Controlled Environments

- "**Controlled environment** is any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure."

[32 CFR 2002.4 (f): https://www.federalregister.gov/documents/2016/09/14/2016-21665/controlled-unclassified-information]

- **Physical** and **Electronic**

Note: Safeguarding standards for Classified National Security Information are sufficient for CUI

Controlled Environments: Physical

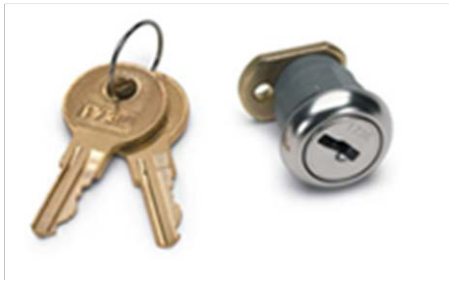
Prevent unauthorized individuals from:

- **Accessing** CUI
- **Observing** CUI
- **Overhearing** conversations discussing CUI

Controlled Environments: Physical

At least one physical barrier, such as:

- Sealed envelopes
- Areas equipped with electronic locks
- Locked:
  - Doors
  - Overhead bins
  - Drawers
  - File cabinets



Controlled Environments: Electronic

In the electronic environment, barriers should exist that limit access to only those with a Lawful Government Purpose. Barriers include:

- Dedicated network drives, file folders, or intranet sites

Organizations should establish procedures to ensure that only authorized individuals have access to CUI on electronic infrastructure. These procedures should also remove an individual's access when it is no longer required.

Guard Against Unauthorized Access