



DoD Annual Security Refresher Briefing

**Presented by the
Specialty Systems, Inc.
Corporate Security Office**

2021

SSI's Obligation



SSI Headquarters

As a cleared defense contractor, SSI has an obligation under Executive Order (EO) 12829 and Department of Defense (DoD) Directives to provide its cleared employees with relevant security briefings.

These annual briefings are consistent with your work assignment and requirements established by the National Industrial Security Program Operating Manual (NISPOM).

Expectations



At the conclusion of this briefing, you will complete a proficiency check that will test how well you understand the topics presented.

After passing the proficiency check, you will be able to print a certificate verifying completion of this annual briefing, and your understanding of your duties and responsibilities as a SSI employee who possesses a security clearance.

Lesson 1

Cleared Contractor Requirements

Objectives:

After you complete this lesson, you will be able to:

- Describe the obligations that SSI has to the U.S. Government in order to work with classified information.
- Identify the purpose of the DD Form 254 and security classification guide.



Lesson 1

Cleared Contractor Requirements

Prerequisites for access to Classified



The first requirement was SSI's execution of a Security Agreement with the Department of Defense. This legal agreement requires SSI to abide by current and future security directives issued by the DoD. By signing this agreement, SSI was authorized to work on classified contracts.



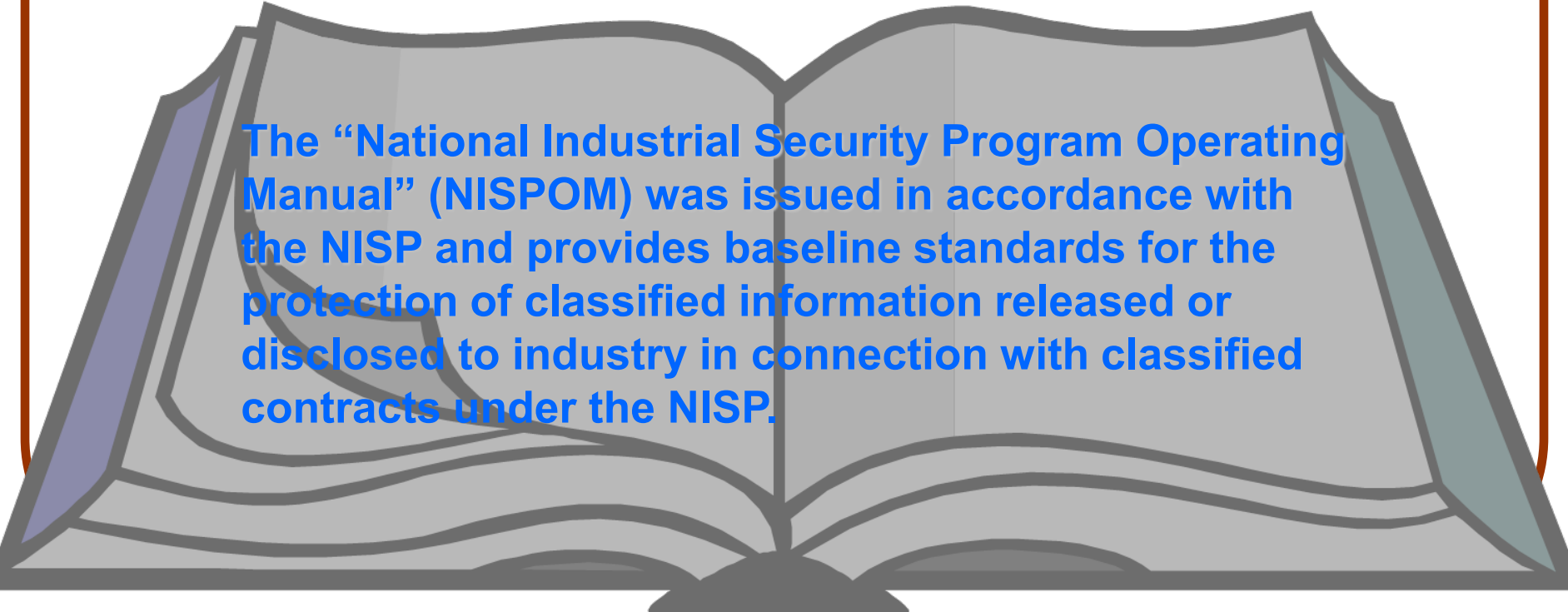
The second requirement was the award of a contract that required access to U.S. Government classified information. It is the awarding of a classified contract that allows SSI and its employees access to classified information.

Lesson 1

Cleared Contractor Requirements

National Industrial Security Program (NISP)

Established by Executive Order 12829 on 6 January 1993, the NISP prescribes requirements, restrictions, and other safeguards that are necessary to prevent unauthorized disclosure of classified information.



The “National Industrial Security Program Operating Manual” (NISPOM) was issued in accordance with the NISP and provides baseline standards for the protection of classified information released or disclosed to industry in connection with classified contracts under the NISP.

Lesson 1

Cleared Contractor Requirements

NISPOM Compliance

The Defense Security Service (DSS) has been designated by the DoD to provide oversight and ensure compliance with Security requirements in the NISPOM.

DSS conducts annual security reviews to evaluate SSI's ability to secure and protect U.S. Government classified material.

A marginal or unsatisfactory rating indicates a substandard security program. It may have detrimental consequences on SSI's ability to work on classified projects and could negatively affect its business. In addition, failure to properly comply with NISPOM requirements could adversely impact National Security.

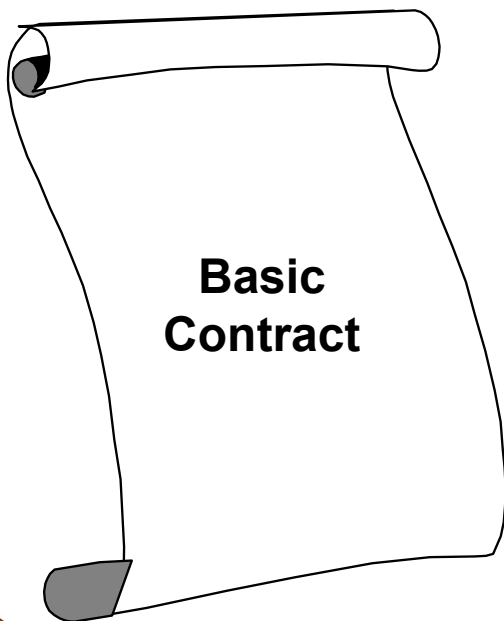


Lesson 1

Cleared Contractor Requirements

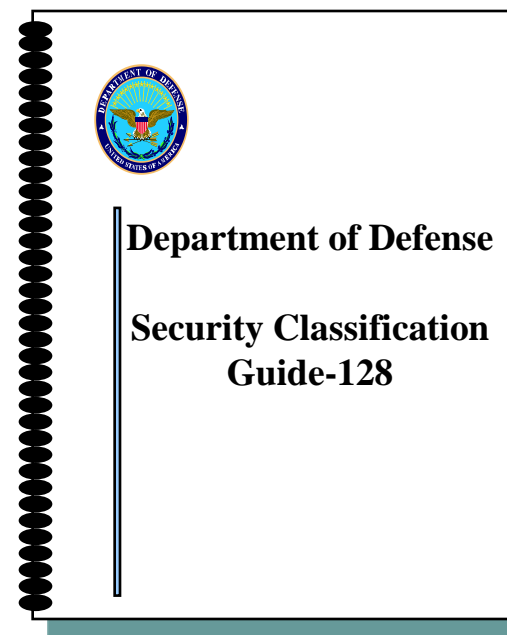
Security Classification Guidance

For all classified contracts, the Government Contracting Activity (GCA) provides appropriate classification guidance. The following documents are used to communicate security requirements:



DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION (The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort)		1. CLEARANCE AND SCHEDULING 1. FACILITY/PERSONNEL REQUIREMENTS	
2. THIS SPECIFICATION IS FOR: (If not complete or applicable)		3. THIS SPECIFICATION IS: (If not complete or applicable)	
A. THIS CONTRACT NUMBER:		A. ORIGIN (Complete date in all cases) DATE (2755MMCC)	
B. SOLICITATION OR OTHER NUMBER: (SEE DATE 2755MMCC)		B. REVISION: (Complete date of publication) DATE (2755MMCC)	
C. RRAL (Complete date in all cases) DATE (2755MMCC)		C. RRAL (Complete date in all cases) DATE (2755MMCC)	
4. IS THIS A FOLLOW-ON CONTRACT? YES <input type="checkbox"/> NO <input type="checkbox"/> IF YES, complete the following: (Priority Contract Number) is transferred to the follow-on contract.		E. YES: (Complete the following) (Priority Contract Number) is transferred to the follow-on contract.	
5. IS THIS A RRAL DO FORM 254? YES <input type="checkbox"/> NO <input type="checkbox"/> IF YES, complete the following: (Priority Contract Number) is transferred to the follow-on contract.		E. YES: (Complete the following) (Priority Contract Number) is transferred to the follow-on contract.	
6. CONTRACTOR (Include Commercial and Government Entity CASE) Code:		C. COORDINATE SECURITY OFFICE (Name, Address, and Zip Code)	
A. NAME, ADDRESS, AND ZIP CODE:		A. DATE CODE	
7. SUB-CONTRACTOR		C. COORDINATE SECURITY OFFICE (Name, Address, and Zip Code)	
A. NAME, ADDRESS, AND ZIP CODE:		A. DATE CODE	
8. ACTUAL PERFORMANCE:		C. COORDINATE SECURITY OFFICE (Name, Address, and Zip Code)	
A. LOCATION:		A. DATE CODE	
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT			
10. CONTRACTOR WILL REQUIRE ACCESS TO:		11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:	
A. COMMUNICATIONS SECURITY SYSTEMS INFORMATION		A. PERSONNEL SECURITY (PERSONNEL SECURITY REQUIREMENTS)	
B. INFORMATION SECURITY INFORMATION		B. INFORMATION SECURITY (PERSONNEL SECURITY REQUIREMENTS)	
C. SPECIAL ACCESS INFORMATION		C. SPECIAL ACCESS INFORMATION	
D. OTHER (Specify):		D. OTHER (Specify):	

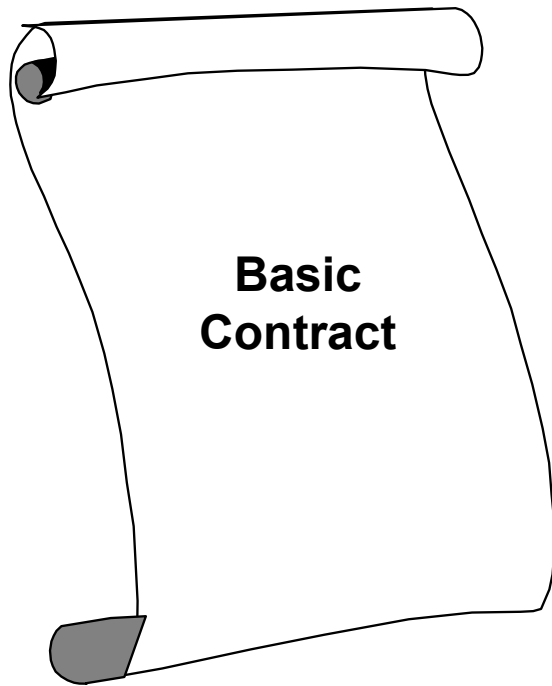
DD FORM 254, DEC 1999 PREVIOUS EDITIONS ARE OBSOLETE.



Lesson 1

Cleared Contractor Requirements

The Basic Contract



- Identifies all clauses applicable to the contract, some of which may address security requirements.
- Mandates compliance with the NISPOM, if the contract is classified.
- Incorporates the DD Form 254 as part of the contract.
- Specifies other security requirements that may or may not be incorporated in other contract documentation.

Lesson 1

Cleared Contractor Requirements

DD Form 254 Contract Security Classification Specification

The DD Form 254 is issued with each contract that requires access to and/or generation of classified information or material. The DD Form 254:

- Identifies the highest level of facility clearance and safeguarding capability required to perform on the contract.
- Indicates access and security requirements for the contract.
- Must be flowed down by SSI to a subcontractor when the effort will involve access to and/or generation of classified material.

DEPARTMENT OF DEFENSE CONTRACT SECURITY CLASSIFICATION SPECIFICATION <small>(The requirements of the DoD Industrial Security Manual apply to all security aspects of this effort.)</small>		1. FACILITY CLEARANCE REQUIRED	
		a. SECRET	
		b. LEVEL OF SAFEGUARDING REQUIRED	
		SECRET	
2. THIS SPECIFICATION IS FOR: (If and complete as applicable)			
a. THIS CONTRACT NUMBER: DASG60-00-C-0072		b. ORIGINAL (Complete date if of contract) DATE: 07/19/00	
b. SUBCONTRACT NUMBER:		k. REVISION: Supplemental (Indicate space)	
c. SOLICITATION OR OTHER NUMBER:		c. TRIAL (Complete date if of contract) DATE: 07/19/00	
4. IS THIS A FOLLOW-ON CONTRACT? <input type="checkbox"/> YES <input type="checkbox"/> NO. If Yes, complete the following: Classified material received generated solely (Indicate Contract Number) is transferred to this follow-on contract.			
5. IS THIS A RIVAL DD FORM 254? <input type="checkbox"/> YES <input type="checkbox"/> NO. If Yes, complete the following: In response to contractor's request dated (Indicate date) reference of the classified material is authorized for the period of _____			
6. CONTRACTOR (Include Government and Government Entity (GAE) Code) NAME, ADDRESS, AND ZIP CODE Raytheon Company 350 Lowell Street Andover, MA 01810		b. GAE CODE	c. COMINT SECURITY OFFICE (Name, Address, and Zip Code) Defense Security Service 187 Ballardsville St. Suite B 205 Wilmington, MA 01887
7. SUBCONTRACTOR NAME, ADDRESS, AND ZIP CODE		b. GAE CODE	c. COMINT SECURITY OFFICE (Name, Address, and Zip Code)
8. ACTUAL PERFORMANCE LOCATION		b. GAE CODE	c. COMINT SECURITY OFFICE (Name, Address, and Zip Code)
9. GENERAL IDENTIFICATION OF THIS PROCUREMENT			
10. CONTRACTOR WILL REQUIRE ACCESS TO:			
11. IN PERFORMING THIS CONTRACT, THE CONTRACTOR WILL:			
a. COMINT SECURITY (COMINT) INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	a. REPRODUCTION OF CLASSIFIED INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
b. RESTRICTED DATA	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	b. RECEIVE CLASSIFIED DOCUMENTS ONLY	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
c. CRITICAL NUCLEAR REACTOR DESIGN INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	c. RECEIVE AND GENERATE CLASSIFIED MATERIAL	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
d. FORMERLY RESTRICTED DATA	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	d. FABRICATE, REPRODUCE, OR STORE CLASSIFIED HARDWARE	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
e. INTELLIGENCE INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	e. REPRODUCE INFORMATION ONLY	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
f. SPECIAL ACCESS INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	f. TAKE ACCESS TO THE CONTRACTOR WORKSPACE OUTSIDE THE U.S.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
g. INFO INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	g. TAKE ACCESS TO THE CONTRACTOR WORKSPACE OUTSIDE THE U.S.	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
h. FOREIGN DISSEM INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	h. HAVE OPERATIONS SECURITY (OS) REQUIREMENTS	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
i. LIMITED DISSEM INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	i. BE AUTHORIZED TO USE THE DEFENSE LOGON SERVICE	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
j. JOB OFFICIAL USE ONLY INFORMATION	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO	j. OTHER (Specify)	
k. OTHER (Specify)			

DD FORM 254, DEC 1999 PREVIOUS EDITION IS OBSOLETE.

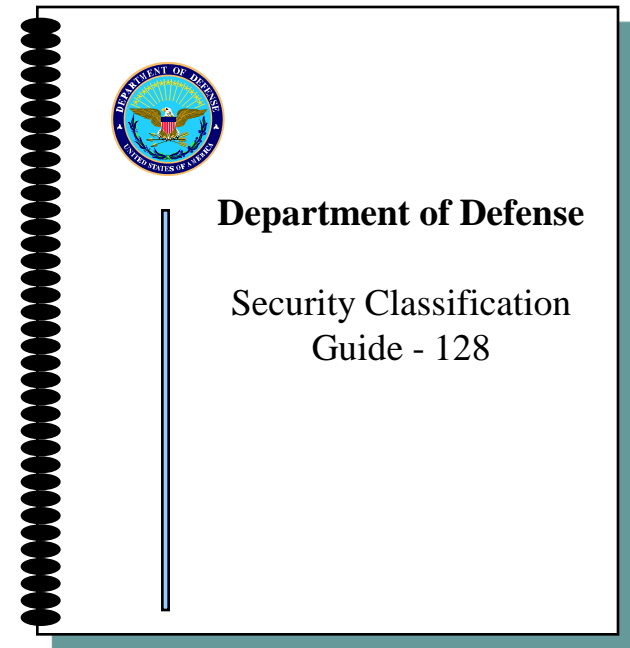
Lesson 1

Cleared Contractor Requirements

Security Classification Guide

A Security Classification Guide (SCG) is provided by the original government classifying authority. The SCG:

- Is part of the DD Form 254.
- Identifies what information or material is classified.
- Identifies the level of classification of the information.
- Identifies downgrading, declassification or exemption instructions.
- All program personnel are obligated to read the their program classification guidance to know what is classified about the program they work on.



Lesson 1

Cleared Contractor Requirements

Public Disclosure of Defense Information

Employees must not disclose classified or unclassified contract information pertaining to a contract to the public without prior review and approval as specified in the DD Form 254.

Disclosing contract information to the public includes:

- Articles submitted for technical journals and books.
- Lectures and presentations made at symposiums.
- Marketing literature prepared for general or specific purpose release.
- Presentations at trade shows and job fairs.
- Dissertations/theses developed in pursuit of advanced degrees.
- Any other method of release to the public domain.

Review SSI Policy and Procedure 5-111 and obtain internal approval for public release.

Lesson 1 Summary

Cleared Contractor Requirements



By signing the Security Agreement, SSI made a commitment to follow the security guidelines, procedures, and requirements for handling classified information, as defined by the DoD. The Defense Security Service (DSS) has been designated by the DoD to provide oversight and ensure compliance with Security requirements in the NISPOM.

Security classification guidance is provided by the government and can be found in the basic contract, DD Form 254, and security classification guides.

Lesson 1 Review

Cleared Contractor Requirements

The NISP was established to safeguard U.S. Government classified information that is released to contractors.

- True**
- False**

Answer

True.

Executive Order (EO) 12829 (and its predecessor orders) establishes the National Industrial Security Program (NISP). “...This order establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. To promote our national interests, the United States Government issues contracts, licenses and grants to non-government organizations [i.e., SSI]. When these arrangements require access to classified information, the national security requires this information be safeguarded in a manner equivalent to its protection within the executive branch of government.”

“...The national security also requires that our industrial security program promote the economic and technological interests of the United States.”

Excerpts from EO 12829, 6 Jan 1993
Signed by President George Bush

Lesson 1 Review

Cleared Contractor Requirements

In order to perform on classified contracts, SSI was required to execute a legal security agreement with the Department of Defense.

- True**
- False**

Answer

True.

Prior to allowing SSI access to classified information, there were legal and contractual agreements that were established. First, a Department of Defense Security Agreement was executed between the DoD and SSI. This agreement requires SSI to abide by the current and future security directives issued by the DoD. This is a legal, binding contract. By SSI signing this agreement, the DoD has authorized the company to work on classified contracts.

Lesson 1 Review

Cleared Contractor Requirements

The DD Form 254 is officially called the:

- Security Requirements List**
- Contract Security Classification Specification**
- Security Clause**
- None of the Above**

Answer

DD Form 254 Contract Security Classification Specification

The DD Form 254 is issued with each contract that requires access to, or generation of classified information or materials.

Lesson 1 Review

Cleared Contractor Requirements

Any public disclosure of unclassified contract information pertaining to a classified contract must be approved (prior to release) by the provisions of the DD Form 254, or as specified by the Government Contracting Agency.

- True**
- False**

Answer

True.

Public Disclosure of Defense Information

Employees must not disclose classified or unclassified contract information pertaining to a classified contract to the public without prior review and clearance as specified in the DD Form 254, or as otherwise specified by the Government Contracting Agency (GCA).

Lesson 1 Review

Cleared Contractor Requirements

A marginal rating on a security inspection indicates that a facility:

- **Far exceed basic DoD security requirements**
- **Has lost, or is in imminent danger of losing its ability to safeguard information**
- **Has a substandard security program**
- **Is in general conformity with DoD Security requirements**

Answer

Marginal

A Marginal rating indicates a substandard security program. This rating signifies a serious finding in one or more security program areas that could contribute to the eventual compromise of classified information. A compliance review is conducted to assess the actions taken to correct the findings that led to the Marginal rating.

Lesson 2

DoD Classification System



CONFIDENTIAL

TOP SECRET

SECRET

Lesson 2

DoD Classification System

Objectives:

After you complete this lesson, you will be able to:

- Understand that the Non-Disclosure Agreement is a legal binding agreement.
- Identify the three classification levels, and special categories of information.
- Explain original and derivative classification authority.
- Identify the required markings on classified material.



Lesson 2

DoD Classification System

Non-Disclosure Agreement

Before having access to classified information, you were required to sign the Non-Disclosure Agreement (NDA), Standard Form (SF) 312.

The NDA is a legal document between you and the U.S. Government. The NDA states that:

- Any unauthorized disclosure of classified information could cause damage to the U.S. Government and is a violation of the NDA.
- All classified information is the property of the U.S. Government.
- Violations of the NDA may result in a fine, imprisonment, or both.



Lesson 2

DoD Classification System

Classification Levels

Information is classified based on the sensitivity of the material and the amount of damage that would be caused to the national security if the information were compromised. The levels of classification in the United States are:

Top Secret - Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security.

Secret - Unauthorized disclosure could reasonably be expected to cause serious damage to the national security.

Confidential - Unauthorized disclosure could reasonably be expected to cause damage to the national security.

Lesson 2

DoD Classification System

Special Category Information

Some classified information is considered especially sensitive and additional access restrictions and/or handling requirements have been imposed. These categories are:

- North Atlantic Treaty Organization (NATO) information
- Foreign Government Information (FGI)
- Intelligence Information
- Critical Nuclear Weapons Design Information (CNWDI)
- Restricted Data (RD)
- Formerly Restricted Data (FRD)
- Communications Security (COMSEC) & CRYPTO

Lesson 2

DoD Classification System

Original Classification

Executive Order (EO) 12958 states that only selected U.S. Government officials have original classification authority:



- The President of the United States, Agency Heads and officials designated by the President in the Federal Register.
- Other United States Government officials delegated this authority by direction of the President or Agency Head.

Contractors and their employees do not have original classification authority.

Lesson 2

DoD Classification System

Derivative Classification

SSI employees obtain their classification authority through the derivative classification process. Derivative classification means:



- Incorporating, paraphrasing, restating, or generating in new form and marking the newly developed material consistent with the classification markings that apply to the source information.
- Classifying and marking newly generated material in accordance with a security classification guide.

Lesson 2

DoD Classification System

Marking Classified Materials

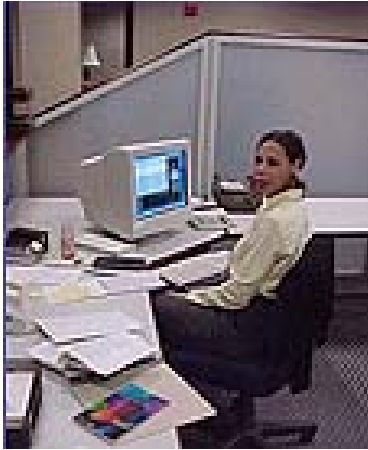
The following basic markings must appear on all classified material:

Overall Classification Marking	SECRET Unclassified Sample
Company Name	Acme Computer Corporation
Cleared Mailing Address	120 Lowell Road Anywhere, MA 01810
Date of Preparation	December 1, 2005
Subject/Title Marking	MEMORANDUM FOR THE DIRECTOR From: David Smith Subject: (U) Funding Problems
Portion Markings	1. (U) This is paragraph 1 and contains unclassified information. Therefore, this portion will be marked with the designation "U" in parentheses. 2. (S) This is paragraph 2 and contains "Secret" information. Therefore, this portion will be marked with the designation "S" in parentheses.
Classification Authority	Derived from: ABC Program SCG, dated 9/20/04
Declassification Instructions	Declassify on: September 21, 2029
	SECRET

Contact your local Security Office for questions on marking and to obtain a guide for marking classified documents.

Lesson 2 Summary

DoD Classification System



The Non-Disclosure Agreement (NDA) is a legal, binding document that prohibits the unauthorized disclosure of classified information.

The U.S. has three levels of classification and information is assigned a level of classification based upon the severity of damage to national security that would result from unauthorized disclosure.

SSI employees classify information based upon derivative rather than original classification authority.

Lesson 2 Review

DoD Classification System

The Non-Disclosure Agreement (NDA) is not a legal contract, rather an acknowledgement that you should abide by DoD security regulations.

- True**
- False**

Answer

False.

Non-Disclosure Agreement

The NDA is legal document between you and the U.S. Government.
The NDA states that:

- Any unauthorized disclosure of classified information could cause damage to the U.S. Government and is a violation of the NDA
- All classified information is the property of the U.S. Government
- Violations of the Non-Disclosure Agreement may result in a fine, imprisonment, or both

Lesson 2 Review

DoD Classification System

The three levels of classified information in the United States are:

- **Confidential, Secret and Top Secret**
- **Secret, Top Secret and FOUO**
- **Secret, Top Secret and SCI/SAP**
- **Top Secret, SCI and Special access Program (SAP)**

Answer

Classification Levels

Top Secret - Information or material the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to national security.

Secret - Information or material the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security.

Confidential - Information or material the unauthorized disclosure of which could be reasonably expected to cause damage to the national security.

Lesson 2 Review

DoD Classification System

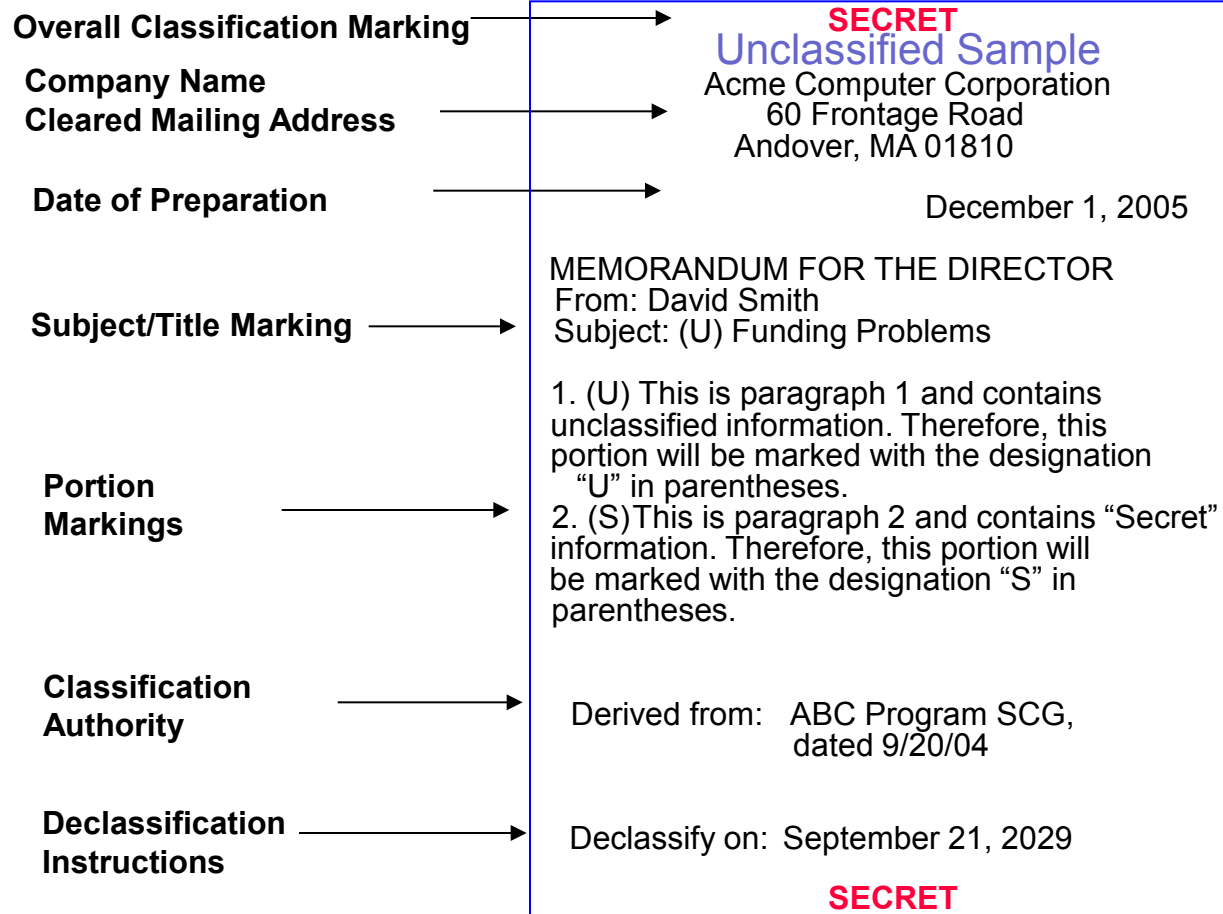
In addition to showing the classification at the top and bottom of each page, a classified document must also:

- Show the authority for the classification decision making the information classified**
- Show declassification instructions or exemption category**
- Be paragraph marked**
- All of the above**

Answer

All of the above

The following basic markings must appear on all classified material:



Lesson 3

Threat Awareness / Defensive Security

Objective:

After you complete this lesson, you will be able to:

- Describe the types of threats to our classified and sensitive information.
- Describe defensive security actions that can be taken to counter those threats.



Lesson 3

Threat Awareness / Defensive Security

The Threat

What is the Threat?

- We must remember that the Foreign Intelligence Service (FIS) networks (including those of “friendly countries”) are worldwide and ever present, and they want our technology.
- Critical technology has never been stolen by force. The FIS obtains information through open sources, friendships, and recruitment of U.S. citizens with access to the information they want.
- The gathering of human intelligence (referred to as “HUMINT”) is the foremost threat, since all espionage recruitment begins with the human element.

Who are the Targets?

- Aerospace and defense industries
- Cleared employees
- Commercial enterprises (economic)



Lesson 3

Threat Awareness / Defensive Security

Foreign Intelligence Threats

Methods of Operation/Techniques:

- Requests for scientific and technological information.
- Solicitation of marketing services.
- Acquisition of U.S. companies and their technologies.
- Blackmail resulting from inappropriate conduct during foreign visits.
- Exploitation of international conventions, seminars, exhibits.
- Exploitation of e-mail and the internet.
- Exploitation of joint ventures and research.
- Exploitation of foreign visits to U.S. facilities.



Lesson 3

Threat Awareness / Defensive Security

Human Intelligence

Who is the Threat?

- Any person who lacks the proper clearance and need-to-know, but still seeks to gain unauthorized access to classified or sensitive information.
- This includes business competitors who need our advanced technology to ensure their economic survival by reducing our competitive edge.

Informed, loyal, and constantly vigilant people are the best defense we have against the loss of our technology and competitive edge.

Lesson 3

Threat Awareness / Defensive Security

Defensive Security Actions

- Actions you can take to reduce or mitigate the risk of espionage include:
- Know and follow good security practices at work, at home, and while on travel.
- Be alert to overly inquisitive people asking about the type of work you do, business information about SSI, or about your personal life.
- Never provide anyone with more information than is absolutely necessary to accomplish your objectives.
- Do not share any contractual, classified, For Official Use Only (FOUO), or SSI proprietary information with anyone who does not have a legitimate need for the information.
- Report any suspected attempts to gain information or other suspicious circumstances to your local Security Office.

Lesson 3 Summary

Threat Awareness / Defensive Security

The threat of espionage against the United States is on the increase as foreign countries struggle to achieve technical and economic parity or superiority in the world.

As a SSI employee, you should be aware of these threats and take defensive security actions to reduce the risk.



Lesson 3 Review

Threat Awareness / Defensive Security

The demise of the Cold War has not reduced the threat of espionage against the United States.

- True**
- False**

Answer

True.

The threat of espionage against the United States is on the increase as foreign countries struggle to achieve parity or technical superiority in the world economy.

As a SSI employee, you should be aware of these threats and take defensive security actions to reduce the risk.

Lesson 4

Employee Reporting Requirements

Objective:

After you complete this lesson, you will be able to:

Identify the requirements to report:

- Events that may impact the status of an employee's personnel clearance (PCL).
- Situations that affect proper safeguarding of classified information.
- Circumstances that indicate classified information has been lost or compromised.



Lesson 4

Employee Reporting Requirements

Reporting Requirements

All cleared SSI employees have the obligation to report the following to their local Security Office:

- Security violations/vulnerabilities.
- Suspicious contacts by anyone attempting to solicit information from you regarding sensitive projects on which you are working, or other information relative to government contracts, company proprietary or competition sensitive information.
- Changes in personal status such as a change in name, marital status (for TS & SAP), citizenship, or job assignment that results in access to classified information no longer being required.
- Espionage, sabotage, subversive and terrorist activities.
- Adverse information. (See next slides for details.)

Lesson 4

Employee Reporting Requirements

Adverse information

Adverse information is defined as "any information that adversely reflects on the integrity or character of a cleared employee that suggests his/her ability to safeguard classified information may be impaired, or that his/her access to classified information may not be in the interest of national security."

SSI managers, supervisors, and employees have the responsibility of reporting to the local Security Office any adverse information which may come to their attention concerning a cleared employee or someone in the process of being cleared. The local Security Office will report factual information to the Defense Security Service for adjudication.

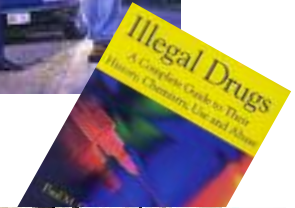
Lesson 4

Employee Reporting Requirements

Adverse Information

Examples :

- Arrests or convictions for criminal offenses, including driving under the influence.
- Financial difficulties, including bankruptcy, excessive indebtedness, and wage garnishments.
- Bizarre or notoriously disgraceful behavior.
- Alcoholism, use of illegal drugs or abuse of legal drugs.
- Emotional or psychological problems requiring treatment or hospitalization.
- Affluence (wealth, acquisitions, investments) beyond known sources of income.
- Membership in organizations which seek to overthrow the government of the United States by unconstitutional means.



Lesson 4 Summary

Employee Reporting Requirements

As a cleared employee, you are responsible for knowing your reporting requirements and for taking the necessary action to report any such circumstances to the Security Office.



Lesson 4 Review

Employee Reporting Requirements

Adverse information is defined as "any information that adversely reflects on the integrity or character of a cleared employee that suggests his/her ability to safeguard classified information may be impaired, or that his/her access to classified information may not be in the interest of national security."

- True**
- False**

Answer

True.

Adverse information is defined as "any information that adversely reflects on the integrity or character of a cleared employee that suggests his/her ability to safeguard classified information may be impaired, or that his/her access to classified information may not be in the interest of national security."

Lesson 5

Your Security Responsibilities

Objectives:

After you complete this lesson, you will be able to:



- Identify procedures for escorted, unescorted and foreign person visitors.
- Describe general safeguarding procedures for classified material.
- Explain general document control procedures.
- Describe **general user responsibilities for processing on a classified** Information System (IS).

Lesson 5

Your Security Responsibilities

General Security Practices

Your work environment, physical location, type of project, and individual job functions play a major role in determining the security procedures and practices to which you must adhere.

The information contained in this section includes those generic practices that every cleared employee must follow, regardless of individual work assignment.



Lesson 5

Your Security Responsibilities

Visitor Control

When hosting visitors, SSI employees must ensure that all government and Company information is protected from unauthorized disclosure.

Unescorted Visitor Badge:

- Visitor is a long term visitor authorized unescorted access to the facility by the SSI host when required for job performance.
- Visitor can come and go within the facility without an escort.
- Citizenship status of the visitor must be verified by Security before the badge is issued.
- Know the requirements to authorize unescorted visitors at your facility.

Lesson 5

Your Security Responsibilities

Visitor Control

Escorted Visitor Badge:

- Visitor has no authorization for unrestricted access to the facility.
- Visitor must be escorted at all times while within the facility.
- Escorting employees must maintain visual and physical control over the visitor.
- Take visitor with this badge to the Security reception area or to find the responsible escort when discovered in the facility without an escort. Notify Security accordingly.



Lesson 5

Your Security Responsibilities

Visitor Control

Foreign Person Visitor Also Receives an Escort
Required Badge:

- Visitor is either a foreign national, a Permanent Resident who cannot provide evidence of such status, or a U.S. Person who is employed by or represents a foreign government or foreign incorporated company.
- A Foreign Person does not have a security clearance.
- A Foreign Person has limited access to the SSI facility under escort only and no access to the SSI computer network
- Visitor must be denied access to export-controlled technology, unless SSI has an appropriate export authorization. Escorting employees must maintain visual and physical control over the visitor.



Lesson 5

Your Security Responsibilities

Foreign Visit Host Responsibilities

Prior to the arrival of the foreign visitor(s), you must:

- Complete a Foreign Visitor Request Form and submit it to the local Import/Export Compliance and/or Security Office for approval.
- Brief all personnel who will escort or meet with the visitors on any restrictions or limitations on information/technology that can be released them and on potential intelligence gathering techniques.
- Ensure that the foreign persons will have no opportunity to access information/technology not specifically approved for the visit by sanitizing the area(s) to be visited.
- Ensure that the foreign persons will be escorted at all times by no fewer than one escort per five visitors.

As a leader in defense technology, SSI and its employees are a target for espionage by both hostile and friendly nations.

Lesson 5

Your Security Responsibilities

Safeguarding Classified Information

- Verify the security clearance and need to know of any employee or visitor who is unknown to you before releasing or disclosing classified information.
- Do not take classified information/material home, to a hotel, or any other uncleared location.
- Memorize the combination of the lock to your safe or Closed Area. If written/recorded on any medium, it becomes classified material which must be properly marked and stored as classified.



When in use, classified material must remain under the continuous physical control of an appropriately cleared individual.

Lesson 5

Your Security Responsibilities

Safeguarding Classified Information

- Always protect the information you are using from unauthorized exposure or release.
- Secure all classified material in an approved security container when not in use.
- Conduct an “end-of-day” security check at the close of each business day to ensure all classified material has been put in a security container and the lock is secured.



Lesson 5

Your Security Responsibilities

Safeguarding Classified Information During an Emergency

- Life Safety is First! Use your best judgment.
- If time permits secure classified material in appropriate container
- If time does not permit:
 - Small amount of classified - take it with you and keep it under your control at all times, do not leave the property. Notify Security As Soon As Possible.
 - Large amount of classified in a Closed Area - Last person out secure the Area with Spin Dial Lock if time allows. Notify Security As Soon As Possible.
 - Large amount of classified out in an open office area - If time allows, place in cabinet, desk, etc. (lock if possible). Notify Security As Soon As Possible.

Lesson 5

Your Security Responsibilities

Document Control



- Process classified material to be transmitted out of the facility through Security's Document Control Center (DCC).
- Obtain approval to hand-carry classified material through your local Security Office and take it to DCC for proper wrapping and receipting.
- Reproduction of classified material must be approved by your local Security Office and must be reproduced only on equipment that has been specifically approved.
- Contact DCC to obtain new accountability numbers when generating and reproducing accountable classified material.
- Hand-carry classified material and classified waste to Security's DCC for destruction.

Lesson 5

Your Security Responsibilities

Retention

Following contract closure/termination, the loss of a proposal, or a no-bid decision, SSI must request retention authority from the customer in order to retain the classified material associated with the effort.

- Respond to any notification to either request retention for or destroy classified material in your custody.



Remember, all classified information is the property of the U.S. Government.

Lesson 5

Your Security Responsibilities

Security Precautions for Cell Phones & Wireless Devices

There are inherent risks in allowing cell phones, Blackberries, PDAs, or two-way transmitters into any area where classified discussions or processing is conducted.

Safeguarding Government classified, For Official Use Only (FOUO), SSI Proprietary, and Competition Sensitive information requires that we mitigate risks associated with wireless devices in areas with classified and/or sensitive information and/or where classified and/or sensitive discussions may be held.

Be aware of classified and sensitive discussions in your vicinity and be vigilant in preventing such information from being transmitted over unsecure communication devices.



Check your local security policy to see which devices are prohibited from your facility or certain areas within your facility.

Lesson 5

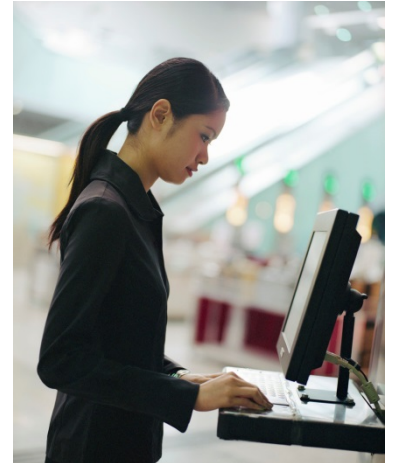
Your Security Responsibilities

Information System (IS) Security

Only Information Systems (IS) that have been certified and accredited may be used to process classified information.

As a user of a classified IS, you must know:

- The programs (contracts) authorized for processing.
- The highest level of classified information which can be processed.
- Hard copy and media handling and marking procedures.
- The required notifications to be made prior to any hardware, software, location, or security-relevant configuration changes.



If you inadvertently process classified information on an unclassified system, notify your local Security Office immediately!

Lesson 5 Summary

Your Security Responsibilities

As a cleared SSI employee, you are responsible for safeguarding classified information and material entrusted to you. In addition, cleared employees must:

- Understand the types of visitor badges and follow the proper guidelines for admitting and escorting visitors .
- Be aware of the functions of the Classified Document Control Center for receipt, dispatch, reproduction and destruction of classified material.
- Ensure that all classified material in your possession **is protected from unauthorized exposure or release.**
- Be familiar with requirements for classified processing on a Information System (IS).

Lesson 5 Review

Your Security Responsibilities

Good employee security practices include:

- Wearing any required badges properly at all times while on SSI or Government property**
- Protecting Government and SSI information from improper disclosure**
- Complying with SSI security policies and procedures**
- All of the above**

Answer

All of the above.

Employee Security Responsibilities

- Always protect the information you are using from unauthorized exposure or release
- Verify the security clearance and need to know before releasing or disclosing classified information to anyone when you cannot personally verify as possessing the requisite clearance and need to know.
- Report any suspicious activity to your supervisor and local security office.
- If you are uncertain about a particular security policy, seek advice from your local security staff.
- If you use a classified computer system, ensure you understand and comply with the security procedures for its operation.
- Wear any required badges at all times on SSI and Government property. Insist others do the same.
- Visitors must be escorted at all times within a SSI facility. Politely challenge those who are not.

Lesson 5 Review

Your Security Responsibilities

All U.S. Government classified information is the property of:

- The contractor facility where the classified contract is being performed**
- SSI if it contains SSI Proprietary information**
- SSI, if developed on a classified contract**
- The U.S. Government**

Answer

The U.S. Government.

It is important to remember that all classified information is the property of the U.S. Government.

SSI can retain classified information only when it has a legitimate need-to-know, as proven by an on-going work effort or government retention authorization.

Following contract closure/termination, the loss of a bid, or a no bid decision, SSI must request retention authority from the customer in order to retain the material.

Lesson 5 Review

Your Security Responsibilities

Employees who notice “Escort Required” visitors not being escorted should:

- Determine where the visitor needs to go and provide directions**
- Locate the Escort or escort the visitor back to the Security reception area**
- Ignore them as the escort probably gave them permission**
- None of the above**

Answer

Employees who notice a visitor with an Escort Required badge not being properly escorted should politely escort the visitor back to the Security reception area or to find the escort.



Congratulations!

**You have successfully completed the
DoD Annual Security Refresher Briefing.**

**Please sign the enclosed
acknowledgement and forward back to
your Facility Security Office**



SSI's Annual Security Refresher Training Attestation

I have received and read the Annual Security Refresher Training for 2021. I am aware and understand that there are requirements that I must meet in order to maintain my security clearance to include: adherence to certain standards of conduct, reporting changes in my personal life that are of security interest, and complying with security regulations and procedures which are used to protect classified information. I also am aware that if I have any questions, need to report any pertinent changes in my personal life, or to report an actual or suspected security violation I should immediately contact SSI's Facility Security Officer.

Signature

Printed Name

Date