Information Security

Unclassified Information

Unclassified is a designation to mark information that does not have potential to damage national security (i.e., not been determined to be Confidential, Secret, or Top Secret). DoD Unclassified data:

- Must be cleared before being released to the public
- May require application of Controlled Unclassified Information (CUI) access and distribution controls
- Must be clearly marked as Unclassified or CUI if included in a classified document or classified storage area
- If aggregated, the classification of the information may be elevated to a higher level of sensitivity or even become classified
- If compromised, could affect the safety of government personnel, missions, and systems

Controlled Unclassified Information (CUI)

Controlled Unclassified Information (CUI) is Government information that must be handled using safeguarding or dissemination controls. It includes, but is not limited to, Controlled Technical Information (CTI), Personally Identifiable Information (PII), Protected Health Information (PHI), financial information, personal or payroll information, and operational information. It may contain information:

- Provided by a confidential source (person, commercial business, or foreign government) on condition it would not be released
- Related to contractor proprietary or source selection data
- That could compromise Government missions or interests

CUI is NOT classified information and may only be marked as CUI if it belongs to a category established in the DoD CUI Registry.

Protecting CUI

To protect CUI:

- Properly mark all CUI
- Store CUI data only on authorized information systems
- Don’t transmit, store, or process CUI on non-approved systems
- Handle, and store CUI properly
    - Reduce risk of access during working hours
    - Store after working hours:
        - Locked or unlocked containers, desks, cabinets, if security is present
        - Locked containers, desks, cabinets if no security is present or is deemed inadequate

- Follow policy in DoD Instruction 5200.48, "Controlled Unclassified Information (CUI)" for retention or disposal
- Comply with the DoD Cyber Regulations outlined in the Defense Federal Acquisition Regulation Supplement (DFARS) for CUI and CTI handling requirements

Transmitting CUI

When transmitting CUI:

- If faxing CUI:
  - Ensure recipient is at the receiving end
  - Use correct cover sheet
  - Contact the recipient to confirm receipt
- Use encryption when e-mailing Personally Identifiable Information (PII) or other types of CUI, as required by the DoD

Personally Identifiable Information (PII)

Personally Identifiable Information (PII) is information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. PII includes, but is not limited to:

- Social Security Number
- Date and place of birth
- Mother's maiden name
- Biometric records
- Protected Health Information
- Passport number

Protected Health Information (PHI)

Protected Health Information (PHI):

- Is a subset of PII requiring additional protection
- Is health information that identifies the individual
- Is created or received by a healthcare provider, health plan, or employer, or a business associate of these
- Relates to:
  - Physical or mental health of an individual
  - Provision of healthcare to an individual
  - Payment for the provision of healthcare to an individual

Protecting PII/PHI

To protect PII/PHI:

- Avoid storing CUI, including PII, in shared folders or shared applications (e.g., SharePoint, Google Docs) unless access controls are established that allow only those personnel with an official need-to-know to access the information.

- Follow your organization's policies on the use of mobile computing devices and encryption
- Use only mobile devices approved by your organization
- Encrypt all CUI, including PII, on mobile devices and when e-mailed. The most commonly reported cause of PII breaches is failure to encrypt e-mail messages containing PII. The DoD requires use of two-factor authentication for access.
- Only use Government-furnished or Government-approved equipment to process CUI, including PII.
- Never allow sensitive data on non-Government-issued or non-Government-approved mobile devices.
- Never use personal e-mail accounts for transmitting PII. PII may only be e-mailed between Government e-mail accounts and must be encrypted and digitally signed when possible.

Classified Data

Classified data are designated by the original classification authority as information that could reasonably be expected to cause a given level of damage to national security if disclosed:

- Confidential – damage to national security
- Secret – serious damage to national security
- Top Secret – exceptionally grave damage to national security

Classified data:

- Must be handled and stored properly based on classification markings and handling caveats
- Can only be accessed by individuals with all of the following:
    - Appropriate clearance
    - Signed and approved non-disclosure agreement
    - Need-to-know

Protecting Classified Data

To protect classified data:

- Only use classified data in areas with security appropriate to classification level
- Store classified data appropriately in a GSA-approved vault/container when not in use
- Don't assume open storage in a secure facility is authorized
- Weigh need-to-share against need-to-know
- Ensure proper labeling:
    - Appropriately mark all classified material and, when required, unclassified and Controlled Unclassified Information (CUI) material
    - Report inappropriately marked material
- Never transmit classified information using an unapproved method, such as via an unsecure fax machine or personal mobile device

Spillage

Spillage occurs when information is "spilled" from a higher classification or protection level to a lower classification or protection level. Spillage can be either inadvertent or intentional.

To prevent inadvertent spillage:

- Always check to make sure you are using the correct network for the level of data
- Do NOT use a classified network for unclassified work. Processing unclassified information on a classified network:
  - Can unnecessarily consume mission-essential bandwidth
  - May illegally shield information from disclosure under the Freedom of Information Act (FOIA)
  - Creates a danger of spillage when attempting to remove the information to an unclassified media or hard copy
- Be aware of classification markings and all handling caveats
- Follow procedures for transferring data to and from outside agency and non-Government networks, including referring vendors making solicitations to appropriate personnel
- Label all files, removable media, and subject headers with appropriate classification markings

Never use or modify government equipment for an unauthorized purpose:

- Such use or modification could be illegal
- Misuse of equipment could have a significant mission impact
- Unauthorized connection to the Internet or other network could introduce malware or facilitate hacking of sensitive or even classified information
- Any unauthorized connection creates a high potential for spillage

Never cross classification boundaries! Do not remove equipment, including mobile devices, from a classified network for use on an unclassified network or a classified network of lower classification, or vice-versa, even if the device's memory has been purged. Never connect any unauthorized device to any network.

Responding to Spillage

If spillage occurs:

- Immediately notify your security POC
- Do not delete the suspected files
- Do not forward, read further, or manipulate the file
- Secure the area

If you find classified government data/information not cleared for public release on the internet:

- Remember that leaked classified or controlled information is still classified/controlled even if it has already been compromised

- Do not download leaked classified or controlled information because you are not allowed to have classified information on your computer and downloading it may create a new case of spillage
- Note any identifying information and the website's URL
- Report the situation to your security POC
- Refer any inquiries to your organization's public affairs office

Remember! Any comment by you could be treated as official confirmation by a Government spokesperson.

Sensitive Compartmented Information (SCI)

Sensitive Compartmented Information (SCI) is a program that segregates various types of classified information into distinct compartments for added protection and dissemination or distribution control. SCI introduces an overlay of security to Top Secret, Secret, and Confidential information. To be granted access to SCI material, one must first have TOP SECRET clearance and be indoctrinated into the SCI program. There are explicit indoctrinations for each compartment under the SCI program umbrella. The Director of National Intelligence has overarching authority concerning SCI policy.

SCI markings, or caveats, identify the specific compartment or compartments with which the material is affiliated. These caveats define the separation of SCI classified material from collateral classified material.

Information that requires a formal need-to-know determination, also known as a special access authorization, exists within Sensitive Compartmented Information.

Compromised SCI

A compromise occurs when a person who does not have the required clearance or access caveats comes into possession of SCI in any manner (i.e., physically, verbally, electronically, etc.).

You are required to contact your security Point of Contact (POC) to report the incident. Do not elaborate detailed information (that may be considered sensitive/classified) concerning the people, processes, technology, file location, specific system information, or URL that may be related to the nature of the incident until secure two-way communications (verbal or transmitted) may be achieved.

Marking SCI

When handling SCI:

- Mark classified information appropriately
  - Use proper markings, including paragraph portion markings
  - Use Security Classification Guides
  - Use Classification Management Tool (CMT) (ICS 500-8) for email and electronic documents
- Attach appropriate cover sheets
- Take precautions when transporting classified information through unclassified areas

- Complete annually required classification training

A Security Classification Guide:

- Provides precise, comprehensive guidance regarding specific program, system, operation, or weapon system elements of information to be classified, including:
  - Classification levels
  - Reasons for classification
  - Duration of classification
- Is approved and signed by the cognizant Original Classification Authority (OCA)
- Is an authoritative source for derivative classification
- Ensures consistent application of classification to the same information

Transmitting SCI

Use proper protections for transmitting and transporting SCI, such as proper wrapping and courier requirements. Dissemination of information regarding intelligence sources, methods, or activities shall be consistent with directives issued by the Director of National Intelligence

Printing:

- Retrieve classified documents promptly from printers
- Use appropriate classification cover sheets
- Ensure classified material is not mixed in with unclassified material being removed from SCIF
- Cover or place classified documents in a container even in an open storage environment

Fax:

- Mark SCI documents appropriately
- Send SCI information using an approved SCI fax machine
- Follow SCI handling and storage policies and procedures
- Immediately report security incidents to your Security POC

Courier:

- Authorization to escort, courier, or hand-carry SCI shall be in accordance with appropriate organization policy (agency-specific resources external to the course)
- Follow SCI transporting badge requirements and procedures
- Only transport SCI information if you have been courier-briefed for SCI
- Refer to agency-specific policies and requirements prior to transporting SCI information
- Contact your Special Security Office (SSO) or Security POC for questions/clarification