**CESR FAQ: Basic Training**

**CUI Related Questions**

1. **What is Controlled Unclassified Information (CUI)?**
A: CUI is non-classified information the US government creates or possesses that requires safeguarding or dissemination controls as defined by law, regulations, and other federal government policies. It was defined on November 4, 2010 in Presidential Executive Order 13556:
<https://www.govinfo.gov/content/pkg/FR-2010-11-09/pdf/2010-28360.pdf>

CUI can also be information that a non-Federal entity, such as the University of South Carolina, receives, possesses, or creates for the US government. It requires information system security controls as defined by the contract, law, regulations, or government policies. The National Archives’ (NARA) CUI Registry is the authoritative repository for all information, guidance, policy, and requirements on handling CUI. It tracks all defined CUI categories and subcategories, including general descriptions for each, the basis for associated controls, markings requirements, and guidance on handling procedures. Examples of categories include:
	* Controlled technical information (CTI) with military or space applications.
	* Export controlled information or materials used in research.
	* Unclassified Controlled Nuclear Information – Defense

The DoD also maintains its own CUI registry which defines additional handling requirements: <https://www.dodcui.mil/>

1. **What are the CUI Control Levels?**
A: The CUI Control Level are defined in the Code of Federal Regulations 32 CFR Part 2002. These levels are:
	* **CUI Basic** – a subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls.
	* **CUI Specified** – a subset of CUI in which the authorizing law, regulation, or Government-wide policy that contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. CUI Specified controls may be different or may be more stringent than those required by CUI Basic; the underlying authority spells out the controls for CUI Specified information and does not for CUI Basic information.
	* **CUI Specified, but with CUI Basic Controls** - requires or permits the agencies to control or protect the information and defines only some of the controls.
2. **This sounds very complicated. What do I need to know about CUI?**A: Research data and other project information that a research team receives, possesses, or creates during the performance of federally funded research **may** be CUI. Determination of whether or not a project will involve CUI is made by the federal sponsor. The contract or award document should specifically identify CUI and applicable security requirements. Specificity is key to reducing scope and cost of required control measures. If you find that your contract document is not specific enough on its definition of what CUI is for your research project, you should go back and amend or clarify these provisions with the project sponsor, even after the project has started.

CUI security requirements (controls) apply to the components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. This includes controls around physical security, record keeping (logs), and some human resource processes (such as training and background checks.)
3. **Are there examples of things that are not CUI?**
A:
	* Proprietary research not funded by the federal government, even if the background information provided by the sponsor or your results are proprietary technical information subject to USC export control regulation.
	* Human subjects data or medical information subject to privacy protections (HIPAA)
	* Information already in the public domain, including US government datasets that are publicly available
	* Non-contextualized research data is not CUI, even if it is associated with a CUI project. This includes raw output from instruments, calculations, or simulations which must be correlated with additional data from a CUI project to give it meaning or context, unless otherwise specified in the contract or unless it bears identifying marks linking it to a CUI project.
	* Commercial-off-the-shelf components that are of a type generally used by the general public or for non-governmental purposes and that has been leased, sold, or licensed to the general public or offered for lease, sale, or license to the general public.
4. **What are the potential consequences for CUI non-compliance?**
A: Failure to comply may result in contract challenges to or loss of the award or contract and result in ineligibility for future government contracts. Failure to accurately report the status of compliance could result in charges of fraud and criminal penalties for the individual researcher. The university could also experience adverse legal or financial consequences.
5. **What if someone sends CUI or controlled information to my regular USC commercial email account?**
A: Do not forward or reply to the email that contains the CUI or controlled information. Do not delete the email. Notify the sender immediately that you cannot receive email at your USC account and tell them your GCC High email address to use instead. Immediately create a security incident ticket in ServiceNow at <https://cec.sc.edu/incident> and inform your project PI or supervisor that you have had a security incident. If you cannot contact your PI or supervisor, send email to security@cec.sc.edu instead. Add the following information to the “How can we help you?” field:
	* The name of your project and the PI.
	* I am reporting that someone accidentally sent an email to my university email account containing Controlled Unclassified Information. The following email contains CUI:
		+ Subject:
		+ From:
		+ Date and Time:
6. **How do I know if my lab or office is considered a CESR lab that needs security cameras, Carolina Card, and removal from the building master key system?**
A: Rooms in which only a CESR laptop is in use do not need special security considerations, other than a desk or cabinet to lock up the CESR laptop when it is unattended in the room. CESR laptops and other media containing CUI **must** be locked up when unattended in a room.

If a room contains equipment, desktop computers, workstations, instruments, servers, or other items that contain CUI or are considered CUI themselves which cannot be locked into an enclosing cabinet or desk, the room must have USC security cameras pointed at the door on the outside, have Carolina Card access installed on the access door(s), and be removed from the building master key system.
7. **Can I host visitors in my lab that contains CUI?**
A: You may host visitors. They need to be escorted at all times. They will need to sign in and out of your room’s visitor log. You will need to make sure that all materials containing or displaying CUI are either locked up or covered up and are not in view.

Visitor log template available here: <https://cec.sc.edu/cesrfiles/Visitor-Log.xlsx>

1. **Can vendors, insurance adjustors, law enforcement, maintenance, etc. come into a lab or room that contains CUI?**
A: They may come into the room, however, they need to be escorted at all times. They will need to sign in and out of your room’s visitor log. You will need to make sure that all materials containing or displaying CUI are either locked up or covered up and are not in view. Law enforcement with body cameras in operation will need to be warned about restrictions on filming in CUI controlled spaces.

During an emergency that threatens health or safety, emergency services such as the fire or police departments may enter rooms without escort. Afterward the emergency is over, it may be required to coordinate with emergency personnel if body cameras were in use and images of CUI were captured to insecure media. A note should be made in the visitor log of the incident afterwards when it is safe to do so.

Visitor log template available here: <https://cec.sc.edu/cesrfiles/Visitor-Log.xlsx>

1. **Can researchers working on my project involving CUI work in the same room as researchers that are not on my CUI project?**
A: In general, they cannot work in the same room at the same time. There are a few options. You can set up a schedule to time-share the space, dedicating the space to each project during scheduled times. You could also get the personnel from the non-CUI project CESR-certified and add them to your Technology Control Plan for your project involving CUI (if they are not a foreign national.)
2. **What is conversational security?**
A. Conversational security involves ensuring that unintended parties cannot overhear conversations that they are not authorized to hear. When discussing information that contains CUI or other protected information, be cognizant of people in hallways or outside of your meeting space. Do not discuss this information in public spaces. In large conference rooms or classrooms where sound can be heard through the walls or windows and it may not be possible to constantly monitor and interrupt meetings to wait for passersby to leave the area, a white noise machine may need to be procured and installed in hallways or spaces directly outside of the meeting space.

**CESR/GCC High Related Questions**

1. **What is the difference between CESR and GCC High?**A: CESR is the Carolina Enclave for Secure Research. It is an initiative to support research that has higher security needs due to regulatory requirements, such as Controlled Unclassified Information, HIPAA, or export-controlled projects. CESR encompasses implementation of technical controls, physical security controls, and the HR and training requirements. It also includes specific processes, standards, and policies associated with these implementations and the associated documentation.

GCC High is a Microsoft suite of cloud-based software tools and platforms hosted in Microsoft’s High security Government Community Cloud (GCC High) that includes higher-security versions of products such as email, Teams, OneDrive, and SharePoint. GCC High accounts are available within the CESR environment as an additional cost per user.
2. **Do I get an @cesr.sc.edu email address?**
A: If you purchase a GCC High account in CESR, you will get an @cesr.sc.edu email account. It is separate from your commercial USC email account.
3. **What is the cesr-*account* used for? Is this different from GCC High accounts?**
A: Accounts with the login name in the format of “cesr-*username*” were from the first-generation implementation of the CESR environment from before we migrated to GCC High and are now deprecated. We are trying to individually migrate original users to the new *username*@cesr.sc.edu format in a non-disruptive manner for all services.
4. **How do I rest my GCC High password?**
	* Go to Office 365 US Portal: https://portal.office365.us/
	* Select “Can’t Access Your Account”
	* Enter your email@cesr.sc.edu and answer the capcha challenge
	* Select “I Forgot My Password”
	* Verify your identity through email or text message
	* Verify your identity again through whichever was not picked in the last step
	* Set a new password
5. **Can I access my GCC High email account from a web portal in my browser?**
A: Yes. They URL is different from your university email account. To access your GCC High email account, you must use the URL <https://portal.office365.us/> from your GCC High computer.
6. **How do you send and receive CUI through email in CESR?**
A: At USC there are two email systems in use. The first is your university commercial email account, which cannot be used to communicate or transmit controlled information such as CUI (Controlled Unclassified Information) or CDI (Covered Defense Information.) The second is the Microsoft GCC High account (Government Community Cloud), which can be used to send and receive controlled information. You can freely send CUI in internal emails to other people with @cesr.sc.edu email addresses. If you’d like to send controlled information through email to people outside of the USC GCC High tenant (@cesr.sc.edu), you must first communicate with them and inquire whether they can receive CUI or controlled information at their email address. Once they confirm that they can receive controlled email or attachments at their email address, you may send and receive encrypted emails with them through your CESR GCC High email account.
7. **Are there other ways to transfer CUI data into and out of CESR?**
A: Some sponsors may provide their own methods or systems for you to transfer data into and out of CESR. This must be documented in your Technology Control Plan. You may also need to work with IT Services to get exceptions made to enable other organization’s file transfer solutions to work.

CESR also has a web-based file transfer service called Liquidfiles. This can be used to exchange data with entities outside of CESR. The URL for this service is <https://sft.cesr.sc.edu/>
8. **Can I use the license I bought from USC’s Software Distribution for Visio or Microsoft Project in GCC High?**
A: No, you cannot use your commercial (USC) license for Visio or Project in GCC High. You must buy the GCC High version of those licenses to use in their high-security platform. Licenses for these projects typically cost roughly three times more that the commercial license. Please contact your IT manager if you need to purchase Visio or Project for GCC High.
9. **Where do I store my data in CESR?**
All data must be stored in the GCC High cloud, either in your project Sharepoint site, your project Teams site, or you GCC High OneDrive. Do not ever store data locally on your laptop, desktop, or workstation. These devices are not backed up and storing un-backed up data on them is not compliant with the security controls. Your project may also have specific local servers or file servers that are backed on which you may store data. Please contact your faculty sponsor or PI to find out about your project’s data storage protocols.
10. **May I use my GCC High computer in public spaces such as a coffee shop or the library?**
A: You may use your GCC High computer in public spaces if you are able to reasonably ensure that you or a physical barrier can protect the CUI from unauthorized access or observation. Devices that contain or can access CUI need to be attended by an authorized CESR user at all times. Privacy screens are available to help shield data displayed on screens from unauthorized observation. You must be aware of conversational security if you attend online meetings in public spaces in which CUI is discussed to ensure that the content of the meeting cannot be overheard.
11. **May I travel with my GCC High computer or media containing CUI?**
A: You may travel domestically with your GCC High computer or media containing CUI. Keep CUI under your direct control or protect it with at least one physical barrier (such as a locked door to an enclosed room), and reasonably ensure that you or the physical barrier protects the CUI from unauthorized access or observation when outside a controlled environment. Laptop cable locks should be used when appropriate. Also logging completely out of your laptop and shutting it down between use is an extra barrier to causal compromise. Do not check your laptop at the airport, luggage locks are not sufficient as a physical barrier. Have it as your carry-on item and make sure it is stored under the seat in front of you or in an overhead bin within your line of sight.
12. **May I travel outside of the United States with my GCC High computer or media containing CUI?**A: You cannot take your GCC High computer or media containing CUI or export controlled information outside of the United States unless you have a specific license or authorization in place to take the information to a specified destination. If international travel involving a GCC High computer, CUI, or export controlled information is necessary please contact Brandi Boniface (bonifacb@mailbox.sc.edu or 803 777-8749) as soon as the need for international travel is identified.  Please note that a license can take 2 to 3 months to obtain and depending upon the specific controls in question may not be available for some countries. If such a license exists, you must keep the device in your personal custody and effective control for the duration of the trip.

Because of the way we have implemented our CESR architecture, our laptops and devices act as though they are “within” our security perimeter, even if the device hosts no sensitive data, it has access to everything as though it is within our secure perimeter. This can be problematic when visiting foreign countries.

For example, the United States Customs and Border Protection can legally search and copy the contents of travelers’ devices and they expect the traveler to turn over passwords and encryption keys to enable this practice. Other countries have similar practices and laws. Results of a refusal to comply can range from denial of entry into the country to seizure of the device in question. Some countries view any encryption suspiciously while others outright made encryption illegal. Once inside such countries, physical loss, eavesdropping, monitoring, or digital espionage are real risks and put information on the device, or that the device can access over the network at risk. There is no expectation of privacy while traveling.

**Security / Technology Related Questions**

1. **What are Controls?**
A: A control is a safeguard or countermeasure prescribed for an information system or an organization and is designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements. (<https://csrc.nist.gov/glossary/term/security_control>)

Controls can be implemented through technical (software, hardware, etc.), operational (processes, procedures), or managerial (policy) measures.
2. **What is considered a security incident?**

A: 45 CFR § 164.304 defines security incident as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. This also includes loss of devices that have the ability to access secure systems or data.

* + Virus infection
	+ Unescorted stranger in secure space
	+ Accidental (or purposeful) exfiltration of CUI data
	+ CUI data being sent to unsecure accounts or devices
	+ Loss or theft of secure laptop, USB key, authentication token (Yubi Key), or other device that contains or can access or provide access to protected/CUI data
1. **What do I do if I think there is a security incident?**
A: Immediately create a security incident ticket in ServiceNow at <https://cec.sc.edu/incident> and inform your project PI or supervisor that you think there is a security incident. If you cannot contact your PI or supervisor, send email to security@cec.sc.edu instead. Add the following information to the “How can we help you?” field in the ServiceNow ticket:
	* I am reporting a CESR security incident involving Controlled Unclassified Information.
	* The name of your project and PI.
	* Provide details about the incident.
2. **What are some indicators of insider threat?**
A: Some common precursors of insider threat include:
* Inordinate, unreasonable log-term job dissatisfaction
* Attempts to gain access to information not needed for job duties
* Unexplained access to financial resources
* Bullying or fellow employees or students
* Sexual harassment
* Workplace violence
* Serious violations of policies, procedures, directives, rules, or practices of the university
1. **What do I do if I think there is an insider threat?**
A: You may report suspected insider threats to the University Police Department.
2. **Are there requirements for reporting health and safety incidents?**
A: The university requires us to report accidents and near misses to Environmental Health and Safety: <https://sc.edu/about/offices_and_divisions/ehs/occupational_and_environmental_safety/accident_incident_and_near_miss_reporting/index.php>
3. **Can I host visitors in my lab that contains Export Controlled information or physical items?**A: You may host visitors that are US citizens or permanent residents. You may not host international visitors/foreign nationals. Foreign nationals may not have access (verbal, written, electronic, and/or visual) to controlled information or controlled physical items unless expressly permitted via an approved Technology Control Plan or license. It is the responsibility of the USC employee hosting the visitor to ensure compliance with export control restrictions and to promptly disclose and report any violation as a security incident.
4. **If someone sends me a secure meeting invite to my USC commercial email, on what device can I click the link to attend?**
A: You may open your USC commercial email on your GCC High secure computer and attend the meeting there. You should not attend the meeting on a regular, non-secure computer. Depending on the meeting technology, regular computers might be fine if the meeting software uses the correct encryption and enforces to recording or copying of data outside the meeting software (GCC High Teams meetings). It is better to err on the side of caution and use your GCC High laptop.
5. **Can I attend secure online meetings from the computer that is installed in conference rooms or classrooms?**
A: No, you cannot. You will need to use your secure laptop or get a secure computer from your IT manager to hook up to the AV in the room. Also, you will need to post signs on the doors during your meeting that state that “Audio and Visual Recording Devices in Use”.
6. **Can I use printers, USB portable storage drives, or cameras in secure spaces with CUI data?**A: Printers, USB storage devices, and cameras must be dedicated for use with CUI data. Individual devices must be tracked in inventory. Small devices such as USB portable storage drives and cameras must be locked up when not in use. When removed from locked storage or returned, and entry must be made in a Media Checkout Log. Media Checkout Log template: <https://cec.sc.edu/cesrfiles/CESR-Media-Log.xlsx>

Digital cameras are preferred over film cameras for photographing CUI because finding a facility that can legally develop photographs containing CUI can be problematic.
7. **Can I have the college print posters containing CUI on the plotter?**
A: No, the plotter is not within the CESR secure boundary, and cannot print posters. We currently do not have a secure way to print posters containing CUI.
8. **Can I use wireless mice, keyboards, headphones, or microphones with my CESR device?**A: Wireless communications must meet specific authentication and encryption standards. Contact your IT Manager to procure authorized Bluetooth devices. For human interface devices, devices must be at least Bluetooth version 2.1 with the following settings:
	* Security mode 3 (Bi-directional encrypted traffic)
	* Minimum PIN length of 8.
	* Hidden mode (non-discoverable)
	* Device firmware must be up to date
	* Activate Bluetooth only when needed, turn off when not in use
	* Encryption must be FIPS 140-2 certified
	* Do not pair devices in public spaces
9. **Are there any security requirements for webcams and microphones used on CUI projects?**
A: Webcams (and other devices) cannot be purchased from companies on the DoD’s list of banned telecommunications or video surveillance entities. <https://www.acquisition.gov/Section-889-Policies>

Webcams and microphones must have a visual indicator such as an LED light that shows when they are turned on in and in use. Ability to remote activate webcams and microphones needs to be disabled. These requirements also apply to built-in webcams and microphones on laptops, as well as recording devices in conference and meeting rooms. (NIST SP 800-171, control SC.L2-3.13.12.)

**CESR Cost Related Questions**

1. **What are the costs related to CESR?
Price List (per user)**
	* Onboarding support - $300 (one-time fee)
	* GCC High Laptop - $2000 (one-time fee)
	* GCC High Purchase Package - $250/month - includes:

GCC High YubiKey

GCC High Microsoft License

GCC High Zscaler License

Nimbus Logic License

* + Monthly CEC Maintenance support - $180/month

**Optional Features Price List**

* GCC High MS Project - $48/month
* GCC High Visio License - $25/month
* Secure Teams Integrated Conference Bridge - $120/year per research project
* Windows365 Enterprise GCCH Virtual Desktop 2vCPU/4GB/64GB - $50/month per user
	+ Pricing for more powerful virtual computers is available upon request
* GCCH Teams Rooms Pro GCon Subscription - $648/year per device