

# Individual Responsibilities

As a cleared user, you are personally responsible for the protection and control of classified information. You must safeguard this information at all times to prevent loss or compromise and unauthorized disclosure, dissemination, or duplication.



**COMMON MISHANDLING:** Unauthorized disclosure of classified material is punishable under Federal Criminal Statutes and organizational policies.

Listed below are reportable mishandling incidents:

- Receiving unmarked classified documents and disseminating them without properly marking them
- Failure to lock all safes at the end of the work day
- Throwing classified information into the trash can
- Processing classified information on a system approved only for unclassified information
- Discussing classified information in an unsecured environment or using unsecured telephones
- Disclosing classified information to a person with no security clearance or to someone who does not have a need-to-know

# Transmission Requirements

## Top Secret

- Transmit by direct contact between authorized persons
- Transmit by Defense Courier Service or an authorized government service or escort with a Top Secret clearance
- Transmit via electronic means over an **approved** secure communications system

*Do not transmit via U.S. Postal Service!*

## Secret

- Any method established by Top Secret
- Cleared commercial delivery services
- U.S. Postal Service Registered or Express Mail

## Confidential

- Any method established by Secret
- U.S. Postal Service Certified Mail

*See your Servicing Security Element (SSE) for local procedures/policies.*

**NOTE: Only approved couriers, designated in writing by an SSE, are authorized to hand-carry classified information/material.**

## Points to Remember

**Classified information/material must always be stored under conditions that will provide adequate protection and prevent access by unauthorized persons.**

- Whenever classified information is not under the personal control or observation of an authorized person, it must be stored in an approved area or container
- **The standard FAA Desktop/Laptop is NOT authorized for classified computer processing.**

**When in doubt about the proper handling (physical or electronic) of classified information, ALWAYS consult with your Servicing Security Element (SSE) or the Office of Security.**

**Any incidents involving Classified Information must be immediately reported to the Servicing Security Element (SSE) or the Office of Security.**

**Cleared individuals are not authorized to designate classified information, only Original Classification Authorities (OCAs) are authorized to designate or classify information as classified. OCAs are usually the agency heads or senior officials within government agencies.**

# Safeguarding Classified National Security Information (CNSI)



**Federal Aviation Administration  
Assistant Administrator for Security  
and Hazardous Materials (ASH-1)  
Office of Security  
Internal Security Division  
800 Independence Ave, SW  
Room 315  
Washington, DC 20591  
202-493-5405**

# Introduction

## Introduction:

- CNSI is also known as “classified information”.
- Individuals who handle, process, use, or store classified information must comply with the Federal laws, Presidential Executive Orders, and agency policies governing CNSI.

**FAA Guidance:** FAA Order 1600.2, Safeguarding Classified National Security Information, sets forth the official policies, standards, and procedures for the FAA employees and non-federal personnel who have access to Classified NSI.

**Designation as Classified Information:** Original Classification Authorities (OCAs) are authorized to designate or classify information as classified. OCAs are usually the agency heads or senior officials within government agencies.

## Levels of Classification

There are only three authorized levels of classification of information:

- **TOP SECRET** shall be applied to information that reasonably could be expected to cause **exceptionally grave damage** to national security if disclosed to unauthorized sources.
- **SECRET** shall be applied to information that reasonably could be expected to cause **serious damage** to national security if disclosed to unauthorized sources.
- **CONFIDENTIAL** shall be applied to information that reasonably could be expected to cause **damage** to national security if disclosed to unauthorized sources.

## The Purpose of Marking

Marking is the principal means of informing holders of classified information about specific protection requirements for that information. Marking of classified information is the specific responsibility of original and derivative classifiers. Marking serves the following purposes:

- Alerts holders to the presence of classified information
- Identifies the exact information requiring protection and indicates the level of classification assigned
- Provides the source and reason for classification

# Marking Classified Information

The following table contains authorized classification levels and the parenthetical symbols that are assigned to each level.

Classification Level	Parenthetical Symbol
Top Secret	(TS)
Secret	(S)
Confidential	(C)
Unclassified	(U)

**It is important that all classified information and material be marked to clearly convey the level of classification assigned, the portions that contain or reveal classified information, and the period of time protection is required.**

**PAGE MARKING:** The first page of a classified document shall be conspicuously marked, top and bottom, with the highest classification of the information contained in the document.

**PORTION MARKING:** Each section, part, paragraph, and similar portion of a classified document shall be marked to show the highest classification level of information the portion contains, or that the portion is unclassified.

**SECRET**

**Federal Aviation Administration**

July 14, 2009

**Memorandum**

**From:** Office of Security

**To:** Internal Security Division

**Subj:** (U) Special Report

1. (S) This is paragraph 1 and contains Secret information. Therefore, this paragraph will be portion marked with the designation (S) in parentheses.

2. (U) This is paragraph 2 and contains Unclassified information. Therefore, this paragraph will be portion marked with the designation (U) in parentheses.

**SECRET**

# Basic Safeguarding

## STORAGE (PAPER OR ELECTRONIC):

Classified information must be stored under conditions that will provide adequate protection and will prevent access by unauthorized persons.

The General Services Administration (GSA) establishes and publishes minimum standards, specifications, and supply schedules for containers, vault doors, and modular vaults suitable for the storage and protection of classified information.

## Below are basic storage safeguarding practices:

- Never leave classified information unattended or unsecured. Throughout the FAA, classified information or material may only be stored in either a Document Control Station (DCS) or Security Control Point (SCP).
- Do not expose classified information to individuals who do not have a security clearance and need to know.
- All classified information will be locked in a GSA approved Class 5 or 6 (letter or legal size) safe at the close of business.
- Never take classified information home.



**COMPUTER PROCESSING:** Classified Information can only be processed (i.e. saving, scanning, downloading, emailing, viewing, etc) on approved computer systems that have been accredited by the Assistant Administrator for Security and Hazardous Materials (ASH).

- **The standard FAA Desktop/Laptop is NOT authorized for classified computer processing.**

**DESTRUCTION:** Prior to any destruction consult with your Servicing Security Element (SSE).

- Only shredder models that have been evaluated by the National Security Agency (NSA) are authorized for the destruction of classified information.