Controlled Environment:

The CUI program [32 CFR 2002.4(f)] explicitly defines a Controlled Environment as any area or space with adequate physical or procedural controls – such as, barriers or managed access controls - to protect CUI from unauthorized access or disclosure. The purpose of a controlled environment is to prevent unauthorized access to CUI.

In physical environments, physical barriers must prevent or detect unauthorized access to CUI. Should unauthorized access occur, the physical barrier in place should show evidence of tampering.

Electronic environments must also prevent or protect CUI from unauthorized access.

Notably, under these requirements, existing safeguards that meet the standards for handling classified information are sufficient for protecting CUI.

To guard against unauthorized disclosure, CUI safeguards must prevent unauthorized individuals from access, observation, or overhearing discussions that contain CUI. Be aware of your surroundings and ensure that CUI is adequately protected.

When not under the direct control of an Authorized Holder, CUI must be protected with at least one physical barrier that protects against unauthorized access. Barriers should show evidence of tampering or alteration.

Examples of physical barriers include: sealed envelopes, locked doors, overhead bins, drawers, or file cabinets. Agencies may employ key control procedures or electronic access devices to limit or control access to areas where CUI is stored, handled, or processed.

Common areas or public areas, such as cafeterias, waiting areas, or public transportation systems, are not acceptable for the storage, discussion, or review of CUI.

In the electronic environment, barriers should exist that limit access only to 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. These procedures should also remove access when it is no longer required.

In short, Controlled Environments, whether physical or electronic, facilitate access to CUI by Authorized Users with a lawful government purpose, by safeguarding CUI from access by unauthorized users.