

FACULTY GUIDE

CUI Projects at Pitt: What to Expect and How to Get Approved

A step-by-step guide for investigators seeking to propose, accept, and perform work involving Controlled Unclassified Information (CUI).

About CUI

Projects involving Controlled Unclassified Information (CUI) are performed in a regulated research environment. CUI requirements are imposed by the sponsor and are conditions of award acceptance and performance — triggering mandatory compliance review and oversight obligations. If your project will create, receive, use, store, or transmit CUI, expect a more demanding process than standard academic research: approval takes time, access is controlled, and daily work practices change. If you are not prepared to follow required controls, Pitt may be unable to accept the award or permit the project to proceed.

Key Definitions

Term	Definition
Controlled Unclassified Information (CUI)	Sensitive government information requiring safeguarding under federal law, regulation, or contract. Not classified but must be protected from unauthorized access or disclosure.
Covered Defense Information (CDI)	A subset of CUI used in DoD contracts — refers to unclassified controlled technical information or other information that requires safeguarding and is marked or identified in the contract.
Controlled Technical Information (CTI)	Technical information with military or space applications that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. CTI is a category of CDI.
GCC High Enclave (CDE)	Pitt's secure Microsoft Government Community Cloud High environment, implemented with Summit 7, for storing and working with CUI.
Technology Control Plan (TCP)	The project-specific document that translates contractual requirements into practical controls for your team (i.e., personnel, locations, workflows). Distinct from the system security plan (SSP) managed centrally by Pitt Digital.

Fundamental Research vs. CUI Research

Area	Typical Fundamental Research	CUI Research (Regulated)
Who can access	Broad project collaboration	Approved users only
Where work happens	Standard Pitt systems	GCC High enclave only (default)
Devices	Often flexible	No CUI on personal devices; restrictions apply
Sharing	Easy by email/cloud	Enclave-provided means only

Startup time

Usually fast

Onboarding takes time (TCP, training, provisioning)

About This Guide

This guide covers the required steps from proposal through closeout. It does not replace contract terms, the System Security Plan, or the TCP — it summarizes what faculty must do to operate compliantly. Steps may overlap, but treat them as **sequential gates: your project may not begin until required controls are in place.**

— PRE-AWARD —

STEP 0

Before You Propose *Is CUI Work Feasible?*

Before submitting, evaluate whether CUI cost and timelines are feasible. CUI work substantially increases administrative burden and can restrict publication and collaboration.

- Review the solicitation for CUI indicators (safeguarding clauses, references to CUI, Covered Defense Information (CDI), or Controlled Technical Information (CTI)) and notify department administrators and Dean's office, as applicable, as well as OSP, ORSTC, and Pitt Digital.
- Contact ORSTC early for a feasibility discussion. ORSTC will advise on eligibility constraints, publication implications, and GCC High requirements.
- Identify your anticipated team — personnel restrictions (e.g., U.S. Person status) may apply — and any specialized computing needs that could affect feasibility.
- Consider publication expectations. Open publication requirements may require negotiated terms or declining the work.

Cost Planning

CUI work carries significant costs for secure environment access, compliance support, and onboarding. Before proposing, consult the CUI Cost Model (available from ORSTC) for the applicable cost approach, per-user and per-project estimates, and allowable budget language. Build these costs and lead times into your proposal from the start.

STEP 1

Proposal Development *Build CUI Requirements into Your Plan*

Incorporate CUI requirements into your proposal budget, timeline, and workflow planning. OSP and ORSTC will work together to ensure the proposal reflects safeguarding obligations.

- Notify OSP that the proposal may involve CUI so the appropriate review is triggered; provide any available sponsor language, including solicitation.
- Plan tasks so all CUI handling occurs within the GCC High enclave. Avoid proposing workflows using unapproved tools or third-party sharing outside GCC High.
- Build time into the schedule for TCP development, personnel screening, training, and access provisioning. Onboarding will increase your overall timeline.
- Ensure proposal language reflects safeguarding obligations.
- Build time into proposal development to account for reviews that go beyond typical OSP proposal review. Reminder — internal deadline for proposals to be received at OSP Specialist is five business days.

Common pitfalls to avoid

- Assuming the project can start immediately upon award.

- Assuming personnel can be added later without review.
- Planning to store data on local drives, lab computers, or personal devices.
- Planning to share deliverables via standard email or consumer cloud tools.
- Sharing CUI information/documents within regular email or MyFunding/MyRA.

STEP 2 Contract Review *CUI Trigger Identification*

After submission, OSP reviews contract terms during negotiation and award processing. When CUI obligations are identified, this triggers an ORSTC and a Pitt Digital review.

- OSP identifies CUI-related clauses and routes the record to ORSTC in MyFunding. Pitt Digital may also be included on the ancillary review. Upon senior leadership approval, award processing continues in parallel.
- ORSTC reviews the full agreement, statement of work, and deliverables; documents its determination; and, if CUI is confirmed, schedules a required PI intake meeting before award signature.

— COMPLIANCE SETUP —

STEP 3 Required PI Intake Meeting ★ *Decision Gate — Award on Hold*

OSP does not sign the award until ORSTC and Pitt Digital provide written clearance confirming this meeting has occurred and the PI has agreed to proceed and Senior Leadership has approved.

- **ORSTC will cover:** what information is CUI; GCC High requirements; personnel eligibility and training; publication constraints; physical space considerations; and onboarding timeline and cost model.
- **You must provide:** a preliminary personnel list (with roles and need-to-know), planned work locations, specialized computing needs, and any planned collaborators or subawards requiring CUI access.

STEP 4 Technology Control Plan (TCP) *Document Project Controls*

Every CUI project requires a TCP documenting project-specific controls. It is the enforceable reference for your team and is distinct from the GCC High SSP managed by Pitt Digital. ORSTC obtains PI signature and approves the TCP before the access request proceeds.

- Confirm with ORSTC the type of CUI and which deliverables and data are in scope.
- Finalize the approved personnel roster with documented need-to-know justifications, approved locations, and approved workflows (where data is created, stored, processed, and transmitted).
- Review and sign the TCP.

STEP 5 Screening, Training & Rules of Behavior *All Prerequisites Before Any Access*

No one may access GCC High until all prerequisites are complete for every person on the roster. ORSTC will not submit an access request until all items are verified for every user.

- **Required training:**
Provided by ORSTC: DoD Cyber Awareness Challenge, DoD Mandatory CUI Training and ORSTC project onboarding session.
Provided by Pitt Digital: Insider Risk Training (KnowBe4)

CDE Rules of Behavior signature.

- **Screening:** Restricted party screening performed by ORSTC; identity verification coordinated by HR; and eligibility confirmation (e.g., U.S. Person status) if required by sponsor.

STEP 6

GCC High Access Provisioning ★ Access Gate — CUI Work May Not Begin Until Cleared

Once the TCP is complete and all prerequisites verified, ORSTC submits a validated access request package to Pitt Digital, who coordinates with Summit 7 to provision accounts. Plan for lead time.

- Users are enabled in Pitt's GCC High tenant with GCC High-specific credentials, Multi-Factor Authentication (MFA) enrollment (Microsoft Authenticator required), and initial login configuration.
- Summit 7 confirms provisioning to Pitt Digital; Pitt Digital confirms to ORSTC. ORSTC verifies alignment with the TCP and notifies the PI that CUI work may begin.

— ACTIVE PROJECT —

STEP 7

Day-to-Day Use of GCC High All CUI Work Must Remain in the Enclave

Your local computer acts as a terminal; CUI data stays in the enclave. ORSTC monitors for compliance and is your primary contact throughout the project. Summit 7 maintains the enclave infrastructure — managing system updates, access controls, and security configurations — and provides day-to-day technical support.

- Keep CUI in GCC High — do not download, copy to USB, or store locally. Use only approved collaboration tools for CUI work.
- Do not transmit CUI through standard or personal email, or unapproved cloud tools. Follow ORSTC-provided file naming and labeling conventions for your project. If you receive CUI unexpectedly by email or another system, do not forward or attach it — describe the content in your reply and contact Pitt Digital immediately.
- Lock screens when unattended and prevent unauthorized viewing. For technical issues (access, passwords, MFA), contact Pitt Digital at helpdesk@pitt.edu. Any technical anomalies or unexpected system behaviors should be reported by the project team to ORSTC promptly.
- External collaborators are not permitted in the enclave unless explicitly approved by ORSTC. Certain software or workflows may require additional IT review.

STEP 8

Managing Changes All Changes Require Prior ORSTC Approval

Any change to personnel, locations, or tools must be reviewed and approved by ORSTC in writing before it occurs (and when applicable approved by sponsor via OSP and/or Dean's area). Pitt Digital acts only on ORSTC-submitted requests — not direct requests from the PI or project team.

- Notify ORSTC before adding team members (new personnel must complete screening and training before access), changing work locations, or adopting new tools.
- Provide written justification for access modifications (need-to-know, role, duration) and wait for ORSTC's written confirmation before proceeding.

STEP 9

Offboarding & Closeout Access Removal and TCP Closure

Access is not indefinite. GCC High accounts are also auto-disabled after inactivity per enclave policy — confirm current thresholds with ORSTC.

- ORSTC processes all personnel departures, submits deactivation requests to Pitt Digital, and confirms final disposition of any CUI held by departing team members.
- ORSTC closes out the TCP, coordinates with OSP on award closeout as relevant, and documents project closure in compliance records.

STEP 10

Incident Reporting *Applies at Every Stage*

If CUI may have been mishandled, lost, or accessed by an unauthorized person — **report immediately. Do not wait. Do not delete files, messages, or logs.**

- **Stop** the specific action that may be causing or continuing the exposure — not necessarily all project work. Report immediately to the Pitt Digital Technology Help Desk AND to ORSTC at researchsecurity@pitt.edu.
- Cooperate fully with IT-led incident response. ORSTC manages sponsor notification per contract terms and serves as compliance liaison.

Where to Get Help

Contact	For
researchsecurity@pitt.edu	Research security and compliance — your primary point of contact for all CUI matters.
helpdesk@pitt.edu https://www.digital.pitt.edu/support (412) 624-HELP (4357)	Technical support, access issues, password resets, and MFA problems within GCC High.

Information You Will Be Asked to Provide

Use this checklist to prepare for the ORSTC intake meeting and TCP development.

Information You Will Be Asked to Provide

Project title, award number, MyFunding and/or MyRA reference numbers, and sponsor contact

CUI indicators in solicitation/contract (safeguarding clauses, memos)

Roster of personnel needing access (roles and need-to-know justification)

Planned project locations (lab, office, meeting rooms)

Specialized software, tools, instruments, and data flows

Planned collaborations, subawards, or third parties needing CUI access

Publication/dissemination expectations and any constraints

Anticipated start date for CUI work (for lead time planning)