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

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.

PII/PHI

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):

- 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

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 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
- Mark, 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:

- Ensure all information receivers have required clearance and official need-to-know before transmitting CUI or using/replying to e-mail distribution lists
- 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

Protecting PII/PHI

To protect PII/PHI:

- Avoid storing Controlled Unclassified Information (CUI) 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 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.

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, sensitive material
  - Report inappropriately marked material
- Never transmit classified information using an unapproved method, such as via an unsecure fax machine or personal mobile device

Collateral Classified Spaces

Follow your organization's policy on mobile devices and peripherals within secure spaces where classified information is processed, handled, or discussed. Mobile devices and peripherals may be hacked or infected with malware and can be used to track, record, photograph, or videotape the environment around them. Powering off or putting devices in airplane mode is not sufficient to mitigate these risks and the threat these devices pose to classified information.

When using unclassified laptops and peripherals in a collateral classified environment:

- Ensure that any embedded cameras, microphones, and Wi-Fi are physically disabled
- Use authorized external peripherals only
    - Government-issued wired headsets and microphones
    - Government-issued wired webcams in designated areas
    - Personally-owned wired headsets without a microphone

All wireless headsets, microphones, and webcams are prohibited in DoD classified spaces, as well as all personally-owned external peripherals other than wired headsets.

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.

Preventing Inadvertent Spillage

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.