**Data Security: CUI**

**What is CUI?**

* Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
* Executive Order 13556 establishes a program for managing CUI across the Executive branch and designates the National Archives and Records Administration (NARA) as Executive Agent to implement the Order and oversee agency actions to ensure compliance. The Archivist of the United States delegated these responsibilities to the Information Security Oversight Office (ISOO).
* The Order standardizes the way in which departments and agencies handle unclassified information that requires safeguarding or dissemination controls, pursuant to and consistent with applicable law, regulations, and Government-wide policies.
* Successful implementation of this Order by agencies will enhance the efficient and effective management, control, and sharing of CUI and further the administration’s goals of openness and uniformity of government practices.

**I am considering a project or contract which has CUI requirements. Where do I start?**

* You should make two groups aware of the requirements for your project: IT Security will need to complete an assessment of compliance requirements and the CTSI Office of Sponsored Programs will need to be aware of the CUI obligations related to your proposed project.

**What are the benefits to WFBMC of being CUI compliant?**

* It is important that investigators receiving awards requiring CUI work with the IT Security to develop and follow a plan to meet these requirements. The mechanism IT Security has developed to meet CUI obligations allow Wake Forest School of Medicine investigators to obtain the increasing number of awards requiring the use of CUI.

**What are the risks of non-compliance?**

* **Breach of Contract:** Just like any other contractual requirement, standard breach of contract theories and damages may result from failing to comply with cyber and IT requirements. If the subcontractor is the responsible party, the government will hold the prime contractor liable, and the prime contractor in turn will look to the subcontractor to make it whole. (Adapted from an [article](https://www.lexology.com/library/detail.aspx?g=e26ba29a-f45d-4253-b36d-96518db17f56) by Pepper Hamilton LLP Attorneys at Law)
* **Liquidated Damages:** Government agencies may include liquidated damages provisions in their contracts, especially if there is sensitive personal information, such as personally identifiable information or protected health information.
* **Termination for Default:** Cyberattacks, data breaches and losses of confidential data are inherently serious in nature, and arguably even more so when the government is a contracting party. Given the seriousness of noncompliance, a government agency may well be in its rights to terminate a contract for default for failure to comply with cyber and IT requirements. Some agencies may even include specific termination provisions relating to cyber and IT noncompliance
* **Termination for Convenience:** Although a convenience termination is a preferable alternative to a default termination, the contractor will nonetheless lose contract revenue and will likely not be made whole through the termination process. If the prime contract is terminated for convenience, the subcontract will likely be terminated as well.
* **Poor Past Performance:** Given the importance of past performance, contractors and subcontractors must take all appropriate steps to ensure that their past performance ratings are as high as possible. Breach of contract, the imposition of liquidated damages and default terminations will unfavorably impact past performance ratings for years.
* **False Claims Act:** A contractor or subcontractor can be liable under the [False Claims Act (FCA)](https://www.justice.gov/sites/default/files/civil/legacy/2011/04/22/C-FRAUDS_FCA_Primer.pdf) for submitting false claims, i.e., invoices. “False certification” cases involve allegations that the contractor has made a false express or implied certification with respect to compliance with a statute, regulation or contract term. Express certification cases are more straightforward — they involve claims for payment that include a false certification regarding a material requirement, i.e., the contractor knows the requirement is material to the government’s payment decision.
* **Suspension / Debarment:** Contractors and subcontractors struggling with cyber and IT requirements should be mindful of the government’s broad suspension and debarment powers.

**How are CUI requirements different from our general data security requirements?**

* Agencies may place limits on disseminating CUI beyond for a lawful government purpose only through the use of the limited dissemination controls listed below, or through methods authorized by a CUI Specified authority.  In these cases, CUI appropriately shared with collaborators will need to be marked with the dissemination limitations as shown below.

| **Limited Dissemination Control** | **Description** | **Marking** | **Portion Marking** |
| --- | --- | --- | --- |
| No foreign dissemination | Information may not be disseminated in any form to foreign governments, foreign nationals, foreign or international organizations, or non-US citizens. | NOFORN | NF |
| Federal Employees Only | Dissemination authorized only to (1) employees of United States Government Executive branch departments and agencies (as agency is defined in 5 U.S.C. 105), or (2) armed forces personnel of the United States or Active Guard and Reserve (as defined in 10 USC 101). | FED ONLY | FED ONLY |
| Federal Employees and Contractors Only | Dissemination authorized only to (1) employees of United States Government Executive branch departments and agencies (as agency is defined in 5 U.S.C. 105), (2) armed forces personnel of the United States or Active Guard and Reserve (as defined in 10 USC 101), or (3) individuals or employers who enter into a contract with the United States (any department or agency) to perform a specific job, supply labor and materials, or for the sale of products and services, so long as dissemination is in furtherance of that contractual purpose. | FEDCON | FEDCON |
| No dissemination to Contractors | No dissemination authorized to individuals or employers who enter into a contract with the United States (any department or agency) to perform a specific job, supply labor and materials, or for the sale of products and services. Note: This dissemination control is intended for use when dissemination is not permitted to federal contractors, but permits dissemination to State, local, or tribal employees. | NOCON | NOCON  |
| Dissemination List Controlled | Dissemination authorized only to those individuals, organizations, or entities included on an accompanying dissemination list. Note: Use of this limited dissemination control supersedes other limited dissemination controls, but cannot supersede dissemination stipulated in federal law, regulation, or Government-wide policy.  | DL ONLY | DL ONLY  |
| Authorized for release to certain nationals only | Information has been predetermined by the designating agency to be releasable or has been released only to the foreign country(ies)/international organization(s) indicated, through established foreign disclosure procedures and channels. It is NOFORN to all foreign country(ies)/international organization(s) not indicated in the REL TO marking. Note: See list of approved country codes for use with REL TO here. USA must always appear first when using REL TO followed by additional permitted trigraph country codes in alphabetical order. | REL TO[USA, LIST] - [see list](https://www.archives.gov/files/cui/registry/policy-guidance/registry-documents/20161214-country-trigraph-codes.pdf) | REL TO [USA, LIST] - [see list](https://www.archives.gov/files/cui/registry/policy-guidance/registry-documents/20161214-country-trigraph-codes.pdf)  |
| DISPLAY ONLY | Information is authorized for disclosure to a foreign recipient, but without providing the foreign recipient with a physical copy for retention, regardless of medium to the foreign country(ies)/international organization(s) indicated, through established foreign disclosure procedures and channels. | DISPLAY ONLY | DISPLAY ONLY |

**Which funders and grant mechanisms are most likely to have CUI requirements?**

* Department of Defense (DoD)
* Defense Advanced Research Project Agency (DARPA)

**How do I determine if CUI is required of my project?**

* The contract or award notification will specify that CUI is necessary for performance of the work.

**What are CUI controls?**

* Federal agencies may not implement safeguarding or dissemination controls for any unclassified information other than those controls consistent with the CUI Program.
* Authorized holders must take reasonable precautions to guard against unauthorized disclosure of CUI. They must include the following measures among the reasonable precautions:

(1) Establish controlled environments in which to protect CUI from unauthorized access;

(2) Reasonably ensure that unauthorized individuals cannot access or observe CUI, or overhear conversations discussing CUI;

(3) Keep CUI under the authorized holder’s direct control or protect it with at least one physical barrier; and

(4) Protect the confidentiality of CUI that agencies or authorized holders process, store, or transmit on Federal information systems in accordance with the applicable security requirements

* When sending CUI, authorized holders:

(1) May use the United States Postal Service or any commercial delivery service when they need to transport or deliver CUI to another entity;

(2) Should use in-transit automated tracking and accountability tools when they send CUI;

(3) May use interoffice or interagency mail systems to transport CUI; and

(4) Must mark packages that contain CUI according to marking requirements

* Reproducing CUI. Authorized holders:

(1) May reproduce (e.g., copy, scan, print, electronically duplicate) CUI in furtherance of a lawful Government purpose; and

(2) Must ensure, when reproducing CUI documents on equipment such as printers, copiers, scanners, or fax machines, that the equipment does not retain data or the agency must otherwise sanitize it

* Destroying CUI.

(1) Authorized holders may destroy CUI when: (i) The agency no longer needs the information; and (ii) Records disposition schedules published or approved by NARA allow.

(2) When destroying CUI, including in electronic form, agencies must do so in a manner that makes it unreadable, indecipherable, and irrecoverable. Agencies must use any destruction method specifically required by law, regulation, or Government-wide policy for that CUI.

**What is involved in WFBMC’s CUI compliance review process for an individual project/contract?**

* The PI and study team will collaborate with the IT Security to:
	+ Determine the scope of CUI requirements;
	+ Complete the Security Controls Assessment; and
	+ Implement any additional needed controls;

**What is required to maintain CUI Compliance?**

* Compliance with the IT Security-approved controls and approved data sharing processes.

**We already have a grant project in progress, do I have a CUI requirement?**

* Work with the Office of Sponsored Programs to determine if Notice of Award, contracts, etc. have CUI requirements that must be addressed.

**How will CUI impact the use of my data?**

* How do I use my data in compliant areas?
	+ The data will need to be used and shared as specified in the award or contract.
	+ If data will need to be shared with other individuals or institution, it may be necessary to establish an Interconnected System Agreement and Memorandum of Understanding and it will need to be marked with the dissemination limitations as shown above.

**What are we doing at the institutional level to comply with CUI requirements?**

* A Compliance Committee has been established with representatives from IT, CTSI, and other research stakeholders to address institutional needs related to CUI.
* Options are being investigated for storage of CUI data in a separate, even more secure environment, consistent with CUI requirements.
* The following Information Technology security [policies](http://intranet.wakehealth.edu/Departments/Information-Technology/IT-Security/Resources.htm) related to CUI; others are under development:
* Risk Management Policy
* System and Services Acquisition Policy
* Configuration Management Policy
* System and Communications Protection Policy
* Personnel Security Policy
* Awareness and Training Policy
* Physical and Environmental Protection Policy
* Media Protection Policy
* Contingency Planning Policy
* System and Information Integrity Policy
* Incident Response Policy
* Identification and Authentication Policy
* Access Control Policy
* Accountability and Audit Policy

* General boilerplate language for Information Technology Services can be found [here](https://ctsi.wakehealth.edu/boilerplates).  This may be sufficient to include in a grant application.  IT Security can assist in providing more detailed information as needed.

**What resources are available to assist me/my team with CUI related questions?**

* Consultation and assistance are available for reviewing grant proposals, contracts, and notices of award for CUI requirements: contact CTSI Office of Sponsored Programs, Ryan Favreau at 336-713-5306.
* Consultation and assistance are also available for conducting risk assessments, and training for PIs and study teams. Contact IT Security at 336-713-ITSO (3-4876) or ITsecurity\_dl@wakehealth.edu or privacy@wakehealth.edu for assistance.

**CUI Forms and Templates**

* [CUI Computing Security Plan Template 180105 (.doc)](https://ctsi.wakehealth.edu/-/media/WakeForest/CTSI/Files/Regulatory/Data-Security/CUI-Computing-Security-Plan-Template-180105doc.dot)
* [CUI SBAR FINAL (.docx)](https://ctsi.wakehealth.edu/-/media/WakeForest/CTSI/Files/Regulatory/Data-Security/CUI-SBAR-FINAL.docx)