



## CS0115-W: Classified Computer Security Training

### Introduction

#### What You Need to Know

#### Classified Information Systems

#### Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

#### Protection Requirements

#### Authorization, Identification, and Authentication

#### Test Your Knowledge

#### Transferring Information

#### What is a File Interchange System?

#### Transferring Information Using File Interchange System

#### Purchase/Reuse of Classified Peripherals

#### Clearing, Sanitizing, and Destroying

#### Marking Hardware, Media, and Output

#### Public Domain and Personally-Owned Software

#### Test Your Knowledge

#### Test

### Introduction to the Course

#### Goal

This training is designed to ensure that you are able to implement proper security procedures on classified information systems so that classified information is protected against unauthorized disclosure or compromise.

This Web training course will take about an hour to complete and is conducted in accordance with NNSA Policy Letter: [NAP-14.1-C](#).

#### Instructions

- A series of topics are presented, followed by an online test. A printable [pdf version](#) of the topics is available.
- You must use a Lab-approved browser in order to take the test, receive a pass or fail confirmation, and have your completion record in LTRAIN.
- You must pass the test with 100% accuracy. You may retake the test as many times as you wish.
- You must acknowledge that you will conduct yourself appropriately when using LLNL computing resources as outlined in the course material. This is referred to as the "Code of Conduct" and is the first statement in the test.

Click on the red arrows in the upper right corner of the page to move forward and backward in the course. Click on the menu titles on the left to move to a specific section.

Section 234B of the Atomic Energy Act of 1954 authorizes the Department of Energy to take enforcement action, under Title 10 CFR Part 824, "Procedural Rules for the Assessment of Civil Penalties for Classified Information Security Violations," against DOE contractors that violate DOE classified information security requirements. DOE's Enforcement Program encourages contractors to identify, report, and correct classified information deficiencies at an early stage, before they contribute to or result in more serious events.



[Privacy & Legal Notice.](#)  
LLNL-PRES-401399

Last updated August 14, 2012

For questions about this course,  
contact [Brenda Janiro](#).



## CS0115-W: Classified Computer Security Training

### Introduction

### What You Need to Know

### Classified Information Systems

### Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

### Protection Requirements

### Authorization, Identification, and Authentication

### Test Your Knowledge

### Transferring Information

### What is a File Interchange System?

### Transferring Information Using File Interchange System

### Purchase/Reuse of Classified Peripherals

### Clearing, Sanitizing, and Destroying

### Marking Hardware, Media, and Output

### Public Domain and Personally-Owned Software

### Test Your Knowledge

### Test

## What You Need to Know

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

- Define a classified information system (IS).
- Identify roles and responsibilities of the key participants in classified information systems security.
- Describe essential classified information systems protection requirements.
- Identify basic classified information system access requirements.
- Understand requirements for transferring information between systems.
- Describe fundamentals of clearing, sanitizing, and destroying classified information system components.
- Follow marking requirements for hardware, media, and output.
- Understand the Laboratory's position on the use of personal and public domain software.
- Accept your responsibilities as stated in the Code of Conduct.



[Privacy & Legal Notice.](#)  
LLNL-PRES-401399

Last updated August 14, 2012

For questions about this course,  
contact [Brenda Janiro](#).



# CS0115-W: Classified Computer Security Training

Introduction  
What You Need to Know

**Classified Information Systems**

Roles and Responsibilities

- User
- ISSO
- System Administrator
- Information System Owner
- OISSO

Protection Requirements

Authorization, Identification, and Authentication

Test Your Knowledge

Transferring Information

What is a File Interchange System?

Transferring Information Using File Interchange System

Purchase/Reuse of Classified Peripherals

Clearing, Sanitizing, and Destroying

Marking Hardware, Media, and Output

Public Domain and Personally-Owned Software

Test Your Knowledge

Test

## Classified Information Systems

Page 1 of 2



The purpose of classified information systems (IS) security is to ensure information processed on a classified IS is protected against unauthorized disclosure or compromise.

### Classified Information

Classified information is sensitive information pertaining to the defense, national security, and foreign relations of the United States that has been removed from the public domain in the interest of national security.

### Classified Information System

A classified IS processes, stores, transfers, or provides access to classified information.

Each classified information system must be certified by the Cyber Security Program to be operating in accordance with the approved Information Systems Security Plan. The information system must also be authorized (accredited) by the Department of Energy Designated Approving Authority.



Once classified, always classified.



[Privacy & Legal Notice.](#)  
LLNL-PRES-401399

Last updated August 14, 2012

For questions about this course, contact [Brenda Janiro](#).

- User
- ISSO
- System Administrator
- Information System Owner
- OISSO

## Classified Information Systems

Page 2 of 2



### Examples of Classified Information Systems

Examples of systems that could process classified information include:

- Mainframe systems
- Word processors
- Microprocessors
- Personal computers
- Programmable controllers
- Automated office support systems
- Memory typewriters
- Numerically controlled machines
- Smart switches
- Single-task preprogrammed controllers
- Programmable facsimile devices
- Automated testers
- Digital-to-analog and analog-to-digital converters
- Networks containing components that process classified information
- Digital cameras



Classified information systems (IS) include more than desktop computers and servers. If you use any of these systems for processing classified information, the classified IS security rules apply to you. This course, however, will focus specifically on computers.

If you have questions or concerns about any of the other listed items, contact your organization's Information Systems Security Officer (ISSO).



Introduction

What You Need to Know

Classified Information Systems

**Roles and Responsibilities**

User

ISSO

System Administrator

Information System Owner

OISSO

Protection Requirements

Authorization, Identification, and Authentication

Test Your Knowledge

Transferring Information

What is a File Interchange System?

Transferring Information Using File Interchange System

Purchase/Reuse of Classified Peripherals

Clearing, Sanitizing, and Destroying

Marking Hardware, Media, and Output

Public Domain and Personally-Owned Software

Test Your Knowledge

Test

## Roles and Responsibilities

The key participants in the classified information systems security program are the users, Information Systems Security Officers (ISSOs), System Administrators, Information System Owners, and Organizational Information Systems Security Officers (OISSOs).

Their roles and responsibilities are described in the following pages.

- **User:** An individual who can receive information from, input information to, or modify existing information on a classified information system (IS). Users include end users, application developers, and data custodians.
- **ISSO:** The individual identified by the organization as having responsibility for the computer security aspects of the classified information system.
- **System Administrator:** The individual who, with the ISSO's approval, installs and maintains applications and user privileges on the classified IS.
- **Information System Owner:** An individual who has programmatic responsibility for the work associated with a classified information system.
- **OISSO:** The individual who has oversight in the organization to create a compliance environment for usage and maintenance of its classified information systems.

## Classified Administrative Specialist

Classified Administrative Specialists (CASs) are control station operators who manage classified work stations and have the following responsibilities:

- Maintain accountability records within the Laboratory Accountability System for accountable matter.
- Maintain records for non-accountable matter within the Centralized Document Index.
- Manage the transition of classified matter to and from the site.
- Manage the receipts and transmittals for classified matter.
- Maintain lists of combination eligible personnel for Closed Areas and repositories authorized to store classified matter.
- Protect classified matter holdings.

**Do you know the name of your CAS?  
How would you find out?  
Ask your supervisor or ISSO.**





# CS0115-W: Classified Computer Security Training

Introduction

What You Need to Know

Classified Information Systems

Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

Protection Requirements

Authorization, Identification, and Authentication

Test Your Knowledge

Transferring Information

What is a File Interchange System?

Transferring Information Using File Interchange System

Purchase/Reuse of Classified Peripherals

Clearing, Sanitizing, and Destroying

Marking Hardware, Media, and Output

Public Domain and Personally-Owned Software

Test Your Knowledge

Test

## User Roles and Responsibilities

Page 1 of 2



A user is an individual who has access to a classified information system. These individuals must be authorized to access a classified information system. Access is controlled by the Information Systems Security Officer (ISSO).

There are three minimum criteria an individual must meet before being allowed access to any classified system. The individual must:

- Complete formal computer security training.
- Have the proper security clearance level and need-to-know the classified information that they will access.
- Acknowledge acceptance of his/her responsibilities (Code of Conduct) for protecting classified information systems and classified information.

### Fundamental Rule Regarding Access to Classified Information

Once a user is authorized to access a classified information system (IS), the individual is responsible for protecting the information and resources on that system to which he/she has access.

### Determining Need-to-Know for Classified Information

The Information System Owner for the classified material must make a need-to-know determination for each user of a classified information system before access to the classified system can be granted.

### Allowing Access to Classified Information

Individuals disseminating classified information are responsible for ensuring that recipients of the information have appropriate access authorization and need-to-know. Note: This does not permit the user to give access to his/her classified system.

LLNL Computer Security Policy [CSP4368](#), Determining Need-To-Know, provides specific guidance for determining an individual's need-to-know classified information.



[Privacy & Legal Notice.](#)  
LLNL-PRES-401399

Last updated September 17, 2012

For questions about this course,  
contact [Brenda Janiro](#).



# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## User Roles and Responsibilities

Page 2 of 2



### Other Important User Responsibilities

Users of classified information systems **must**:

- Protect the system from unauthorized access.
- Protect their authenticators (passwords, smart cards, etc.) and report any compromise or suspected compromise to their Information Systems Security Officer (ISSO).
- Ensure that system media and system output are properly classified, marked, controlled, and stored.
- Protect all media and output at the highest level and category that the system processes.
- Be accountable for their actions and immediately report to their ISSO any suspicious events, activities, or vulnerabilities that they observe involving the classified Information System (IS).
- Obtain authorization from their ISSO before they reconfigure, move, or relocate the classified IS equipment.
- Use a system with an approved waiver and obtain authorization from their ISSO before they write to external media (i.e., removable writable storage technologies include and are not limited to, floppies, diskettes, ZIP cartridges, tapes, Jaz cartridges, CDs).

Users of classified information systems **must not**:

- Install or use unauthorized software, firmware, or hardware on a classified information system.
- Attempt to circumvent any of the security features.
- Move unclassified information from a classified system to unclassified electronic media without prior approval from their ISSO. Users must then use an approved File Interchange System (see [P4406](#)).
- Write data to or read data from external media without prior authorization from their ISSO.



# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO**
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## ISSO Roles and Responsibilities



Each classified information system has an Information Systems Security Officer (ISSO) identified by the organization as having responsibility for computer security aspects of the system. **As a user, the ISSO is your primary contact for all computer-security-related issues.**

Each system has an associated Computer Security Plan that specifies the highest level and most restrictive category of data, including any Sigma data, that can be processed on the system. The ISSO is identified in the Computer Security Plan and is responsible for the implementation of security requirements for the system.

The ISSO:

- Prepares, maintains, and implements a Computer Security Plan that accurately reflects the security protection measures for each classified information system for which he or she is responsible.
- Works closely with the System Administrator to maintain the system's security and accreditation status.
- Ensures implementation of these security measures by conducting security reviews and system tests.
- Implements site procedures for marking, handling, controlling, removing, transporting, sanitizing, reusing, and destroying media/equipment containing classified information.
- Is responsible for changes to the classified system components, environment, and location, including temporary relocation to another classified area.
- Serves as a resource to users for all questions concerning classified systems.
- Verifies users' access requests are approved; controls users' access.
- Ensures users are instructed on the appropriate use of computer systems.
- Obtains one-time approval on Cyber Security Program (CSP) approved workstations or servers for all data written to or read from external media.



## CS0115-W: Classified Computer Security Training

### Introduction

#### What You Need to Know

#### Classified Information Systems

#### Roles and Responsibilities

User

ISSO

**System Administrator**

Information System Owner

OISSO

#### Protection Requirements

#### Authorization, Identification, and Authentication

#### Test Your Knowledge

#### Transferring Information

#### What is a File Interchange System?

#### Transferring Information Using File Interchange System

#### Purchase/Reuse of Classified Peripherals

#### Clearing, Sanitizing, and Destroying

#### Marking Hardware, Media, and Output

#### Public Domain and Personally-Owned Software

#### Test Your Knowledge

#### Test

### System Administrator Roles and Responsibilities

System Administrators install, configure, and maintain hardware and software components of classified information systems. They work closely with the Information Systems Security Officer (ISSO) to maintain the security of these systems.

Some examples of System Administrator responsibilities include:

- Employing appropriate security mechanisms to achieve accreditation of the system and to ensure compliance with security policies.
- Maintaining user privileges on the classified information system.
- Ensuring data is backed up on a regular basis as determined by Information System Owner (ISO).
- Reviewing system logs for unusual or unauthorized access (or attempted access).
- Reporting findings of inappropriate use and incidents.
- Ensuring that proper authorization from the ISSO is obtained before writing to external media, and only on approved workstations or servers.





## CS0115-W: Classified Computer Security Training

### Introduction

### What You Need to Know

### Classified Information Systems

### Roles and Responsibilities

#### User

#### ISSO

#### System Administrator

#### Information System Owner

#### OISSO

### Protection Requirements

### Authorization, Identification, and Authentication

### Test Your Knowledge

### Transferring Information

### What is a File Interchange System?

### Transferring Information Using File Interchange System

### Purchase/Reuse of Classified Peripherals

### Clearing, Sanitizing, and Destroying

### Marking Hardware, Media, and Output

### Public Domain and Personally-Owned Software

### Test Your Knowledge

### Test

## Information System Owner Roles and Responsibilities



An Information System Owner has programmatic responsibility for the work associated with a classified information system (IS). This individual is typically a program leader, division leader, or higher.

Some examples of an Information System Owner's responsibilities are:

- Making determinations regarding:
  - The levels of concern for integrity and availability of information processed on the IS.
  - The appropriate classification and categories for which the system will be accredited.
  - The need-to-know of the users of the IS.
- Authorizing users' access to the IS.
- Annually reviewing and revalidating users' authorization to access the IS.
- Ensuring adequate resources are available to comply with the approved security plan for the IS, including timely submission of security plans, test plans, and test results for original accreditation and subsequent reaccreditations.
- Ensure that proper authorizations have been approved before writing to external media on approved workstations or servers.





## CS0115-W: Classified Computer Security Training

### Introduction

### What You Need to Know

### Classified Information Systems

### Roles and Responsibilities

#### User

#### OISSO

#### System Administrator

#### Information System Owner

#### OISSO

### Protection Requirements

### Authorization, Identification, and Authentication

### Test Your Knowledge

### Transferring Information

### What is a File Interchange System?

### Transferring Information Using File Interchange System

### Purchase/Reuse of Classified Peripherals

### Clearing, Sanitizing, and Destroying

### Marking Hardware, Media, and Output

### Public Domain and Personally-Owned Software

### Test Your Knowledge

### Test

## OISSO Roles and Responsibilities



The Organizational Information System Security Officer ([OISSO](#)) has organizational responsibility for administering the cyber security program within their directorate and for ensuring the compliance and secure operation of their classified information systems.

The OISSO responsibilities for classified information systems are:

- Implementing and supervising the security requirements of the classified IS security plans.
- Certifying compliance and approving operation of Single User Stand Alone (SUSA) classified Information Systems (IS).
- Conducting risk assessments when necessary.
- Approving access to LLNL ISs.
- Implementing LLNL Vulnerability Assessment Program.
- Participating in computer security incident investigations.
- Ensuring continuity of operation planning to include backup and restoration of data.





# CS0115-W: Classified Computer Security Training

**Introduction**

**What You Need to Know**

**Classified Information Systems**

**Roles and Responsibilities**

User

ISSO

System Administrator

Information System Owner

OISSO

**Protection Requirements**

**Authorization, Identification, and Authentication**

**Test Your Knowledge**

**Transferring Information**

**What is a File Interchange System?**

**Transferring Information Using File Interchange System**

**Purchase/Reuse of Classified Peripherals**

**Clearing, Sanitizing, and Destroying**

**Marking Hardware, Media, and Output**

**Public Domain and Personally-Owned Software**

**Test Your Knowledge**

**Test**

## Protection Requirements

Page 1 of 3



Classified information systems and the classified material on them must be physically located in a security area appropriate to the classification and sensitivity of the data. Users have an important role in ensuring that the system and associated classified information are protected to the required levels.

### Physical Protection

- Classified information system equipment has varying separation distance requirements (see your ISSO or OISSO for separation distances) depending on the work performed (including computers, cables, telephones, Secure Telephone Equipment [STEs], radios, etc.).
- Connections between classified systems and unclassified systems or networks are prohibited.
- Removable classified electronic media may not be present in a work area containing unclassified systems that can read or write to similar media.
- Computer equipment may not be connected, disconnected, or moved unless authorized by the ISSO.
- Monitors, printers, and other devices that display or output classified information must be positioned to deter unauthorized individuals from reading the information without the knowledge of the user.
- During classified processing it is required that the classification level and category of the system accreditation be displayed on the monitor using a placard or sticker.





# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements**
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Protection Requirements

Page 2 of 3



### Personnel Access Requirements

All personnel granted unescorted physical access to a classified information system must have an appropriate security clearance and a need-to-know for all information on the information system. Otherwise, an authorized Computer Security Escort (CSE) must accompany them.

### Leaving Classified Information Unattended

Per the [Day-lock Policy Change Security Bulletin](#):

“ Day-lock procedures may be utilized for classified matter in use during an authorized user’s scheduled or self-initiated working hours and should not be confused with storage of classified matter. Storage is a condition considered long term and may be met only by an alarmed Closed Area (formerly a Vault-Type Room) or by a GSA-approved repository.”

If a classified information system does not meet the conditions set forth in the Day-lock Security Bulletin, that system and all of its components must be powered off and secured when not attended.



# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements**
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Protection Requirements

Page 3 of 3



### Classified Removable Electronic Media

Classified Removable Electronic Media (CREM) is defined as hard-drives and storage media ([view a list](#)) that can easily be removed and transported by one individual (e.g., those media that are not secured to classified systems through rack mountings or other means that require chassis disassembly with a tool).

Secret/Restricted Data (S/RD) computer media (unless defined as [Accountable Matter](#)):

- Are not accountable
- Are not subject to monthly or annual inventories
- Do not require Records of Destruction
- Do not require Accountable Document Receipts when transferred to a new location or custodian on site

See [Security Bulletin, ACREM Policy Change](#)



# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication**
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Authorization, Identification, and Authentication

Page 1 of 2

In order to access a classified information system, users must obtain approval of the Information Systems Security Officer (ISSO) and authorization of the Information System Owner for the system by reading the Implementation Manual [IM4348](#), and completing a Request for Classified Access form [F4348](#).

This form authorizes access to the classified information system (IS) and assignment of a unique user identification (ID) and an authenticator.

### User Authorization

An Information System Owner for each user must make a need-to-know determination before access to a classified IS is granted. The user, the Information System Owner, and the ISSO must sign a Request for Classified Access form.

This form must be kept on file by the ISSO and renewed annually.

### User Identification

After a required Request for Classified Access form is completed, the ISSO or System Administrator will assign the user a unique ID.



The image shows a document titled "Request for Access to Classified Information Systems" from the Computer Security Program Implementation Manual (IM4348 v1.3). The form includes sections for "Introduction", "User Access", and "Access Approval". It contains fields for user name, SSN, LIA, and various signatures and dates for approval. The form is dated January 26, 2010.



# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication**
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Authorization, Identification, and Authentication

Page 2 of 2



### User Authentication

Users are required to authenticate their identities at log-on by supplying their authenticator, such as a password, smart card, or biometrics. The Information Systems Security Officer (ISSO) or System Administrator will provide this authenticator.

Before access is permitted, users of a classified information system must be authenticated by entering their ID and authenticator (usually a password).

### User Password Criteria for Classified Information Systems

The requirements for user passwords for classified information systems are as follows:

- Must be machine-generated and a minimum of eight characters. The ISSO will assist users in obtaining their machine-generated passwords.
- Must be unique to the user.
- Must not be shared with anyone.
- Must be protected at a level commensurate with the classification level and most restrictive classification category of the information to which it allows access.
- Must be changed at least every six months or immediately if compromised.



## CS0115-W: Classified Computer Security Training

### Introduction

#### What You Need to Know

#### Classified Information Systems

#### Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

#### Protection Requirements

#### Authorization, Identification, and Authentication

#### Test Your Knowledge

#### Transferring Information

#### What is a File Interchange System?

#### Transferring Information Using File Interchange System

#### Purchase/Reuse of Classified Peripherals

#### Clearing, Sanitizing, and Destroying

#### Marking Hardware, Media, and Output

#### Public Domain and Personally-Owned Software

#### Test Your Knowledge

#### Test

### Test Your Knowledge



1. All classified information systems prior to processing classified information must be:
  - a. Certified by Cyber Security Program (CSP) to be operating according to the approved Information Systems Computer Security Plan
  - b. Authorized (accredited) by the Department of Energy Designated Approving Authority (DOE DAA)
  - c. Both a and b
2. Classified information systems only include desktop computers and servers.
  - a. True
  - b. False
3. A user's primary contact for all computer security-related issues is:
  - a. CSP
  - b. OISSO
  - c. ISSO
  - d. System Administrator
4. System Administrators are solely responsible for the accreditation of a classified computer information system.
  - a. True
  - b. False
5. An Information System Owner's responsibilities include:
  - a. Authorizing users' access to the information system
  - b. Annually reviewing and revalidating user's authorization to access the information system
  - c. Making determinations regarding how many times weekly a user should access the information system
  - d. All of the above
  - e. Both a and b
6. Before a user can be granted access to a classified information system, a need-to-know determination for the classified information is made by the:
  - a. Information System Owner for the classified material
  - b. OISSO for the classified information
  - c. Cyber Security Program (CSP)
  - d. SAFE Office





# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information**
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Transferring Information



Computer security policies provide specific guidance for transferring information between systems. Only systems accredited at the same level can be connected to each other. All other transfers occur via the use of electronic media or NNSA-approved File Interchange System (FIS).

Transfer of information must conform to requirements embodied in the CSP Implementation Manual, *Physical Port Control on Classified Information Systems* ([IM4200](#)), and *Classified Diskless Workstation Controls* ([IM4210](#)). See your Information Systems Security Officer (ISSO) for further information.

### Types of Transfers

Click on the menu bars below to see more details.

#### Transferring Classified Information to a Classified Information System

Before classified information is transferred onto a system, the user must ensure that the system has been accredited to process classified information at the appropriate classification level and category. The user must ensure information being shared is based on a need-to-know.

It is important to remember the following rule:

**Classified data must never be loaded onto, or created by, a classified information system unless the system is accredited for classified processing.**

#### Transferring Unclassified Information to a Classified Information System

#### Transferring Unclassified Information from a Classified Information System

#### Transferring Information between Classified Systems



- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information**
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Transferring Information

Computer security policies provide specific guidance for transferring information between systems. Only systems accredited at the same level can be connected to each other. All other transfers occur via the use of electronic media or NNSA-approved File Interchange System (FIS).

Transfer of information must conform to requirements embodied in the CSP Implementation Manual, *Physical Port Control on Classified Information Systems* ([IM4200](#)), and *Classified Diskless Workstation Controls* ([IM4210](#)). See your Information Systems Security Officer (ISSO) for further information.

### Types of Transfers

Click on the menu bars below to see more details.

#### Transferring Classified Information to a Classified Information System

#### Transferring Unclassified Information to a Classified Information System

Classified systems are prohibited from being connected to unclassified systems. Unclassified and classified systems with compatible electronic media are prohibited from being colocated in the same work area. All media (classified and unclassified) located in a mixed environment must be clearly marked.

When moving unclassified information from unclassified electronic media to a classified information system, the resulting media classification is determined as follows:

- Any medium (thumb drives) that cannot be write-protected becomes classified.
- A CD ROM remains unclassified only if used with a read-only CD ROM drive. If used with a read-write CD ROM drive, the media becomes classified.

#### Transferring Unclassified Information from a Classified Information System

#### Transferring Information between Classified Systems



- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information**
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Transferring Information

Computer security policies provide specific guidance for transferring information between systems. Only systems accredited at the same level can be connected to each other. All other transfers occur via the use of electronic media or NNSA-approved File Interchange System (FIS).

Transfer of information must conform to requirements embodied in the CSP Implementation Manual, *Physical Port Control on Classified Information Systems (IM4200)*, and *Classified Diskless Workstation Controls (IM4210)*. See your Information Systems Security Officer (ISSO) for further information.

### Types of Transfers

Click on the menu bars below to see more details.

**Transferring Classified Information to a Classified Information System**

**Transferring Unclassified Information to a Classified Information System**

**Transferring Unclassified Information from a Classified Information System**

Unclassified information on a classified information system may only be moved to unclassified electronic media through a NNSA-approved File Interchange System (FIS). A FIS assures that no classified data is transferred to an unclassified system. FIS procedures and controls reduce the chance of deliberate, malicious, illegal acts, or the inadvertent transfer of classified data onto unclassified systems.

Contact your Information Systems Security Officer (ISSO) to verify that the classified system has an NNSA-accredited FIS included in the Information System Security Plan and follow the specified procedures.

**Transferring Information between Classified Systems**



Introduction

What You Need to Know

Classified Information Systems

Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

Protection Requirements

Authorization, Identification, and Authentication

Test Your Knowledge

**Transferring Information**

What is a File Interchange System?

Transferring Information Using File Interchange System

Purchase/Reuse of Classified Peripherals

Clearing, Sanitizing, and Destroying

Marking Hardware, Media, and Output

Public Domain and Personally-Owned Software

Test Your Knowledge

Test

## Transferring Information

Computer security policies provide specific guidance for transferring information between systems. Only systems accredited at the same level can be connected to each other. All other transfers occur via the use of electronic media or NNSA-approved File Interchange System (FIS).

Transfer of information must conform to requirements embodied in the CSP Implementation Manual, *Physical Port Control on Classified Information Systems (IM4200)*, and *Classified Diskless Workstation Controls (IM4210)*. See your Information Systems Security Officer (ISSO) for further information.

### Types of Transfers

Click on the menu bars below to see more details.

[Transferring Classified Information to a Classified Information System](#)

[Transferring Unclassified Information to a Classified Information System](#)

[Transferring Unclassified Information from a Classified Information System](#)

[Transferring Information between Classified Systems](#)

Prior to transferring information between classified systems, the user must determine that the recipient has the appropriate need-to-know.

Information transferred from a system accredited at a higher classification level or category to a system accredited at a lower classification level or category must also be reviewed by a Derivative Classifier (DC).

An example of transferring information between classified systems is moving a Secret National Security Information (S/NSI) file from a system accredited for Secret Restricted Data (S/RD) to a system accredited only up to Secret National Security Information (S/NSI).

Prior approval is required before transferring information to a classified system operating at a lower classification level or category. For assistance, contact your ISSO.



## CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
  - What is a File Interchange System?
  - Transferring Information Using File Interchange System
  - Purchase/Reuse of Classified Peripherals
  - Clearing, Sanitizing, and Destroying
  - Marking Hardware, Media, and Output
  - Public Domain and Personally-Owned Software
  - Test Your Knowledge
  - Test

### Considerations When Transferring Information



#### Reading and Writing Removable Media on Classified Systems

If you need capability to READ or WRITE on a classified machine, then you need a waiver for the diskless workstation from your Information Systems Security Officer (ISSO).

#### Classified Diskless Workstation

A classified diskless workstation is a general-use desktop computer that does not contain any READ or WRITE capability to any removable or external media device (e.g., sled drive, USB/firewire external drive, "thumb" drive of any kind, CD/DVD internal and external drive).

- Classified diskless workstations may have an internal fixed boot disk as long as they are located in a closed area.
- Classified systems must not be located in the same work area with unclassified machines that can READ media written on a classified machine.



#### Classification Review

Authors and originators are responsible for having their work appropriately reviewed for classification before it leaves their work area or ad-hoc working group. Derivative Classifiers (DC) help authors by providing a classification review to determine if a document, its references, or any urls it links to are classified and if so, at what level and category.

Prior to classification review, matter that may be classified must be protected at the highest potential classification level and category. The originator is responsible for obtaining a classification review by a derivative or original classifier if there are any questions regarding the classification of any draft document or working paper. It is prudent to issue a stop work before publishing potentially classified information and have it assessed by a technical subject matter expert and/or classifier rather than rushing to meet a deadline.

Reference: [Classified Matter Protection and Control Manual](#)



## CS0115-W: Classified Computer Security Training

Introduction

What You Need to Know

Classified Information Systems

Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

Protection Requirements

Authorization, Identification, and Authentication

Test Your Knowledge

Transferring Information

What is a File Interchange System?

Transferring Information Using File Interchange System

Purchase/Reuse of Classified Peripherals

Clearing, Sanitizing, and Destroying

Marking Hardware, Media, and Output

Public Domain and Personally-Owned Software

Test Your Knowledge

Test

### What is a File Interchange System (FIS)?



A *File Interchange System*:

- Consists of a NNSA-accredited classified computer used with an approved, specific set of procedures, software tools, and controls designed to help assure that no classified data is transferred to media that is protected at a classification level lower than that of the data transferred (e.g., to prevent the transfer of Secret-level data to removable media protected as Confidential).
- FIS procedures, tools, and controls are intended to reduce the chance of a deliberate, malicious, illegal act or the inadvertent transfer of classified data onto media protected at a lower classification level.

A **special case of the FIS process is denoted as a Lateral File Process (LFP)**, and is:

- Employed to accommodate lateral file transfers to move appropriate data across discrete classified "air gapped" systems at the same classification level but different category.
- The two systems involved in an LFP must be operated by the same LLNL organization, and be located on-site, typically in close proximity (e.g., between SRD and SNSI computers located in the same closed area).
- Transfers of files onto classified electronic removable media that is to be physically transported off-site (i.e., away from LLNL) are not considered LFP transfers and must instead be handled as FIS transfers.
- LFP-specific controls are included in the FIS policy and implementation plan which must be followed by LFP systems.



[Privacy & Legal Notice.](#)  
LLNL-PRES-401399

Last updated August 14, 2012

For questions about this course,  
contact [Brenda Janiro](#).



# CS0115-W: Classified Computer Security Training

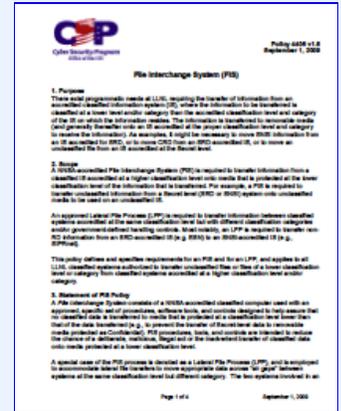
- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Transferring Information Using File Interchange System



Per [CSP Policy 4406](#):

- **A NNSA-accredited File Interchange System (FIS)** is required for:
  - Transfers of **unclassified files from classified systems to unclassified media**
  - Transfers of **classified files from a classified system of a higher category to classified media of a lower category**
- **An approved Lateral File Process (LFP)** is required to transfer information between classified systems accredited at the same classification level but with different classification categories and/or government-defined handling controls.
  - Most notably, an LFP is required to transfer non-RD information from an SRD-accredited IS (e.g. ESN) to an SNSI-accredited IS (e.g., SIPRnet).
- **Each FIS requires the Information System Security Plan (ISSP) of the higher-category system indicate that it will be used for FIS (refer to P4406 for requirements).**
  - ISSP must contain the elements as described in P4406 (Section 4)—read P4406 and IM4406 for detailed information on risk mitigation methodology and tools.
- **Any IS intended to operate as a File Interchange System**, must be included in the approved IS security plan (See [IM4406](#) for requirements, controls, and process):
  - Each file to be transferred must be approved in advance by a "FIS- Derivative Classifier" (F-DC) and the FIS operations may only be carried out by FIS-authorized personnel.
  - All F-DCs and FIS-authorized personnel must be so designated by the Directorate owning the FIS.
  - The FIS must be operated in accordance with the procedures and with the controls specified in the Implementation Manual (IM4406).
  - The physical transfer of the files to the media protected at the lower classification level requires a two-person control.





## CS0115-W: Classified Computer Security Training

### Introduction

#### What You Need to Know

#### Classified Information Systems

#### Roles and Responsibilities

##### User

##### ISSO

##### System Administrator

##### Information System Owner

##### OISSO

#### Protection Requirements

#### Authorization, Identification, and Authentication

#### Test Your Knowledge

#### Transferring Information

#### What is a File Interchange System?

#### Transferring Information Using File Interchange System

#### Purchase/Reuse of Classified Peripherals

#### Clearing, Sanitizing, and Destroying

#### Marking Hardware, Media, and Output

#### Public Domain and Personally-Owned Software

#### Test Your Knowledge

#### Test

### Purchase/Reuse of Classified Peripherals



Steps to purchase/reuse peripheral equipment in open areas for classified use:

1. Gather requirements for use of the device and assess whether those requirements conflict with security controls in the Information System Security Plan (ISSP).
2. Use IM2398, "Making Changes to Information Systems" to determine if the change will be security-significant and to document the configuration management change.
3. Once approved, proceed with purchase/reuse, ensuring product specifications meet requirements — verify the proper model device is being requested.
4. Upon arrival, verify the correct model is received, inspect for unwanted or unanticipated extras — return if necessary.
5. Set up, configure, implement security controls, and validate to ensure expected results.
6. If required, obtain final approvals from Cyber Security Site Manager (CSSM) and/or Designated Approving Authority (DAA) before processing classified information.
7. Update configuration management documentation to reflect changes.
8. Train system personnel on proper use of device.

For more information about reusing classified peripherals, see CSP [Guideline 4400](#).





# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying**
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Clearing, Sanitizing, and Destroying Electronic Media

Page 1 of 2



The following information provides general guidelines as agreed upon between LLNL and DOE for the clearing, sanitization, and destruction of electronic media.

### Clearing Classified Electronic Media

Clearing permits the reuse of classified electronic media outside the need-to-know group but within the same or higher classification level and category.

Media must be cleared by an approved DOE method. Contact your Information Systems Security Officer (ISSO) when you have media that requires clearing.

For media that will be reused within the same need-to-know group at the same or higher classification level, clearing is not required.

### Classified Media

Per CSP [Policy 4334](#), *Clearing, Purging, and Destruction of Unclassified and Classified Information System Storage Media, Memory Devices, and Related Hardware Implementation Manual*, once media is classified, it must remain classified and be destroyed as classified media when it is no longer needed. Classified media may not be cleared or sanitized for use at a lower classification level or category.

Classified media that is no longer needed must be physically destroyed in accordance with the procedures outlined in the [Classified Matter Protection and Control Manual CMPC Manual](#).

Classified media may be used by different personnel with the same classification level, category, and need-to-know for which the media last was used without clearing or sanitizing.

[See an example.](#)



# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Clearing, Sanitizing, and Destroying Electronic Media

Page 2 of 2



### Contaminated Media

If unclassified storage media becomes contaminated with classified information, your OISSO and Cyber Security Program (CSP) must be notified immediately (CSP Hotline 2-4655). This event must be handled in accordance with [CSP Procedure 5005](#), *Procedure for Clearing Contaminated Electronic Storage Media*.

[See an example.](#)

### Classified Hardware

Once hardware has been used to process classified information or has been connected to classified equipment, it must remain classified and be destroyed as classified when no longer needed. The hardware cannot be used in unclassified areas.

See CSP [Policy 4334](#) and the tables in the corresponding Implementation Manual, [IM4334](#), Appendix A *Approved Processes* for:

- Exemptions to use in unclassified areas.
- Reuse at a lower or higher classification level, category, or need-to-know level, including Top Secret information.
- Decommissioning of classified hardware no longer needed.

[See examples.](#)

Classified — cradle to grave



# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test

## Marking Hardware, Electronic Media, and Output

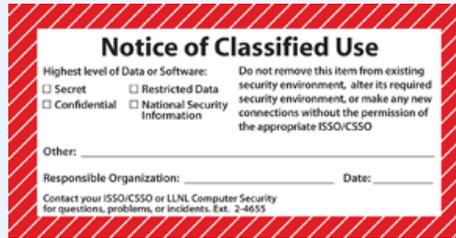
Page 1 of 4



Hardware, electronic removable media, software, hard-copy output, signal cables, and protected transmission systems (PTS) associated with classified information systems must all be properly marked in accordance with DOE requirements pertaining to classified information systems.

Users of a classified information system must know the following general marking requirements:

- Classified system hardware must be marked at the highest classification level and category for which the classified system is accredited.
- Classified computing components must be identified, and the computer input/output devices marked (e.g., Central Processing Unit, external disk drives) with one of the following labels.



- The following label is to be used for marking classified communications cabinets, lines, conduits, or raceways.



## Introduction

### What You Need to Know

#### Classified Information Systems

#### Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

#### Protection Requirements

#### Authorization, Identification, and Authentication

#### Test Your Knowledge

#### Transferring Information

#### What is a File Interchange System?

#### Transferring Information Using File Interchange System

#### Purchase/Reuse of Classified Peripherals

#### Clearing, Sanitizing, and Destroying

#### Marking Hardware, Media, and Output

#### Public Domain and Personally-Owned Software

#### Test Your Knowledge

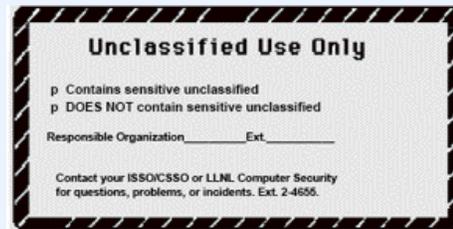
#### Test

## Marking Hardware, Electronic Media, and Output

Page 2 of 4



- Computer hardware in a mixed environment may be marked to avoid confusion. This includes components of both classified and unclassified systems. A mixed environment is one that contains both classified and unclassified systems.
- This label is to be used to denote that a system contains only unclassified information. It may be used on input/output devices (such as computers, disk drives, and printers) and may be used for marking unclassified devices located in close proximity to classified computers. This label may be required on hardware in environments that also do classified processing.



- This label is used for marking unclassified computer communications cables, conduit, trays, telephone cables, etc., if used within a classified environment.





# CS0115-W: Classified Computer Security Training

## Introduction

### What You Need to Know

### Classified Information Systems

### Roles and Responsibilities

#### User

#### ISSO

#### System Administrator

#### Information System Owner

#### OISSO

### Protection Requirements

### Authorization, Identification, and Authentication

### Test Your Knowledge

### Transferring Information

### What is a File Interchange System?

### Transferring Information Using File Interchange System

### Purchase/Reuse of Classified Peripherals

### Clearing, Sanitizing, and Destroying

### Marking Hardware, Media, and Output

### Public Domain and Personally-Owned Software

### Test Your Knowledge

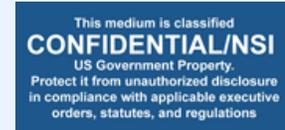
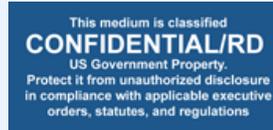
### Test

## Marking Hardware, Electronic Media, and Output

Page 3 of 4



- Removable media must be marked at the highest classification level and category for which the system is accredited.
- These labels are used on such devices as tapes, removable platters, and CDs. CDs may be labeled using the CD (donut shaped) labels.



- All removable media in a co-located/mixed office environment must be marked. This includes media from both classified and unclassified systems. A mixed-media environment is any space that contains both classified and unclassified media comingled in an office, a vault, a closed area, or an approved repository drawer. A Derivative Classifier (DC) may not reclassify media to a lower level.





# CS0115-W: Classified Computer Security Training

## Introduction

### What You Need to Know

### Classified Information Systems

### Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

### Protection Requirements

### Authorization, Identification, and Authentication

### Test Your Knowledge

### Transferring Information

### What is a File Interchange System?

### Transferring Information Using File Interchange System

### Purchase/Reuse of Classified Peripherals

### Clearing, Sanitizing, and Destroying

### Marking Hardware, Media, and Output

### Public Domain and Personally-Owned Software

### Test Your Knowledge

### Test

## Marking Hardware, Electronic Media, and Output

Page 4 of 4



- In a "mixed" environment, removable unclassified media shall be uniquely marked to protect against accidental mixing with classified media.



- Hardcopy output from a classified information system must be marked at the same accreditation level as the classified information system. However, it may be marked at a lower level and/or category if a Derivative Classifier makes the determination.

For more information on classification marking requirements, see the [Classified Document User's Manual](#) or [IM4337](#), *Marking in a Limited Area*.

Preprinted labels are available from stock inventory on site through Technical Information Department (TID) Customer Service Desk @ 2-9624.

Contact your Information Systems Security Officer (ISSO) for assistance on how to maintain the proper markings for the system components and electronic media.



## CS0115-W: Classified Computer Security Training

### Introduction

### What You Need to Know

### Classified Information Systems

### Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

### Protection Requirements

### Authorization, Identification, and Authentication

### Test Your Knowledge

### Transferring Information

### What is a File Interchange System?

### Transferring Information Using File Interchange System

### Purchase/Reuse of Classified Peripherals

### Clearing, Sanitizing, and Destroying

### Marking Hardware, Media, and Output

### Public Domain and Personally-Owned Software

### Test Your Knowledge

### Test

## Public Domain and Personally-Owned Software



Only software authorized by the Information Systems Security Officer (ISSO) may be installed on a classified system. Changes and updates must be reviewed and approved by the ISSO prior to installation.

### Personally-Owned Software

The use of any personally-owned software on a classified information system is prohibited.

### Public-Domain Software

The use of public-domain software is strongly discouraged.

The system's ISSO may approve the use of public-domain software if such software is required or needed to enhance system operation. The ISSO must maintain documentation of any approvals for the use of public-domain software.

### Anti-Virus Software

All networked classified systems must have antivirus software installed.

### Resources

More detailed information and guidance about installing software on classified information systems can be found in [P4351](#), *Protecting Classified Computers from Viruses & Malicious Code*.



[Privacy & Legal Notice.](#)  
LLNL-PRES-401399

Last updated August 14, 2012

For questions about this course,  
contact [Brenda Janiro](#).



## CS0115-W: Classified Computer Security Training

### Introduction

#### What You Need to Know

#### Classified Information Systems

#### Roles and Responsibilities

User

ISSO

System Administrator

Information System Owner

OISSO

#### Protection Requirements

#### Authorization, Identification, and Authentication

#### Test Your Knowledge

#### Transferring Information

#### What is a File Interchange System?

#### Transferring Information Using File Interchange System

#### Purchase/Reuse of Classified Peripherals

#### Clearing, Sanitizing, and Destroying

#### Marking Hardware, Media, and Output

#### Public Domain and Personally-Owned Software

#### Test Your Knowledge

#### Test

### Test Your Knowledge



1. How do you assure that no classified data is transferred to an unclassified system?
  - a. Contact the Computer Protection Program Manager
  - b. Use a NNSA-approved File Interchange System
  - c. Use a program such as Javascript
  - d. Transfer the data and have it reviewed by a Derivative Classifier
2. Personnel who do not have the need-to-know for all the information on a classified information system can be granted physical access to the system if accompanied by a Computer Security Escort (CSE).
  - a. True
  - b. False
3. Information transferred from system accredited at a higher classification level or category to a lower classification level or category must be reviewed by a Derivative Classifier (DC).
  - a. True
  - b. False
4. If there is a need to destroy classified electronic media, contact your department head.
  - a. True
  - b. False
5. A Derivative Classifier (DC) may:
  - a. Reclassify electronic media to a lower level
  - b. Determine hardcopy output from a classified IS to be different from the accreditation level of the IS
  - c. Both a & b
6. When approved by the ISSO, the use of public domain software required or needed to enhance system operation is allowed.
  - a. True
  - b. False
7. You may only electronically move unclassified information from a classified system with prior approval from your ISSO.
  - a. True
  - b. False





# CS0115-W: Classified Computer Security Training

- Introduction
- What You Need to Know
- Classified Information Systems
- Roles and Responsibilities
  - User
  - ISSO
  - System Administrator
  - Information System Owner
  - OISSO
- Protection Requirements
- Authorization, Identification, and Authentication
- Test Your Knowledge
- Transferring Information
- What is a File Interchange System?
- Transferring Information Using File Interchange System
- Purchase/Reuse of Classified Peripherals
- Clearing, Sanitizing, and Destroying
- Marking Hardware, Media, and Output
- Public Domain and Personally-Owned Software
- Test Your Knowledge
- Test**

## Test



To receive credit and have the course completion entered into LTRAIN, you must take a test. The minimum required score for passing this test is 100%. You must use your LITE user name and password to access and log on to the test. A printable [pdf version](#) of the topics is available for review purposes.

### Code of Conduct Information

Your completion of this training for users of classified information systems and acceptance of the Code of Conduct statement (which is the first test question) meets LLNL's minimum requirements; your management may impose additional requirements. Failure to accept the Code of Conduct will result in your failing to pass the course.

### Do you have an Official LLNL User Name (OUN) and Personal Access Code (PAC)?

(Off-site collaborators may select "No.")

Yes

No

### Important Information About Taking the Test

- In order to take the test, receive a pass or fail confirmation email, and have your completion record in LTRAIN, you must use a **Lab-supported browser**. Refer to the chart below to determine the appropriate browser.

Lab-Supported Browsers	
Platform	Minimum Browser
Windows	Internet Explorer 8.X Firefox 3.6X or greater
Mac	Firefox 3.6X or greater Safari

- In order to receive both the confirmation email and LTRAIN credit for having completed this course, you must also have your **pop-up blockers turned off**.
- If you need help configuring your browser, contact your Desktop Support or 4-HELP (x4-4357).