Controlled Environments Transcript

Scene 1 INT. OFFICE HALLWAY
Employee:
Protecting Controlled Unclassified Information in a controlled environment is paramount to the success of your organization The CUI program defines a Controlled Environment as any space or area with adequate physical or procedural controls to limit unauthorized access to CUI. Let's step inside of this office to see some measures that your organization can take to create a Controlled Environment.

Scene 2 INT. INSIDE OF OFFICE, ENTRANCE AREA
Employee:
Suppose this is the office of an organization that regularly uses CUI. Is this a Controlled Environment appropriate for CUI storage and use? Let's take a closer look.

There is conference table in the center of the room. On this table, there are several documents marked as CUI haphazardly stacked. There are several people in this office, two of whom are deep in conversation about CUI and the third is a member of the office's cleaning crew, who does not have a lawful government purpose to access the information.

Slide 2 CONTROLLED ENVIRONMENTS: PHYSICAL
Employee:
For CUI that exists in the physical environment, such as documents, the CUI Program requires that inside a Controlled Environment there is at least one physical barrier to prevent unauthorized access to CUI. Organizations have some flexibility when deciding what constitutes a controlled environment. Suitable environments can be established by using measures that limit or control access to the area. Examples of ways to control access include: using standard key locks, utilizing electronic access control devices, or even employing security or administrative personnel. In areas where employees work in close proximity to individuals who may not have the same need for access, or what we call Lawful Government Purpose in the CUI program, it may be necessary to ensure that the workforce has adequate security equipment, such as lockable doors, cabinets, or drawers to secure CUI when it is not in use. It is also important to establish suitable areas for holding meetings in which CUI will be discussed.

Slide 3 CONTROLLED ENVIRONMENTS: PHYSICAL
Employee:
When considering your controlled environment, ask yourself:
- Who works in this space?
- Who has unescorted access to this space during and after normal business hours? Often times cleaning or maintenance crews have unrestricted access to areas where CUI is handled or processed, and this presents a risk to the information.
- Is the area suitable for sensitive discussions? Can anyone, even those who are unauthorized, overhear conversations?
- Is there a visitor escort policy? Most controlled environments will employ some sort of escort control policy to ensure that there is no unauthorized disclosure of CUI.

Scene 2 INT. INSIDE OF OFFICE, ENTRANCE AREA
Employee:
Very quickly, it becomes apparent that this space is not a Controlled Environment. What could have been done differently to make this office more secure?

Now back inside of the office, we see that several secure, locked file cabinets have been added to the area, and that all CUI has been moved inside these receptacles. Each file cabinet is marked as containing CUI. The cleaning crew now has conscientious escorts.

Much better. This office is now on its way to being a Controlled Environment suitable for CUI Storage and handling. But what about for CUI use? What other precautionary measures must an organization take when working with CUI?

Slide 4 Controlled Environments: Physical
Employee:
To guard against unauthorized disclosure, CUI safeguards must not only prevent unauthorized individuals from access, but also prevent them from observing or overhearing discussions that contain CUI.

Scene 3 EXT/INT. SPLIT SCREEN
Employee:
For this reason, common areas or public areas, such as cafeterias, waiting rooms, or public transportation systems, are not acceptable for the storage, discussion, or review of CUI. It is important to be aware of your surroundings and ensure that CUI is adequately protected from unauthorized disclosure at all times.

Scene 4 INT. COMPUTER DESK
Employee:
Here is an employee's work station. There are several "red flags" that indicate that CUI is not being properly protected. So how can we protect CUI that is electronically stored? Similar to the protections in the physical world, the CUI program requires that some barrier or compartmentalization exist to prevent unauthorized users from accessing electronic CUI.

Slide 5 Controlled Environments: Electronic
Employee:
These barriers should limit access only to those with a Lawful Government Purpose. Barriers include: dedicated network drives, file folders, or intranet sites.

Slide 6 Controlled Environments: Electronic
Employee:
In the electronic environment, ask yourself:
- Who has access? Who needs access? Is access removed when it is no longer needed?
- What happens when an individual transfers to another division within the organization? Is their access removed?
- Are there checks to verify who has access and who needs access? 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, like when an employee has left the agency, or has been reassigned to a new role.

Scene 4 INT. COMPUTER DESK
Employee:
Can you spot the security problems with this computer containing CUI?

Computers left unlocked are easy opportunities for unauthorized access.

This person has access to too many network drives. Access should be limited to the current project and responsibilities of each individual.

Writing down passwords and storing them in plain sight is never a good cybersecurity practice.

Unauthorized users are always looking for opportunities to access to CUI.

Scene 5 INT. OFFICE HALLWAY - MORNING
Employee:
In summary, whether in the physical world or the electronic, Controlled Environments should limit the access to CUI only to those with a lawful government purpose. By safeguarding CUI in this way, you are ensuring the protection of our Nation's sensitive materials. Thanks taking this time to learn about Controlled Environments.