time access permits an individual access at a security classification level higher than that for which the individual is eligible.

1. True
2. False

4-33. Who may grant one-time access?

1. Flag officer
2. General officer
3. General courts-martial convening authority or equivalent Senior Executive Service member
4. All of the above

4-34. The individual granted one-time access must be a U.S. citizen, have a current DoD security clearance and have been continuously employed by DoD or a cleared DoD contractor for the preceding 24-month period.

1. True
2. False

4-35. One-time access may be granted to a part-time or temporary employee.

1. True
2. False

4-36. One-time access will expire after what maximum time period?

1. 2 weeks
2. 30 days
3. 180 days
4. 1 year

4-37. If the need for one-time access is to extend beyond 30 days, written approval is required from CNO (N09N2). If access will extend beyond 90 days, the command must initiate a request for the appropriate security clearance.

1. True
2. False

4-38. One-time access at the next higher level may be authorized for COMSEC, SCI, NATO, or foreign government information.

1. True
2. False

4-39. For what minimum period must access records be maintained after access is terminated?

1. 90 days
2. 1 year
3. 2 years
4. 5 years

4-40. Temporary access may NOT be granted to DON personnel who have been determined to be eligible for a security clearance, but do not currently require a security clearance to perform assigned duties.

1. True
. 2. False

4-41. There are clear indications that a new employee reporting for duty had a security clearance which meets the command's needs; however, there is no DON CAF message in his record. Which of the following statements, if any, is correct?

1. The command may not grant access but must submit an OPNAV 5510/413 indicating the level of clearance required, to the DON CAF
2. The command may grant temporary access and complete an OPNAV 5510/413 indicating the level of clearance required and submit it to the DON CAF
3. The command may grant access
4. None of the above

4-42. Commands with DCII access may NOT use DCII data in lieu of the DON CAF clearance certificate to grant access.

1. True
2. False

4-43. Retired personnel are entitled to have access to classified information by virtue of their present and/or former status.

1. True
2. False

4-44. Requests for access authorization for attorneys representing DON personnel will be submitted to CNO (N09N2) via which of the following activities?

1. General Services Administration
2. Joint Chiefs of Staff
3. Defense Security Service
4. Office of General Counsel or Navy Judge Advocate General

4-45. As an exception, access may be granted to a retired flag/general officer for compelling reasons by which of the following personnel?

1. CNO (N09N2)
2. An active duty flag or general officer
3. SSO
4. CO

4-46. Limited Access Authorizations may be granted for non-U.S. citizens by which of the following officials?

1. CNO (N09N2)
2. SSO
3. CO
4. All of the above

4-47. Individuals granted Limited Access Authorization are subject to a periodic reinvestigation at what minimum time interval?

1. Annually
2. Every 2 years
3. Every 5 years
4. Every 10 years

4-48. Requests for access to DON classified information by persons outside of the Executive Branch must be submitted to what agency?

1. DON CAF
2. CNO (N09N2)
3. DSS
4. OPM

4-49. When is it appropriate for a CO to administratively withdraw an individual's access?

1. A permanent change in rating/MOS negates the need for access
2. Upon retirement from military service
3. Upon termination of employment
4. All of the above

4-50. When the level of access required for an individual's official duties changes, the command will adjust the authorized access accordingly, provided the new requirement does not exceed the level allowed by the security clearance.

1. True
2. False

4-51. Within what maximum time period must commands report suspension of access to DON CAF?

1. 3 working days
2. 5 workings days
3. 10 working days
4. 2 weeks

4-52. Requests for access to RD not under the control of DoD or NASA will be made in accordance with what governing regulation?

1. DOEINST 5200.2R
2. SECNAVINST 5510.30A
3. DoD 5210.2
4. DCID 1/14

# ASSIGNMENT 5

Textbook Assignment: ***Department of the Navy Personnel Security Program Regulation,* SECNAVINST 5510.30A**,"Continuous Evaluation," chapter 10, pages 10-1 through 10A-2; "Visitor Access to Classified Information," chapter 11, pages 11-1 through 11-6; and Appendixes A through I, pages A-1 through I-4.

---

***LEARNING OBJECTIVE***: *Describe administrative requirements of the command continuous evaluation program.*

5-1. In order to ensure that everyone who has access to classified information remains eligible for a clearance, continuous assessment and evaluation is required.

1. True
2. False

5-2. Who within the command is responsible for establishing and administering a program for continuous evaluation?

1. Security Assistant
2. Security Officer
3. SSO
4. CO

5-3. The continuous evaluation program depends upon which of the following elements?

1. Individuals must be encouraged to report to their supervisor or appropriate security official any incident or situation which could affect their continued eligibility for access to classified information
2. Co-workers have an obligation to advise their supervisor or appropriate security official when they become aware of information with potential security clearance significance
3. Supervisors and managers play a critical role in assuring the success of the program
4. All of the above

5-4. The keys to an active continuous evaluation program are security education and positive reinforcement of reporting requirements.

1. True
2. False

5-5. For original classification authorities, security managers, security specialists, and all other personnel whose duties significantly involve the creating, handling, or management of classified information, which of the following statements apply(ies)?

1. Their performance contract or rating system must include the management of classified information as a critical element or item to be evaluated
2. Their supervisors will comment on their continued security clearance eligibility in conjunction with their performance appraisals
3. Both 1 and 2 above
4. They are required to be subjected to psychological evaluations

5-6. SECNAVINST 5510.30A, Appendix F, "Personnel Security Standards," identifies areas of security concern which must be reported to the DON CAF.

1. True
2. False

5-7. Before reporting information which meets standards contained in Appendix F to SECNAVINST 5510.30A, commands should consider the mitigating factors.

1. True
2. False

5-8. When reporting unfavorable information, commands may take which of the following actions?

1. Use exhibit 10A of SECNAVINST 5510.30A to ensure that the DON CAF has sufficient information
2. Suspend the individual's access for cause
3. Both 1 and 2 above
4. Revoke the individual's security clearance

5-9. Which of the following actions may be taken by the DON CAF upon receipt of a command report of locally developed unfavorable information?

1. Evaluate and adjudicate all reported information
2. Promptly notify commands of the determination regarding the individual's continued eligibility for security clearance and/or assignment to sensitive duties
3. Either request additional information from the command or request that the command forward the necessary investigative forms to open an investigation to resolve outstanding or missing information
4. All of the above

5-10. Which of the following security issues must be reported to the DON CAF?

1. Criminal conduct
2. Alcohol abuse
3. Misuse of Information Technology Systems
4. All of the above

***LEARNING OBJECTIVE***: *Describe the basic policy and procedures regarding visitor access to classified information*

5-11. For security purposes, a visitor on board a ship or aircraft is a person who is not a member of the ship's company or not a member of a staff using the ship as a flagship.

1. True
2. False

5-12. For security purposes, which of the following personnel are considered visitors?

1. Civilian employees permanently assigned to the command
2. Persons on temporary additional duty
3. Reservists on active duty for training
4. Both 2 and 3 above

5-13. Which of the following persons are NOT required to sign visitor records or display identification badges when being escorted as visitors?

1. DON contractors
2. Flag officers, general officers or their civilian equivalents
3. Non U. S. citizens
4. U. S. scientists

5-14. A cleared and properly trained military or civilian member or a contractor assigned to the command being visited may function as an escort for a visitor.

1. True
2. False

5-15. What information must be provided on a civilian or military employee visiting a DON command?

1. Purpose of visit
2. Date and duration of visit
3. Security clearance status
4. All of the above

5-16. Which of the following information is NOT required on a contractor employee visiting a DON command?

1. Name of person being visited
2. UIC/RUC
3. Date and place of birth
4. Certification of security clearance

5-17. Visit requests may be transmitted by facsimile, by message or electronically transmitted via electronic mail.

1. True
2. False

5-18. Which of the following statements pertain(s) to visit requests?

1. Under no circumstances will personnel handcarry their own visit requests to the places being visited
2. All visit requests will provide a certification of the visitors need to know in the form of an authorization signature by an official, other than the visitor, with command signature authority
3. Both 1 and 2 above
4. Requests must be submitted two weeks prior to visit

5-19. Which of the following regulations governs visits by foreign nationals and representatives of foreign entities?

1. DoD 5210.2
2. SECNAVINST 5510.34
3. SECNAVINST 5350.4C
4. SECNAVINST 5400.1

5-20. Members of Congress, by virtue of their elected status, do NOT require DoD security clearances.

1. True
2. False

5-21. Which of the following statements does NOT apply to visits by the GAO?

1. Written notice of visit request is not required
2. GAO personnel can be identified by serially numbered credential cards issued by the Comptroller General
3. Security clearance eligibility of visiting GAO personnel need not be verified
4. The DON GAO liaison office will provide telephonic visit authorization for GAO Headquarters and Washington Regional Office personnel whose clearances are on file with DoD

***LEARNING OBJECTIVE***: *Identify security terms and acronyms contained in SECNAVINST 5510.30A*

5-22. An adjudication decision to grant or continue a security clearance or SCI access despite a failure to meet adjudicative or investigative standards is known as an exception.

1. True
2. False

5-23. Issue information is any information that could NOT adversely affect a person's eligibility for access to classified information.

1. True
2. False

5-24. Which of the following acronyms is used for the Industrial Security Program?

1. ISSO
2. IRR
3. NISP
4. NACI

***LEARNING OBJECTIVE***: *Recognize guidelines for a command security instruction, the purpose of the Defense Clearance and Investigations Index (DCII), and the applicability of personnel security standards.*

5-25. Which of the following elements should be included in the command security instruction?

1. An identification of the command's security organization, including the chain of command
2. Security education program requirements
3. Assignment of responsibilities for continuous evaluation requirements
4. All of the above

5-26. The Defense Clearance and Investigations Index (DCII) is the single, automated central repository that identifies investigations conducted by DoD

1. True
2. False

5-27. Commands are NOT permitted access to the DCII.

1. True
2. False

5-28. Commands must report any behavior, incident, or allegation which falls under which of the following areas of security concern?

1. Sexual behavior that is criminal or reflects lack of judgement or discretion
2. Alcohol abuse
3. Unexplained affluence or excessive indebtedness
4. All of the above

***LEARNING OBJECTIVE***: *Recognize adjudication guidelines for personnel security determinations, including areas of concern; the structure and functions of the Personnel Security Appeals Board; and U.S. citizenship criteria.*

5-29. The adjudication guidelines found in SECNAVINST 5510.30A were established for all U.S. Government civilian and military personnel, consultants, contractors, employees of contractors and other individuals who require initial or continued access to classified information, access to SCI and/or employment or retention in sensitive duties.

1. True
2. False

5-30. Each adjudication is to be an overall common sense determination based upon which of the following criteria?

1. Consideration and assessment of all available information, both favorable and unfavorable
2. The nature, extent, and seriousness of the conduct
3. Both 1 and 2 above
4. Who reported the information.

5-31. The adjudicator will ensure the adequacy of the available information in terms of E.O. 12968 requirements. Incomplete and unsubstantiated information must be sufficiently developed before the determination process proceeds.

1. True
2. False

5-32. Which of the following is an example of adjudicative "disqualifying factors"?

1. Association or sympathy with persons or organizations that advocate the overthrow of the U.S. Government, or any state or subdivision, by force or violence or by other unconstitutional means
2. The individual was unaware of the unlawful aims of the individual or organization and severed ties upon learning of these
3. The individual's involvement was only with the lawful or humanitarian aspects of such an organization
4. The person has had no recent involvement or association with such activities

5-33. Which of the following is an example of adjudicative "mitigating factors"?

1. The exercise of dual citizenship
2. Possession and/or use of a foreign passport
3. Voting in foreign elections
4. An expressed willingness to renounce dual citizenship

5-34. Which of the following mitigating factors pertain(s) to criminal conduct?

1. The criminal behavior was not recent
2. The crime was an isolated incident
3. Acquittal
4. All of the above

5-35. Which of the following disqualifying factors pertain(s) to financial considerations?

1. Affluence resulting from a legal source
2. A history of not meeting financial obligations
3. Unexplained affluence
4. Both 2 and 3 above

5-36. Noncompliance with security regulations raises doubt about an individual's trustworthiness, willingness, and ability to safeguard classified information.

1. True
2. False

5-37. Which of the following criteria will be considered as potentially impacting personnel security determinations?

1. Cohabitation
2. An individual's immediate family, including cohabitants and other persons to whom he or she may be bound by affection, influence, or obligation are not citizens of the United States or may be subject to duress by a foreign power
3. Demonstrated misuse of classified information technology systems
4. Both 2 and 3 above

5-38. In adjudications, the protection of the national security may NOT be the paramount determinant.

1. True
2. False

5-39. Which of the following entities is responsible for deciding appeals from DON personnel of unfavorable personnel security determinations made by the DON CAF?

1. SECNAV
2. PSAB
3. CNO (09B)
4. NCIS

5-40. DON CAF officials are prevented from serving as members of the PSAB or communicating with PSAB members concerning the merits of an appeal.

1. True
2. False

5-41. Which of the following is NOT a responsibility of the President of the PSAB?

1. Appoints board members
2. Ensures an attorney is available for legal questions, guidance or opinions
3. Appoints an Executive Director of the PSAB
4. Establishes administrative procedures

5-42. The PSAB consists of how many members?

1. 5
2. 4
3. 3
4. 2

5-43. Appellants may request a personal presentation/appearance before the PSAB.

1. True
2. False

5-44. First time candidates and candidates for clearance at a higher level than currently held must have their U.S. citizenship status verified before security processing begins.

1. True
2. False

5-45. The requirement to verify U.S. citizenship for first time candidates and candidates for clearance at a higher level than currently held is satisfied under which of the following conditions?

1. A valid BI or SBI completed before 1 Sep 79 exists proving citizenship
2. The record of an officer in the Navy or Marine Corps does not contain evidence of non-U.S. citizenship
3. The service record contains a DD 1966 with certification that the documents verifying U.S. citizenship have been sighted
4. All of the above

5-46. Which of the following primary forms of evidence may be used to prove U. S. citizenship?

1. Signed affidavit from mother
2. A U.S. birth certificate with a raised seal
3. Family bible records
4. A baptismal record

5-47. Exactly who are considered non-U.S. citizens?

1. U. S. nationals
2. Foreign nationals
3. Immigrant aliens
4. Both 2 and 3 above

5-48. Non-U.S. citizens are NOT eligible for access to Top Secret information and can NOT perform Presidential Support duties or Nuclear Weapons Personnel Reliability Program duties.

1. True
2. False

5-49. In all cases, only United States citizens are eligible for a security clearance.

1. True
2. False

5-50. For security purposes, which of the following persons are considered U. S. citizens?

1. U.S. nationals
2. Naturalized citizens
3. Citizens of the Federated States of Micronesia
4. All of the above

# ASSIGNMENT 6

Textbook Assignment: ***Department of the Navy Information Security Program Regulation, SECNAVINST 5510.36,*** "Introduction to the Information Security Program," chapter 1, pages 1-1 through 1-11, "Command Security Management," chapter 2, pages 2-1 through 2B-2, and "Security Education," chapter 3, page 3-1.

---

***LEARNING OBJECTIVE***: *Describe the basic policy of the Navy Information Security Program and identify responsibilities of designated authorities.*

6-1. The ISP is implemented within DoN in compliance with which of the following references?

1. E.O. 12958
2. 32 CFR Part 2001
3. ISOO Directive 1
4. All of the above

6-2. What publication is the controlling regulation for the implementation of the ISP?

1. SECNAVINST 5510.30A
2. OPNAVINST 5510.1H
3. SECNAVINST 5510.36
4. OPNAVINST S5460.4C

6-3. What standards concerning the classification, safeguarding, transmission and destruction of classified information are represented in the ISP regulation?

1. The maximum acceptable standards
2. The minimum acceptable standards
3. The uniform mandatory standards
4. The GSA standards

6-4. What individuals are responsible for compliance with the ISP regulation?

1. All Navy civilian employees
2. All Marine Corps civilian employees
3. All Navy and Marine Corps military personnel
4. All of the above

6-5. What official is responsible for the authorization of SAPs?

1. CNO
2. Director, Naval Intelligence
3. SECDEF or Deputy SECDEF
4. SECNAV

6-6. What regulation governs SCI?

1. DoD 5105.21-M-1
2. DoD Directive O-5205.7
3. DoD 5220.22-M
4. SECNAVINST 5510.36

6-7. What reference(s) established the NISP?

1. E.O. 12958
2. E.O. 12829
3. Atomic Energy Act of 30 Aug 54
4. All of the above

6-8. The NISP is applicable to information classified under what authority?

1. Atomic Energy Act of 30 Aug 54
2. E.O. 12958
3. Both 1 and 2 above
4. DoD Directive 5200.1

6-9. Which of the following is/are considered "controlled unclassified information"?

1. FOUO
2. DEA sensitive information
3. Both 1 and 2 above
4. FRD

6-10. Requests for guidance or interpretations regarding the policies contained in SECNAVINST 5510.36 should be made to what authority?

1. Local command security office
2. CNO (N09N2)
3. Both 1 and 2 above
4. NCIS

6-11. Under what circumstances, if any, may the commanding officer modify SECNAVINST 5510.36 safeguarding requirements?

1. During training exercises
2. During combat or combat-related operations
3. During a civil disturbance
4. Never

6-12. When a commanding officer seeks permission to waive a requirement for a specific safeguarding requirement, the request must be submitted to what official?

1. Director, Defense Security Service
2. Director, Naval Intelligence
3. CNO (N09N2)
4. SECNAV

6-13. What authority is responsible for overseeing agency implementation of E.O. 12958?

1. SPB
2. Director, ISOO
3. NSA
4. SECNAV

6-14. What interagency security organization was created by the President and is co-chaired by the Deputy SECDEF and the DCI?

1. NFIB
2. SPB
3. NDPB
4. NSC

6-15. What agency has jurisdiction over investigative matters which include espionage, sabotage, treason, and other subversive activities?

1. NCIS
2. FBI
3. DCI
4. DIA

6-16. What military department is the executive agency for the Central U.S. Registry?

1. Navy
2. Marines
3. Army
4. Air Force

6-17. What authority is responsible for providing signals intelligence and COMSEC for the U.S. Government?

1. DIA
2. ONI
3. NSA
4. SECDEF

6-18. Within the DoD, what official must approve requests to lower any COMSEC standards?

1. Chairman, JCS
2. SECDEF
3. SECNAV
4. Director, CIA

6-19. Within the DON, who is responsible for implementing an ISP in accordance with the provisions of public laws, executive orders, and directives issued by other authorities?

1. CNO (N09N)
2. SECNAV
3. DNI
4. Director, Navy IPO

6-20. Who is responsible for the administration of the DON CMS program and acts as the central office of records for DON CMS accounts?

1. Director, Special Programs
2. NSA
3. DNI
4. DCMS

6-21. Who is responsible for signals intelligence activities and the administration of the SCI programs within the DON cryptologic community?

1. NSC
2. Director, ONI
3. COMNAVSECGRU
4. DNI

***LEARNING OBJECTIVE***: *Recognize command security management requirements and identify key command officials and their responsibilities.*

6-22. The term "command" is a generic term for which of the following activities?

1. Installation
2. Laboratory
3. Detachment
4. All of the above

6-23. The term "commanding officer" is a generic term for which of the following officials?

1. Commander
2. Director
3. Both 1 and 2 above
4. Any administrative officer

6-24. What command official is responsible for the effective management of the command ISP?

1. The security manager
2. The commanding officer
3. The security officer
4. The SSO

6-25. Commands shall NOT exceed the standards established by SECNAVINST 5510.36.

1. True
2. False

6-26. The commanding officer has which of the following responsibilities?

1. Issue a command security instruction
2. Approve a command emergency plan
3. Establish a command industrial security program
4. All of the above

6-27. What is the primary duty of the command security manager?

1. Serve as principal advisor to the commanding officer
2. Serve as COMSEC custodian
3. Serve as the TSCO
4. Serve as the SSO

6-28. When a security guard force is in place, threats to security and other security violations are NOT reported, recorded, or investigated.

1. True
2. False

6-29. What command official(s) is/are responsible for ensuring that all proposed press releases and information intended for public release are subjected to a security review?

1. Commanding officer
2. Security manager
3. Public Affairs officer
4. Both 2 and 3 above

6-30. The TSCO reports directly to what official?

1. Commanding officer
2. Executive officer
3. Security manager
4. SSO

6-31. The security manager may act as the TSCO.

1. True
2. False

6-32. Commands that store large volumes of TS documents are exempt from the annual inventory requirement.

1. True
2. False

6-33. Which of the following positions requires a favorably adjudicated SSBI completed within the previous 5 years?

1. Security manager
2. Security assistant
3. TSCA
4. PAO

6-34. What command official is the commanding officer's primary advisor on the handling of COMSEC information?

1. NWP custodian
2. CMS custodian
3. SSO
4. Security manager

6-35. The NWP Custodian position may be a collateral duty.

1. True
2. False

6-36. The NATO control officer is required to have an alternate.

1. True
2. False

6-37. What command official is responsible for signing DD 254s?

1. Security manager
2. Commanding officer
3. Contracting officer's representative
4. Assistant security manager

6-38. What command official implements the command INFOSEC program?

1. ISSM
2. ISSO
3. Security manager
4. Commanding officer

6-39. The duties of the ISSM and ISSO are NEVER performed by the same official.

1. True
2. False

6-40. What official is responsible for the receipt, storage and processing of SCI within a command?

1. SSO
2. CO
3. CMS custodian
4. Security officer

6-41. What official is responsible for the operation, control and use of all command SCIFs?

1. Security officer
2. SSO
3. CO
4. Physical Security officer

6-42. What instruction governs the requirements for the designation of a command security officer?

1. SECNAVINST 5510.36
2. SECNAVINST 5510.30A
3. OPNAVINST 5530.14C
4. OPNAVINST 3120.32C

6-43. The purpose of an SSA is to enable the host command to perform specific security functions for the tenant command.

1. True
2. False

6-44. How often are command inspections, assist visits, and program reviews conducted?

1. Annually
2. Biannually
3. Semi-annually
4. As necessary

6-45. The security manager is responsible for developing a command security instruction that supplements SECNAVINST 5510.36.

1. True
2. False

6-46. A command should have an emergency plan in the event of which of the following occurrences?

1. A natural disaster
2. A civil disturbance
3. Both 1 and 2 above
4. International terrorism

6-47. All commands are required to have an emergency destruction supplement.

1. True
2. False

***LEARNING OBJECTIVE***: *Describe security education policy and specific education requirements.*

6-48. It is the commanding officer's responsibility to ensure that all command personnel receive the necessary security education to enable quality performance of their security functions.

1. True
2. False

6-49. What DON authority is responsible for policy guidance, education requirements and support for the DON security education program?

1. CNO (N2)
2. CNO (N09N)
3. CNO (N64)
4. CNO (N89)

6-50. In addition to general security education, specialized training is required for which of the following personnel?

1. Original Classification Authorities
2. Derivative classifiers
3. Classified couriers
4. All of the above

# ASSIGNMENT 7

Textbook Assignment: ***Department of the Navy Information Security Program Regulation, SECNAVINST, 5510.36,*** "Classification Management," chapter 4, pages 4-1 through 4-16, and "Security Classification Guides," chapter 5, pages 5-1 through 5-3.

---

***LEARNING OBJECTIVE***: *Recognize classification management criteria, including classification levels, responsibilities of original and derivative classification authorities, procedures, and special categories of classified information.*

7-1. What is the only basis for classifying NSI?

1. E.O. 12333
2. E.O. 12958 and the Atomic Energy Act of 30 Aug 54
3. The Counter-Espionage Act
4. Original Classification Prerogative

7-2. Information classified by DON OCAs shall be declassified when?

1. As soon as it no longer meets the standards for classification
2. Within 5 years of creation
3. Within 10 years of creation
4. Within 25 years of creation

7-3. What are the authorized classification levels of NSI?

1. SCI, TS, and Secret only
2. FOUO, Secret Sensitive, SCI, and TS
3. TS, Secret, and Confidential only
4. SCI, TS, Secret, and Confidential

7-4. What is the unauthorized disclosure of classified information expected to cause?

1. Damage
2. Espionage
3. Technology transfer
4. Public media compromise

7-5. What does the classification level assigned to classified information indicate?

1. The degree of damage its unauthorized disclosure would cause to the national security
2. The sensitivity level of the information
3. The possibility of compromise
4. The military application of the information

7-6. Original classification is the creation of classified information based upon existing classification guidance.

1. True
2. False

7-7. Who is authorized to originally classify DON information?

1. Officials delegated the authority
2. The author of the information
3. The commanding officer
4. The security manager

7-8. Who approves the DON designation of TS Original Classification Authority?

1. Commanding officer
2. Secretary of the Navy
3. Security manager
4. CNO (N09N)

7-9. Who approves the designation of Secret OCAs?

1. CNO (N09N)
2. Secretary of the Navy
3. Commanding officer
4. Security manager

7-10. The authority to originally classify Secret and Confidential information is inherent in TS Original Classification Authority.

1. True
2. False

7-11. What is required of OCAs after the required approval and prior to originally classifying information?

1. Submit their name and position title to the CNO (N09N2)
2. Notify the commanding officer
3. Be trained and provide written confirmation of that training to the CNO (N09N2)
4. Notify their security manager

7-12. At the time of original classification, the OCA shall attempt to establish a specific date or event, not to exceed 5 years from the date of the original classification.

1. True
2. False

7-13. What is derivative classification?

1. The incorporating, paraphrasing, restating, or generating, in new form, information that is already classified
2. The initial determination that information requires, in the interest of the national security, protection against unauthorized disclosure
3. The reproduction of classified information
4. The duplication of classified markings

7-14. What is required of derivative classifiers?

1. Observe and respect original classification determination made by OCAs
2. Use caution when paraphrasing or restating extracted classified information
3. Carry forward to any newly created document the pertinent classification markings
4. All of the above

7-15. The majority of classified information produced by a command is based on original classification decisions.

1. True
2. False

7-16. Information previously declassified and officially released to the public may be reclassified.

1. True
2. False

7-17. When reason exists to believe information is improperly classified, what shall the challenger do?

1. Contact the CNO (N09N) for resolution
2. Contact the local NCIS office for resolution
3. Remark the material with the correct classification
4. Contact the cognizant command security manager or the classifier of the information for resolution

7-18. After a final determination of a classification challenge, if the challenger is still not satisfied, that person may appeal the OCA's decision to what official?

1. CNO (N09N)
2. CO
3. The security manager
4. The derivative classifier

7-19. If there is reasonable doubt about the need to classify information, it shall NOT be classified.

1. True
2. False

7-20. When is information marked with a "tentative" classification?

1. It is included in a working paper
2. The classification level is uncertain or it is generated in conjunction with an IR&D/B&P effort
3. It was previously declassified
4. It is a presentation

7-21. What DON official serves as the Patent Counsel for the DON?

1. SECDEF
2. SECNAV
3. CNO (N09N)
4. CNR (Code 300)

7-22. The authority to assign the U.S. classification equivalent to FGI requires Original Classification Authority.

1. True
2. False

7-23. Foreign government unclassified and RESTRICTED information provided with the expectation, expressed or implied, that it, the source, or both, are to be held in confidence, shall be marked at what classification level?

1. RESTRICTED
2. TS
3. Confidential
4. Secret

7-24. What is classified information relating to the tactical characteristics and capabilities of naval nuclear ships and propulsion plant design typically categorized as?

1. NSI
2. RD
3. FRD
4. TS

7-25. What is classified information primarily relating to the reactor plant of a nuclear propulsion system typically categorized as?

1. TS
2. RD
3. FRD
4. RESTRICTED

7-26. Who is the program manager for the DON Naval Nuclear Reactor Program?

1. CNO (N09N)
2. SECNAV
3. Commander, NAVSEA (SEA-08)
4. Commanding Officer, Naval Surface Warfare Center

7-27. Where is detailed classification guidance concerning NNPI found?

1. CG-RN-1 (Rev.3)
2. SECNAVINST 5510.36
3. E.O. 12958
4. E.O. 12968

7-28. The SECNAV is authorized to downgrade, declassify, or modify an OCA's decision, provided the DON exercises final classification authority over the information.

1. True
2. False

7-29. What regulation contains detailed policy concerning the automatic declassification of DON information?

1. OPNAVINST 5513.16A
2. OPNAVINST 5510.1H
3. DoD 5200.1-R
4. OPNAVINST 5513.1E

7-30. Only the SECDEF and the Secretaries of the Military Departments may exempt information from automatic declassification.

1. True
2. False

7-31. What is systematic declassification review?

1. The review for declassification of certain categories of classified information
2. The review for declassification of classified information contained in records determined by the Archivist of the U.S. to have permanent historical value
3. The review for declassification of classified information 25 years or older
4. The review for declassification of classified information 10 years or older

7-32. What DON official is responsible for identifying to the Archivist of the U.S., classified information 25 years old or older, which still warrants protection?

1. SECNAV
2. Director, NAVHIST
3. CNO (N09N)
4. SECDEF

7-33. Special procedures for systematic review for declassification of classified cryptologic information are established by what authority?

1. SECDEF
2. SECNAV
3. CNO (N09N)
4. The NSA

7-34. What official may establish procedures for the systematic declassification review of classified intelligence information?

1. SECDEF
2. SECNAV
3. DCI
4. Commander, NIC

7-35. The provisions for systematic declassification review do NOT apply to which of the following special types of classified information?

1. FGI
2. RD
3. FRD
4. All of the above

7-36. Information classified under E.O. 12958 or predecessor orders may be subject to mandatory declassification review under what circumstances?

1. The information is not exempted from search or seizure under Title 50, U.S.C. Section 401, Central Intelligence Agency Act
2. The information has not been reviewed within the preceding 2 years
3. The request for review describes the information with sufficient specificity to enable its location with a reasonable amount of effort
4. Both 2 and 3 above

7-37. Information originated by the incumbent President, the current White House staff, its appointed committees, commissions, boards, or other entities of the incumbent President's Executive Office is exempted from which of the following reviews?

1. Congressional declassification review
2. Senate declassification review
3. Oversight review
4. Mandatory declassification review

7-38. The downgrading or declassification review of classified information officially transferred to a DON command becomes the responsibility of what official?

1. The commanding officer or senior official with OCA at that command
2. The security manager
3. CNO (N09N)
4. Director, ISOO

7-39. OCAs are responsible to notify all holders of any classification changes involving information they originally classified.

1. True
2. False

***LEARNING OBJECTIVE***: *Recognize the functions of Security Classification Guides and describe the Rankin program.*

7-40. Which of the following purposes do security classification guides serve?

1. As the primary reference source for derivative classifiers
2. As source documents to identify the level and duration of classification for specific information elements
3. Both legal and management functions by recording DON original classification determination
4. All of the above

7-41. What officials are authorized to prepare and submit DON SCGs?

1. Commanding officers
2. Approved DON OCAs
3. Security managers
4. Security specialists

7-42. The approved format for DON SCGs is found in what regulation?

1. OPNAVINST 5513.1E
2. OPNAVINST 5513.16A
3. E.O. 12958
4. DoD 5200.1-R

7-43. What is the computerized data base that provides for the standardization, centralized management and issuance of all DON SCGs?

1. NEBS Program
2. RANKIN Program
3. SCG Program
4. DON Directive Program

7-44. The DON RANKIN Program Manager is charged with what primary responsibility?

1. Notifying all holders of all changes in DON classified information
2. Approving OCAs that create SCGs
3. Maintaining historical files for all SCGs
4. Periodically rewriting all DON SCGs

7-45. Cognizant DON OCAs shall conduct periodic reviews of their SCGs at what minimum time interval?

1. Every year
2. Every 2 years
3. Every 5 years
4. Every 10 years

7-46. All changes to existing DON SCGs are reported to what official?

1. SECNAV
2. CNO (N09N)
3. SECDEF
4. Director, ISOO

7-47. Who typically issues SCGs for systems, plans, programs, or projects involving more than one DoD component?

1. OSD or the DoD component designated by the OSD as executive or administrative agent.
2. ISOO
3. SECNAV
4. Director, ISOO

7-48. What OPNAVINST series contains, as enclosures, individual SCGs for classified DON systems, plans, programs or projects?

1. OPNAVINST 5510
2. OPNAVINST 5530
3. OPNAVINST 5513
4. OPNAVINST 5520

7-49. Most instructions in the OPNAVINST 5513 series can be ordered through what source?

1. CNO (N2)
2. ISOO
3. CNO (N89)
4. DON supply system

7-50. Should a conflict arise between an SCG and a classified source document, the instructions in the SCG take precedence.

1. True
2. False

# ASSIGNMENT 8

Textbook Assignment: ***Department of the Navy Information Security Program Regulation, SECNAVINST 5510.36,*** "Marking," chapter 6, pages 6-1 through 6-26.

---

***LEARNING OBJECTIVE***: *Describe the marking policy and procedures for classified information, including requirements for portion marking and placement of associated markings and warning notices.*

8-1. What shall all classified information be clearly marked with?

1. The appropriate classification level and date only
2. The appropriate classification level, office of origin, and date only
3. The appropriate classification level and office of origin only
4. The appropriate classification level, date, office of origin, and all applicable associated markings

8-2. Classified markings serve to warn holders of which of the following requirements?

1. Storage requirements
2. Special access requirements
3. Special control requirements
4. All of the above

8-3. No classification level or associated markings shall be applied to any article or portion of an article that has appeared in the public domain.

1. True
2. False

8-4. RD (including CNWDI) or FRD information shall NOT be marked with a classification level.

1. True
2. False

8-5. Classified documents provided to foreign governments, their embassies, missions, or similar official offices within the U.S., shall be marked only with the applicable associated markings.

1. True
2. False

8-6. Exceptions to the basic marking policy include which of the following documents?

1. RD (including CNWDI), and FRD
2. Documents that have appeared in the public domain or that may reveal a confidential source
3. Documents provided to foreign governments, their embassies, missions, or similar official offices within the U.S.
4. All of the above

8-7. The "face" of a document is also referred to as the front cover, first page, or title page.

1. True
2. False

8-8. The highest overall classification level shall be marked, top and bottom center, on the face and back cover of all classified documents.

1. True
2. False

8-9. What shall be included on documents that cannot be marked with the overall classification level on the face and back cover?

1. A distribution statement
2. An index
3. An explanatory statement on the face
4. A distribution list

8-10. All interior pages of a document shall be marked with the highest overall classification level with what exception?

1. Blank pages
2. The table of contents
3. Reference pages
4. Index pages

8-11. When the alternative marking method of marking document interior pages with the highest overall classification scheme is used, the requirement to portion mark is eliminated.

1. True
2. False

8-12. Each portion (i.e., title, section, part, paragraph, subparagraph, etc.) of a classified document shall be marked to show its classification level.

1. True
2. False

8-13. What does the marking "FOUO" designate about unclassified information?

1. That it was formerly sensitive but unclassified
2. That it is "eyes only" information
3. That it may be used for Navy purposes only
4. That it is exempt from mandatory release to the public under SECNAVINST 5720.42E

8-14. In addition to the overall classification level, what shall portion markings include?

1. The abbreviated form of all applicable warning notices and intelligence control markings
2. The date
3. The applicable downgrading or declassification instructions
4. The initials of the OCA responsible for the information

8-15. In the exceptional case that a document cannot be portion marked, what is included on the face of the document?

1. The reason why the document cannot be portion marked
2. A description of what portions are marking document interior pages classified and at what level
3. The name and personal identifier of the person authorizing the exception to the marking requirement
4. A description of what portions of the document are unclassified

8-16. What must figures, tables, graphs, graph captions or titles, charts and similar illustrations appearing within a document be marked with?

1. The highest overall classification level of the document only
2. The abbreviated form of any applicable warning notices or intelligence control markings only
3. Applicable warning notices and intelligence control markings only
4. The classification level and the short form of any applicable warning notices and intelligence control markings

8-17. How shall portions of U.S. documents containing NATO or FGI be marked?

1. "FGI"
2. To reflect the country or international organization, and the appropriate classification level
3. "NATO"
4. "RESTRICTED"

8-18. Portions of U.S. documents marked with an "(R)" indicates that the portions contain what information?

1. NATO RESTRICTED or Foreign Government RESTRICTED
2. DOS SBU
3. FOUO
4. FGI or NATO

8-19. The authority to grant waivers of the portion marking requirement rests with the CNO (N09N).

1. True
2. False

8-20. Portion marking waivers granted by DoD officials prior to what date are no longer valid?

1. 17 May 1999
2. 10 May 1999
3. 14 October 1995
4. 20 October 1996

8-21. All DON marking waiver requests must be sent via the CNO (N09N2).

1. True
2. False

8-22. When subjects or titles of classified documents are included in the reference line, enclosure line, or the body of the information, where is the classification level marked?

1. Immediately before the subject or title
2. Immediately following the subject or title
3. On the reference page
4. On the cover page

8-23. On what page of the document are associated markings spelled out in their entirety?

1. Face
2. First page
3. Title page
4. All of the above

8-24. Where on the document are associated markings NOT spelled out?

1. Interior pages
2. Front cover
3. Face
4. First page

8-25. What is marked on the face of documents containing information originally classified?

1. A "Classified by" line only
2. A "Derived from" line only
3. "Classified by" and "Reason" lines
4. "Derived from" and "Reason" lines

8-26. How is the face of a document containing information both originally and derivatively classified marked?

1. With "Classified by" and "Reason" lines
2. With a "Classified by" line only
3. With a "Derived from" line only
4. With "Derived from" and "Reason" lines

8-27. How is the face of a document containing information derivatively classified marked?

1. With “Derived from" and "Reason" lines
2. With a "Derived from" line only
3. With "Classified by" and "Reason" lines
4. With a "Classified by" line only

8-28. How is the "Classified by" or "Derived from" line of a document classified by a combination of sources annotated?

1. "Compilation of Sources"
2. "Various Sources"
3. "Multiple Sources"
4. "See attached listing"

8-29. At a minimum, where shall a record of the sources of documents classified by a combination of sources be maintained?

1. With the file or record copy of the document
2. With all copies of the document
3. With the bibliography page
4. With the reference list

8-30. What does the "Downgrade to" line indicate?

1. The date or event the document is unclassified
2. The classification level the document is to be downgraded to only
3. The date or event that a document will be downgraded to a lower classification level only
4. The specific date or event in which a document is to be downgraded and at what classification level

8-31. What does the "Declassify on" line indicate?

1. The date or event on which a document should have a declassification review
2. The date or event on which a change in a document's classification level will occur
3. The date or event at which a document no longer requires classification in the interest of national security
4. The date or event the document is releasable to the public

8-32. What does an "X" code annotated on the "Declassify on" line indicate?

1. The document is exempt from automatic declassification
2. The document is declassified
3. The document should be reviewed for declassification
4. The document is tentatively declassified

8-33. What instruction discusses the use of "25X codes" as a declassification instruction applied to permanently-valuable records?

1. SECNAVINST 5510.36
2. OPNAVINST 5513.16A
3. OPNAVINST 5513.1E
4. SECNAVINST 5510.30A

8-34. What is the "Declassify on" line of a document classified by a combination of sources annotated with?

1. The most restrictive downgrading and declassification instructions of all the sources
2. The most restrictive downgrading instructions of all the sources only
3. An "X" code
4. The date of the most recent source

8-35. Warning notices serve to advise holders of classified documents that additional protective measures are required.

1. True
2. False

8-36. Dissemination and Reproduction notices are considered warning notices.

1. True
2. False

8-37. How are documents containing either RD or FRD information marked?

1. Top and bottom center on the face of a document
2. Lower left corner on the face of the document with the applicable warning notice
3. Center top on the face of a document
4. On the cover sheet only

8-38. A document containing both RD and FRD information is marked with which of the following warning notices?

1. Both the RD and the FRD
2. Only the FRD
3. Only the RD
4. The CNWDI

8-39. RD and FRD documents do NOT have to be portion marked.

1. True
2. False

8-40. Since CNWDI is a subset of RD, documents containing CNWDI shall be marked with which of the following warning notices?

1. Both the RD and the CNWDI
2. Only the RD
3. The RD/FRD and the CNWDI
4. Only the CNWDI

8-41. How are portions of RD paragraphs containing CNWDI marked?

1. "(CNWDI)"
2. "(RD/CNWDI)"
3. "(RD)(N)"
4. "(RD/CN)"

8-42. How are interior pages containing CNWDI marked?

1. At the bottom center, after the classification level, with "CNWDI"
2. At the bottom center, after the classification level with "CRITICAL NUCLEAR WEAPONS DESIGN INFORMATION"
3. At the bottom left-hand corner with "CNWDI"
4. At the bottom right-hand corner with “CNWDI”

8-43. Where are the marking policies and dissemination procedures for CNWDI found?

1. OPNAVINST 5570.2
2. NAVSEAINST C5511.32B
3. DoD Directive 5210.2
4. CG-RN-1 (Rev. 3)

8-44. The marking policies and procedures for NNPI are contained in what regulations?

1. NAVSEAINST C5511.32B and CG-RN-1 (Rev. 3)
2. NAVSEAINST C5511.32B and DoD Directive 5210.2
3. DoD Directive 5210.2 and CG-RN-1 (Rev. 3)
4. NAVSEAINST C5511.32B and OPNAVINST 5570.2

8-45. Associated markings are required for classified NNPI not containing RD or FRD information.

1. True
2. False

8-46. SIOP documents are NOT marked in the same manner as any other classified document in what instance?

1. They contain Secret information
2. They contain Confidential information
3. They are being released to NATO
4. They contain unclassified information

8-47. SIOP-ESI documents are subject to special dissemination controls.

1. True
2. False

8-48. What designator is included on messages containing SIOP-ESI?

1. "SIOP-ESI"
2. "SIOP"
3. "SPECAT"
4. "TS"

8-49. What designator is included on COMSEC documents?

1. "SPECAT"
2. "TS"
3. "SENSITIVE"
4. "CRYPTO"

8-50. Only the face of an unclassified FOUO document should be marked "FOR OFFICIAL USE ONLY."

1. True
2. False

8-51. The FOUO portions of a classified document should be marked "(FOUO)."

1. True
2. False

8-52. How shall unclassified letters of transmittal with FOUO attachments or enclosures be marked at the top left corner?

1. "FOUO"
2. "This transmittal contains information exempt from mandatory disclosure under the FOIA."
3. "FOR OFFICIAL USE ONLY ATTACHMENT"
4. “FOUO SPACE ATTACHED”

8-53. With what notice shall FOUO documents transmitted outside the DoD be marked?

1. "FOR OFFICIAL USE ONLY"
2. "Exemption(s) ____ apply"
3. "Exempt from mandatory disclosure "
4. "This document contains information exempt from mandatory disclosure under the FOIA. Exemption(s) __apply."

8-54. Where on the document shall unclassified documents containing DoD UCNI be marked with "DoD Unclassified Controlled Nuclear Information"?

1. The face only
2. The back cover only
3. The face and back cover
4. The face and interior pages

8-55. Classified documents containing DoD UCNI are marked as any other classified document with what, if any, exception?

1. Unclassified interior pages shall be marked “DoD UCNI"
2. Unclassified interior pages shall be marked "For Official Use Only"
3. Unclassified interior pages shall be marked, top and bottom center, with "DoD Unclassified Controlled Nuclear Information"
4. There is no marking exception

***LEARNING OBJECTIVE***: *Recognize the procedures for marking intelligence and other special categories of information and describe marking requirements for correspondence and letters of transmittal; messages; files and folders; blueprints and maps and charts; and audio-visual media.*

8-56. Intelligence control markings are applicable to documents containing what information?

1. Sensitive but unclassified
2. Intelligence
3. RD or FRD
4. FGI

8-57. Documents classified by a foreign government or international organization retain their original foreign classification designation or are assigned the U.S. classification equivalent.

1. True
2. False

8-58. Authority to assign U.S. designations to foreign government information requires original classification authority.

1. True
2. False

8-59. Downgrading or declassification instructions are not included on FGI information unless specified or agreed to by the foreign entity.

1. True
2. False

8-60. What are nicknames?

1. A combination of two non-code words which may or may not be classified
2. An exercise term which may or may not be classified
3. A combination of two unclassified words with an unclassified meaning
4. A single word with a classified meaning

8-61. Classification by compilation may occur when items of unclassified or classified information are combined.

1. True
2. False

8-62. What information shall be included in the statement on the face of a document classified by compilation?

1. The fact that individual parts are unclassified or are of a lower classification
2. The authority for the compilation classification
3. The reason why the compilation warrants classification or a higher classification
4. All of the above

8-63. Component parts of a document which are likely to be removed shall be marked as a separate document.

1. True
2. False

8-64. Upon notification by proper authority, holders of classified documents that have been upgraded, downgraded, or declassified shall remark the affected portions.

1. True
2. False

8-65. How shall a newly created document be marked when the classification is based on source documents with old declassification instructions that have indeterminate declassification dates or events?

1. "Review on: ___"
2. "Declassify on: ___"
3. No marking until OCA determination
4. "Source marked OADR, source dated _____"

8-66. Letters of transmittal may or may not have classified enclosures or attachments.

1. True
2. False

8-67. Mark only the face of a two-page unclassified letter of transmittal with the highest overall classification level of its enclosures or attachments.

1. True
2. False

8-68. Both classified and unclassified letters of transmittal shall provide what additional information?

1. Classified serial number
2. Instructions concerning the classification level of the transmittal with and without its enclosures or attachments
3. A "Declassify on" line
4. The name or personal identifier of the OCA

8-69. There are no marking requirements for letters of transmittal containing controlled unclassified information.

1. True
2. False

8-70. Classified messages shall be portion marked with the exception of certain preformatted messages.

1. True
2. False

8-71. When self-processing film or paper is used to photograph or reproduce classified information, how should the negative or last exposure be handled?

1. Removed from the camera and secured
2. Secured with the camera as classified
3. Properly destroyed
4. Each of the above

8-72. How are slides or transparencies which are permanently removed from a set marked?

1. As separate documents
2. With a copy number
3. With the overall classification of the original presentation
4. With a "tentative" classification marking

8-73. How shall classified motion pictures, films, and videotapes be marked?

1. With the highest overall classification level only
2. With the highest overall classification level and all applicable associated markings
3. With the address of the originator
4. With downgrading instructions only

8-74. How is classified AIS media not programmed in a readily accessible format identified?

1. Marked documentation is kept with the media
2. The media is marked on the outside with the overall classification level and all applicable associated markings
3. Both 1 and 2 above
4. It is placed in a classified folder

8-75. Miscellaneous classified materials created during the production of a document, such as rejected copies, typewriter ribbons, or carbons, do NOT require any markings, unless necessary to ensure their protection.

1. True
2. False

# ASSIGNMENT 9

Textbook Assignment: ***Department of the Navy Information Security Program Regulation, SECNAVINST 5510.36,*** "Safeguarding," chapter 7, pages 7-1 through 7-11; and "Storage and Destruction," chapter 10, pages 10-1 through 10D-8.

---

***LEARNING OBJECTIVE***: *Recognize the policy and procedures for safeguarding classified information, including measures for Top Secret, Secret, and Confidential information, working papers, and special types of classified and controlled unclassified information.*

9-1. Which of the following statements regarding the safeguarding of classified information is/are correct?

1. The information shall be processed only on accredited AISs
2. The information may be used only where unauthorized persons may not gain access
3. The information shall be stored in approved equipment
4. All of the above

9-2. Which of the following areas must be designated, in writing, by the commanding officer?

1. Exclusion areas
2. Controlled areas
3. Restricted areas
4. Sensitive areas

9-3. When a military or civilian individual retires from the Navy, all classified information in his or her possession must be returned to the appropriate authority, EXCEPT for that information specifically originated by the individual.

1. True
2. False

9-4. What type of information must be continuously accounted for?

1. All classified information
2. TS and Secret
3. TS only
4. Secret and Confidential

9-5. TS publications that are mass-produced reproductions must be marked with individual copy numbers.

1. True
2. False

9-6. A receipt is NOT required for TS disseminated within a command.

1. True
2. False

9-7. TS documents must be inventoried at what maximum interval?

1. Monthly
2. Quarterly
3. Semiannually
4. Annually

9-8. The commanding officer shall establish administrative procedures for controlling Secret and Confidential information based on which of the following criteria?

1. Command location
2. Threat assessment
3. Command mission
4. All of the above

9-9. What are working papers?

1. Finished classified documents that have been published and distributed
2. Classified notes, drafts, and similar items that are not finished documents
3. All documents and material used in the performance of official duties
4. Drawings, photographs, schematics, or diagrams used to describe the operation of machinery or equipment

9-10. How must classified working papers be safeguarded?

1. Dated and marked "Working Paper" when created
2. Marked with the highest overall classification level and protected accordingly
3. Destroyed when no longer needed
4. All of the above

9-11. Classified working papers must be controlled and marked as a finished document when retained for more than 90 days.

1. True
2. False

9-12. What instruction provides guidance for safeguarding NATO information?

1. OPNAVINST C5510.101D
2. OPNAVINST 5510.1H
3. SECNAVINST 5510.36
4. OPNAVINST S5511/35K

9-13. Only second echelon commands that receive NWPs must establish an NWP library.

1. True
2. False

9-14. For what minimum number of years must a command retain records for TS FGI?

1. Two
2. Three
3. Four
4. Five

9-15. When a foreign government's requirement to protect its RESTRICTED or unclassified information is lower than that prescribed for U.S. Confidential, what should you do to prevent unauthorized access?

1. Ensure that the information is provided to only those individuals who have a need to know
2. Provide, in writing or oral briefing, applicable handling instructions to those given access
3. Provide storage instructions
4. All of the above

9-16. What authority provides guidance for safeguarding RD (including CNWDI) and FRD?

1. DoD 5105.29-M-1
2. DoD Dir 5210.2
3. SECNAVINST 5510.36
4. SECNAVINST 5510.30A

9-17. What authority governs the control and safeguarding of sensitive information contained in AISs?

1. The Privacy Act, U.S.C. Section 552a
2. Computer Security Act of 1987
3. SECNAVINST 5720.42E
4. OPNAVINST 5510.158A

9-18. What authority must approve the use of alternative or compensatory control measures?

1. CNO (N09N2)
2. CNO (N89)
3. CNO (N09N)
4. CNO (N2)

9-19. Alternative or compensatory control measures may NOT be used on which of the following types of information?

1. RD
2. FRD
3. CNWDI
4. All of the above

9-20. Code words must be established and approved by CNO (N09N) prior to applying alternative or compensatory control measures to classified information.

1. True
2. False

9-21. Which of the following precautions must be taken to safeguard classified information during working hours?

1. Classified documents removed from storage must be under constant surveillance at all times or covered when not in use
2. Any kind of item used in the preparation of a classified document must either be protected according to its level of classification or destroyed
3. Visitors who are not authorized access to classified information should not be received in areas where classified information is being used or discussed
4. All of the above

9-22. At the end of the day individuals are personally responsible for which of the following security actions?

1. Placing their classified documents and related classified material in the appropriate security container, vault, or secure room
2. Ensuring that each container drawer, vault or secure room is secured
3. Conducting an end of the day security check of their working spaces
4. All of the above

9-23. Classified information shall be disclosed at a meeting only when it serves a specific U.S. Government purpose.

1. True
2. False

9-24. Under which of the following circumstances is it permissible to grant a visitor access to classified information?

1. The security officer verifies the visitor’s need to know
2. The visitor presents a visit request
3. The visitor's clearance level and need to know have been verified by the custodian of the information
4. All of the above

9-25. A Secret classified meeting may be held at which of the following locations?

1. A naval facility
2. Andrews AFB Conference Center
3. A cleared DoD contractor facility
4. All of the above

9-26. What instruction governs the TSCM policy regarding discussions of TS information at classified meetings?

1. SECNAVINST 5720.42E
2. SECNAVINST 5500.31A
3. SECNAVINST 5510.36
4. OPNAVINST 5530.14C

9-27. Which of the following conditions must be met before a command agrees to host a classified meeting outside the command, including those supported by non-U.S. Government associations?

1. Confirm that other means for communicating or disseminating the classified information would not accomplish the purpose
2. Ensure that attendance is limited to U.S. Government personnel or cleared DoD contractor employees
3. Request approval from CNO (N09N2)
4. All of the above

9-28. Which of the following DON authorities must approve any participation by foreign nationals prior to their attendance at classified meetings?

1. CNO (N09N2)
2. SECNAV
3. Security manager
4. Navy IPO or cognizant command foreign disclosure office

9-29. What command official is responsible for establishing procedures for the reproduction of classified information?

1. Security manager
2. Commanding officer
3. Physical Security officer
4. SSO

9-30. Who must approve the reproduction of TS FGI?

1. CNO (N09N2)
2. NAVY IPO
3. Originating government
4. Director, International Security Policy

9-31. Records of receipt, internal distribution, destruction, inventory, access, transmission and reproduction must be maintained for both TS and Secret FGI.

1. True
2. False

***LEARNING OBJECTIVE***: *Identify storage requirements and destruction standards and procedures for classified information*

9-32. When, if ever, may money or jewelry be stored in a GSA-approved container used to store classified information?

1. During emergency and combat situations
2. When the articles are to be used as evidence in a military court
3. When the articles are double-wrapped and segregated from the classified information
4. Never

9-33. Any weakness, deficiency, or vulnerability found to exist in any equipment used to safeguard classified information shall be reported to which of the following authorities?

1. Naval Supply System Command
2. CNO (N09N2)
3. GSA
4. CNO (N09N3)

9-34. What agency has the responsibility for establishing and publishing minimum standards, specifications, and supply schedules for security equipment and devices used for storage and destruction of classified information?

1. Naval Facilities Engineering Service Command
2. NCIS
3. GSA
4. Naval Supply Systems Command

9-35. Any GSA-approved container housing TS information must be marked on the outside of the container for emergency situations.

1. True
2. False

9-36. When a GSA-approved security container used to store TS information is located in the U.S., no supplemental controls are required.

1. True
2. False

9-37. Which of the following supplemental controls is/are required for Secret information stored in an open storage area?

1. Continuous protection provided by cleared guard or duty personnel
2. Inspection by cleared guard or duty personnel every 8 hours
3. An IDS with response time within 45 minutes of alarm annunciation
4. All of the above

9-38. Which of the following individuals is/are authorized to change the combination on security containers, vault doors or secure room doors housing Secret information?

1. A civilian Navy employee with a Secret clearance
2. A chief petty officer with a Top Secret clearance
3. Both 1 and 2 above
4. A locksmith

9-39. All non-GSA-approved cabinets must be replaced with GSA-approved security containers prior to what replacement date?

1. 1 January 2002
2. 1 October 2002
3. 30 September 2005
4. 1 October 2015

9-40. Which of the following materials should NOT be used to construct the walls, floor, and roof of a secure room?

1. 2-inch wire mesh
2. Plaster or plywood
3. Gypsum wallboard or wood
4. Metal panels

9-41. The combination of a security container used to store classified information must be changed on which of the following occasions?

1. When the combination has been subjected to compromise
2. When first placed in use
3. When taken out of service
4. All of the above

9-42. What combination should be set on a built-in combination lock that has been taken out of service?

1. 10-20-30
2. 10-15-20
3. 50-25-50
4. 50-30-50

9-43. What combination should be set on a combination padlock that is taken out of service?

1. 10-20-10
2. 10-20-30
3. 50-25-50
4. 20-40-20

9-44. Each security container, vault, or secure room must have a record showing its location and the name, home address, and phone number of which of the following individuals?

1. The security manager only
2. The commanding officer only
3. The responsible custodian of the stored information only
4. All persons having knowledge of the combination

9-45. Which of the following safeguards apply(ies) to the combination of a security container?

1. It must be treated as having a classification equal to the highest category of information stored therein
2. It must be marked appropriately on any written record
3. It shall be stored in a security container other than the one to which it applies
4. All of the above

9-46. What authority governs key security and lock control?

1. OPNAVINST 5530.1B
2. SECNAVINST 5510.36
3. OPNAVINST 5530.14C
4. SECNAVINST 5510.30A

9-47. To secure a classified container, you must rotate the dial of the combination lock a minimum of how many times in the same direction?

1. Five
2. Two
3. Three
4. Four

9-48. A civilian locksmith who has no security clearance but is continuously escorted while in the security area may perform which of the following services on a security container?

1. Neutralize a lock-out
2. Repair a locking drawer
3. Both 1 and 2 above
4. Change the combination

9-49. In reference to an intrusion detection system in an area where classified information is stored, what statement is NOT true?

1. It complements other physical security measures
2. It prevents an attempted intrusion
3. It provides additional controls at vital areas
4. It may provide a more economical and efficient substitute for other protective measures

9-50. When purchasing a new shredder, you may select either a cross-cut or a strip shredder.

1. True
2. False

9-51. When classified information is shredded, what should be the maximum width of the strip?

1. 1/32 inch
2. 1/16 inch
3. 1/64 inch
4. 3/64 inch

9-52. A wet process pulper is capable of destroying which of the following materials?

1. Typewriter ribbons
2. Microforms
3. Paper products
4. All of the above

9-53. How many witness signatures are required on a TS destruction record?

1. One
2. Two
3. Three
4. Four

9-54. TS records of destruction shall be retained for what minimum number of years?

1. Two
2. Three
3. Four
4. Five

9-55. Unclassified NNPI may be destroyed in the same manner as FOUO information.

1. True
2. False

9-56. When the commanding officer of a U.S. Navy ship transfers classified information to a friendly foreign government, what SECNAV instruction is the source of guidance?

1. 5510.36
2 5510.34
3 5510.48J
4. 5530.14C

# ASSIGNMENT 10

Textbook Assignment: ***Department of the Navy Information Security Program Regulation, SECNAVINST 5510.36,*** "Dissemination," chapter 8, pages 8-1 through 8B-1; "Transmission and Transportation," chapter 9, pages 9-1 through 9A-6; and "Loss or Compromise of Classified Information," chapter 12, pages 12-1 through 12-11.

---

***LEARNING OBJECTIVE***: *Recognize the policy and procedures for dissemination of classified and controlled unclassified information, including the procedures for assigning distribution statements on technical documents and review requirements*

10-1. Authority for disclosure of classified information to foreign governments has been centralized in what office?

1. Security manager
2. Director, Navy IPO
3. ASD(PA)
4. TSCO

10-2. DoD departments and agencies may disseminate Secret and Confidential information to each other unless specifically prohibited by the originator.

1. True
2. False

10-3. Transmission through NATO channels is required when disseminating DON documents that incorporate NATO information.

1. True
2. False

10-4. FOUO information may NOT be disseminated within DoD components and between officials of the DoD components.

1. True
2. False

10-5. DEA sensitive information in the possession of the DoD shall be released outside the DoD only with authorization from what entity?

1. Navy IPO
2. CNO (N09N2)
3. DEA
4. Security manager

10-6. Commands which generate technical documents shall notify DTIC and other information repositories when classification markings, export control statements, or distribution statements are changed.

1. True
2. False

10-7. The author of a paper about a new naval weapon is required to submit the information for review and clearance prior to publishing.

1. True
2. False

10-8. A technical paper, written with the potential of becoming an item of national or international interest, has to be reviewed by ASD(PA) via the CNO (N09N2) prior to public release.

1. True
2. False

10-9. What information shares the same policies and procedures for dissemination as those used for FOUO?

1. DOS SBU
2. DEA sensitive
3. RD
4. SAPs

10-10. All newly generated DoD unclassified technical documents shall be assigned one of the distribution statements listed in Chapter 8 of SECNAVINST 5510.36.

1. True
2. False

10-11. The author of a technical document assigned Distribution Statement A can provide a copy of the document to a foreign national.

1. True
2. False

10-12. Which of the following Distribution Statements is assigned to documents containing export-controlled technical data?

1. Distribution Statement G
2. Distribution Statement A
3. Distribution Statement E
4. Distribution Statement B

10-13. A classified technical document may be assigned Distribution Statement X.

1. True
2. False

10-14. When a classified document is assigned Distribution Statement F and is then declassified, that distribution statement shall be retained until specifically changed or removed by the originating command.

1. True
2. False

***LEARNING OBJECTIVE***: *Identify methods approved for the transmission and transportation of classified information and requirements for transmitting and transporting special types of classified and controlled unclassified information.*

10-15. What must the commanding officer do when classified material is to be transmitted or transported?

1. Ensure that only appropriately cleared personnel discharge these responsibilities
2. Select a means that would minimize the risk of a loss or compromise
3. Permit the use of the most cost effective mode of conveyance
4. All of the above

10-16. How do all transfers of U.S. classified information to a foreign government take place?

1. By cleared DOE contractors
2. Through government-to-government channels
3. Through the International Security Document Transfer Program
4. By USPS Certified Mail Only

10-17. U.S. TS information is transmitted or transported by which of the following means?

1. By direct contact between appropriately cleared U.S. personnel
2. By the Defense Courier Service
3. By the DOS Diplomatic Courier Service
4. All of the above

10-18. U.S. Secret information is transmitted or transported by which of the following means?

1. By USPS Registered Mail within and between the U.S. and its territories
2. By Canadian Royal Mail Service
3. By USPS Certified Mail
4. All of the above

10-19. U.S. Confidential information is transmitted or transported by which of the following means?

1. Via an approved carrier that provides courier service
2. By USPS first class mail in the U.S. and its territories
3. By UPS express mail service plus
4. All of the above

10-20. NATO RESTRICTED information is transmitted by which of the following means?

1. By USPS certified mail
2. By USPS first class mail within CONUS
3. By USPS second class mail
4. By UPS express mail service plus

10-21. FOUO information is transported by which of the following means?

1. By USPS certified mail
2. By USPS first class or standard mail
3. By USPS parcel post
4. By U.S. registered mail

10-22. How is Foreign Government RESTRICTED and unclassified information provided "in confidence" transmitted or transported?

1. By a method approved for classified information
2. By UPS express mail service
3. By International Program Office mail
4. By USPS registered mail

10-23. Classified telephone conversations are permitted only under which of the following circumstances?

1. If you have verified the security clearance of the military or civilian personnel you are calling
2. If it's an emergency and not cost effective to travel
3. Over satellite communications circuits
4. Over secure communications circuits approved for the classification level of the information to be discussed

10-24. Classified information is prepared for shipment by following which of the following procedures?

1. Packaging and sealing it with tape which will retain the impression of any postal stamp
2. Packaging to minimize risk of accidental exposure or undetected deliberate compromise
3. Packaging so that classified text is not in direct contact with the inner envelope or container
4. All of the above

10-25. How is classified information transported outside the command enclosed?

1. In an opaque envelope
2. In a cardboard box
3. In two opaque envelopes, wrappings, or containers
4. In wrapping paper

10-26. How are outer envelopes or containers of classified information addressed?

1. An official U.S. Government activity only
2. Cleared DoD contractor facility only
3. Either an official U.S. Government activity or cleared DoD contractor facility
4. The command designee

10-27. What are inner envelopes or containers of classified information addressed with?

1. The address of the recipient
2. The address of the sender
3. The highest classification level and applicable warning notices or intelligence control caveats of the contents
4. All of the above

10-28. The USPS Express Mail envelope may serve as an outer wrapper for classified information.

1. True
2. False

10-29. The delivery envelope of the current holder of the GSA contract for overnight delivery may NOT be used as the outer wrapper.

1. True
2. False

10-30. Receipting is required when classified information is transferred in which of the following cases?

1. For all classified packages handcarried to the U.S. Senate
2. For all classified information provided to a foreign government or its representatives
3. For TS and Secret information transmitted or transported in and out of the command
4. All of the above

10-31. When classified information is escorted or handcarried within the command, it must be covered to prevent inadvertent disclosure.

1. True
2. False

10-32. Which of the following authorities are authorized to approve escorting or handcarrying of classified information aboard commercial aircraft traveling outside the U.S., its territories, and Canada?

1. Second echelon commands
2. All commanding officers
3. All security managers
4. All administrative officers

10-33. Which of the following instructions must be given to couriers escorting or handcarrying classified information?

1. That the information is never to be left unattended
2. That the information is never to be discussed or disclosed in a public place or conveyance
3. That the information may not be stored overnight in hotel rooms or vehicles
4. All of the above

10-34. Which of the following written authorizations may be used to identify appropriately cleared DoD military and civilian personnel approved to escort or handcarry classified information?

1. DD 2501
2. Official travel orders
3. Visit requests
4. All of the above

10-35. The DD 2501 must have an expiration date not to exceed 2 years from the date of issue.

1. True
2. False

10-36. How is classified information or material approved for release to a foreign government transmitted or transferred?

1. Delivered or transmitted only to a person designated, in writing, by the recipient government
2. Transferred only by a foreign embassy representative of each government
3. Transmitted only by Navy IPO
4. Transmitted by a foreign disclosure office only

10-37. In most cases, U.S. classified material delivered to a foreign government within the recipient country shall be delivered on arrival, in the recipient country, to a U.S. Government representative, who shall arrange for its transfer to a designated representative of the recipient government.

1. True
2. False

10-38. Overseas shipments of U.S. classified material shall be made only via which of the following ships, aircraft, or other carriers?

1. Those owned or chartered by the U.S. Government or under U.S. registry
2. Those owned or chartered by or under the registry of the recipient government
3. Those otherwise authorized by the head of the DoD component who has classification jurisdiction over the classified material involved
4. All of the above

10-39. In any FMS case, the foreign recipient is exclusively responsible for developing a transportation plan for the DoD component having security cognizance over the classified material involved.

1. True
2. False

10-40. A contractor should prepare a transportation plan for each commercial contract, subcontract, and other legally binding arrangement providing for the transfer of classified freight to foreign governments, to be moved by truck, rail, aircraft, or ship.

1. True
2. False

10-41. The requirement for a transportation plan applies to all U.S. and foreign classified and unclassified contracts.

1. True
2. False

***LEARNING OBJECTIVE***: *Recognize the policy and procedures for reporting and investigating incidents of loss or compromise of classified information.*

10-42. When an individual becomes aware that classified information is lost or compromised, what shall he or she immediately do?

1. Notify the commanding officer or security manager
2. Notify the local PAO
3. Start a Preliminary Inquiry
4. All of the above

10-43. The commanding officer should appoint the security manager to conduct a PI.

1. True
2. False

10-44. After notification that a compromise of classified information may have occurred at his or her command, which involves a foreign intelligence service, the CO should report this important counterintelligence information to which of the following authorities?

1. Director, ODUSDP(PS)
2. CNO (N2)
3. Local NCIS office
4. FBI

10-45. The "initial report," required by the CMS-1A for reporting the loss of COMSEC information or keying material, satisfies the requirement for a PI, provided copies are sent to CNO (N09N2), NSA, and the local NCIS office.

1. True
2. False

10-46. Whenever serious disciplinary action or prosecution is contemplated against any person(s) believed responsible for the compromise of classified information, a formal classification review shall be coordinated with CNO (N09N2), NCIS and OJAG (Code 11).

1. True
2. False

10-47. An NCIS ROI shall NOT be made part of a JAGMAN investigation involving the loss or compromise of classified information.

1. True
2. False

10-48. A formal damage assessment is a brief impact statement on the harm to the national security caused by a compromise of classified information.

1. True
2. False

10-49. Upon becoming aware that classified or unclassified information is unofficially released to the public, an individual or command should immediately notify which of the following authorities?

1. SECNAV
2. CNO (N09N2)
3. CNO (N2)
4. FBI

10-50. Losses or compromises involving RD are reported to what authority?

1. CNO (N09N2)
2. JCS
3. CNO (N89)
4. SECNAV

10-51. What is the initial process to determine the facts surrounding a possible loss or compromise?

1. A JAGMAN investigation
2. An initial report
3. A Preliminary Inquiry
4. A security review

10-52. Upon completion of the JAGMAN investigation, the convening command shall forward the completed investigation to the Director of Naval Intelligence.

1. True
2. False

10-53. What characterizes a formal damage assessment?

1. It is always unclassified
2. It is long-term
3. It is post-prosecutorial
4. Both 2 and 3 above

10-54. Losses or compromises involving SIOP and SIOP-ESI are reported to which of the following authorities?

1. NFIB, FBI, and CNO (N09)
2. CNO (N2) and OASD
3. SECNAV and CNO (N64)
4. JCS and USCINCSTRAT

10-55. What do we call the unofficial release of DoD classified information to the public (e.g., via newspaper, books, radio, TV, or Internet) which results in an unauthorized disclosure?

1. Compromise "de facto"
2. Public media compromise
3. Nondisclosure
4. All of the above

# ASSIGNMENT 11

Textbook Assignment: ***Department of the Navy Information Security Program Regulation, SECNAVINST 5510.36,*** "Industrial Security Program," chapter 11, pages 11-1 through 11-12.

---

***LEARNING OBJECTIVE***: *Recognize the requirements of a command industrial security program, including restrictions and safeguards mandated to protect classified information and special classes of information.*

11-1. What command official is responsible for establishing an industrial security program, when necessary?

1. The security manager
2. The security officer
3. The commanding officer
4. The SSO

11-2. Command security procedures shall include guidance regarding the safeguarding of classified information released to industry.

1. True
2. False

11-3. What instruction establishes policy for the acquisition system protection program?

1. SECNAVINST 5510.30A
2. SECNAVINST 5510.34
3. SECNAVINST 5510.36
4. DoD Directive 5200.1-M

11-4. What is required with the acquisition of classified defense systems?

1. Program Protection Survey
2. Program Protection Plan
3. Risk Syllabus
4. Technology Maturation Plan

11-5. By what means are security requirements levied on contractors if not conveyed in the contract document?

1. DoD 5220.22-M
2. DD 1540
3. DD 254
4. DD 2345

11-6. What E.O. established the NISP?

1. E.O. 12958
2. E.O. 12829
3. E.O. 12933
4. E.O. 12968

11-7. The purpose of the NISP is to safeguard classified information released to industry.

1. True
2. False

11-8. What regulation implements the NISP within the DON?

1. SECNAVINST 5510.30A
2. SECNAVINST 5510.34
3. SECNAVINST 5510.36
4. SECNAVINST 5530.14C

11-9. What authority governs the policy for safeguarding of classified information to cleared DoD contractors?

1. DoD 5200.1R
2. DoD 5220.22-M
3. DoD 5220.3
4. DoD 5200.1-M

11-10. What authority governs the protection of special classes of information?

1. DoD Directive 5200.1-M
2. DoD 5220.22-M
3. DoD 5220.22-M. Supp 1
4. SECNAVINST 5510.36

11-11. The CNO (N09N2) is responsible for implementing the NISP within the industrial community.

1. True
2. False

11-12. What element of the DSS provides administrative assistance and policy guidance to cleared DoD contractors?

1. Cognizant Security Agency
2. Operating Locations
3. Operating Center Columbus
4. Cognizant Security Office

11-13. What authority is responsible for granting personnel security clearances to contractors when access to classified information is required?

1. SECDEF
2. SECNAV
3. DSS Operations Center Columbus
4. Defense Office of Hearing and Appeals

11-14. Cleared DoD contractors are exempt from submitting visit requests for classified visits to a ship.

1. True
2. False

11-15. A contractor engaging in classified procurement is required to have an FCL.

1. True
2. False

11-16. When a contractor is a tenant on a command, which of the following options does the commanding officer have in providing oversight?

1. Requests, in writing, that DSS OCC grant the contractor an FCL and that DSS assume security oversight
2. Requests, in writing, that DSS grant the contractor an FCL and the command retain security oversight
3. Determines that an FCL is not required
4. All of the above

11-17. Cleared DoD contractors who are short-term visitors do NOT have to conform with command security regulations.

1. True
2. False

11-18. When a contractor is physically located overseas, the cognizant DSS Operating Location issues the contractor's facility clearance.

1. True
2. False

11-19. When a command awards a classified contract and actual performance of the contractor is at another location, the awarding command should provide which of the following documents to the host command?

1. Notification of contract award
2. Copy of the DD 254
3. Other pertinent documents
4. All of the above

11-20. Commanding officers may NOT provide security oversight over cleared DoD contractors overseas.

1. True
2. False

***LEARNING OBJECTIVE***: *Identify administration requirements relating to contractor facility clearances and contractor access to classified information and intelligence.*

11-21. The FAD program assists commands in making trustworthiness determinations on contractor employees and may be used for access to classified information.

1. True
2. False

11-22. For which of the following services may commanding officers employ the FAD program?

1. Unclassified contracts
2. Janitorial services
3. Equipment maintenance
4. All of the above

11-23. A "Contract Security Classification Specification," DD 254 and its attachments, shall be issued for all classified contracts.

1. True
2. False

11-24. What individual is authorized to sign a DD 254?

1. A qualified security assistant
2. The COR
3. The program manager
4. The contract monitor

11-25. The Government provides classification guidance to the contractor primarily through what specification?

1. DD 1540
2. DD 254
3. DD 2345
4. DD 2301

11-26. How often is a revised DD 254 issued?

1. Annually
2. Biannually
3. Upon changes in security requirements
4. On final delivery

11-27. A COR has which of the following responsibilities?

1. To verify facility clearances and storage capability prior to release of classified information to contractor facilities
2. To validate security classification guidance, complete, and sign the DD 254
3. To validate justification for Interim Top Secret personnel security clearances and facility security clearances
4. All of the above

11-28. When a cleared contractor's facility clearance requires upgrading or revalidating, who submits the written request to DSS OCC?

1. The facility security officer
2. The cognizant contracting command
3. The security officer
4. The DSS representative

11-29. It is permissible for a cleared DoD contractor to handcarry his/her personal visit request.

1. True
2. False

11-30. Who is responsible for determining the need-to-know of a cleared DoD contractor making a classified visit?

1. The COR
2. The security manager
3. The program manager
4. The individual disclosing classified information

11-31. What individual has final approval of a contractor visit request?

1. The security manager
2. The commanding officer
3. The program manager
4. The COR

11-32. Which of the following authorities is responsible for issuing facility security clearances?

1. The DSS Chief Operating Officer
2. The appropriate DSS OPLOC
3. The DSS OCC
4. The DSS CVA

11-33. Which of the following authorities issues interim Secret or Confidential facility security clearances?

1. DISCO
2. TSCO
3. DSS OCC
4. DSS CVA

11-34. Which of the following officials is responsible for validating requests for Interim TS facility security clearances for contractors?

1. The facility security officer
2. The commanding officer
3. The TSCO
4. The contracting officer's representative

11-35. What official has the responsibility for briefing cleared DoD contractors on their responsibility to safeguard classified information?

1. The program manager
2. The security manager
3. The COR
4. The facility security officer

11-36. During travel, classified information may be secured in a locked briefcase and stored in the baggage compartment of a commercial carrier.

1. True
2. False

11-37. Which of the following authorities must formally approve the use of the GSA commercial contract carrier for cleared DoD contractors?

1. DSS Headquarters
2. Defense Office of Hearings and Appeals
3. DSS Operating Location
4. DoD

11-38. Classified information may only be disclosed to contractors cleared under what program?

1. DISP
2. DSS CVA
3. NISP
4. FAD

11-39. Cleared contractors are authorized the use of the GSA commercial contract carrier to transmit Top Secret information within CONUS.

1. True
2. False

11-40. Which of the following security elements must be in place when a cleared DoD contractor has physical custody of classified information at the facility?

1. A valid facility security clearance
2. Storage capability
3. Both 1 and 2 above
4. A transportation plan

11-41. Which of the following authorities provides written verification of a contractor's level of facility clearance and storage capability?

1. DISCO
2. DSS Headquarters
3. DSS CVA or the contractor's OPLOC
4. CNO (N09N2)

11-42. Classified information provided to cleared DoD contractors performing overseas may be stored in a host government military installation if a U.S. Government-controlled facility or military installation is not available.

1. True
2. False

11-43. Which of the following items should be furnished to the overseas installation commander and the DSS Operating Location with regard to contract performance overseas?

1. A copy of the DD 254
2. Transmission and disposition instructions
3. Storage requirements
4. All of the above

11-44. What is required prior to allowing access to U.S. classified information in joint contracts with NATO activities or foreign governments under agreement with the U.S.?

1. A Security Servicing Agreement
2. A Technical Data Agreement
3. The assurance of foreign employee's clearance level
4. A Foreign Disclosure Agreement

11-45. Which of the following DD forms certifies individuals and enterprises to receive unclassified export-controlled technical data?

1. DD 1540
2. DD 2345
3. DD 254
4. DD 2501

11-46. Intelligence information may be released to cleared DoD contractors if it falls within the scope of the contract.

1. True
2. False

11-47. Which of the following authorities is responsible for sanitizing and coordinating the release of intelligence to a cleared DoD contractor?

1. CNO (N09N2)
2. The DSS Operating Location
3. ONI
4. The releasing command

11-48. Commands are NOT required to keep records of intelligence information released to cleared DoD contractors if the information is contract specific.

1. True
2. False

11-49. What authority is responsible for executing the policy and procedures governing the release of intelligence information to cleared DoD contractors?

1. CNO (N09N2)
2. ONI (ONI-5)
3. CNO (N2)
4. CNO (N89)

11-50. A foreign national or immigrant alien who possesses an LAA may have access to intelligence information without prior approval from ONI-5.

1. True
2. False

11-51. The command must obtain the consent of the originator prior to releasing intelligence information marked for special handling in specific dissemination channels to cleared contractors.

1. True
2. False