

CUI Process — Central Office Workflow

Internal desk procedure: responsibilities of OSP, ORSTC, and Pitt Digital from proposal review through project closeout. Staff reference only. Faculty-facing guidance: researchsecurity.pitt.edu

OSP action	ORSTC action	Pitt Digital / Summit 7 action	Incident reporting (any stage)	Step description	No action at this step
OSP <i>Office of Sponsored Programs</i>	ORSTC <i>Research Security & Trade Compliance</i>		Pitt Digital + Summit 7 <i>IT provisioning & technical support</i>		
PRE-AWARD					
Step 0— Before proposal <i>Department and/or PI notify OSP, ORSTC, and Pitt Digital about potential CUI work and as time allows are assisted by those offices regarding feasibility before a proposal is submitted to OSP Specialist Review in MyFunding (or to the sponsor).</i>					
As able and time allows, reviews solicitation for safeguarding clauses and CUI/CDI/CTI references. Loops ORSTC and Pitt Digital into conversation with PI/Departments for feasibility assessment.	Available on request from OSP or PI/Department before proposal submission within MyFunding for feasibility assessment. Reviews sponsor language and advises on eligibility constraints, publication implications, and GCC High requirements at the proposal stage as needed.		Available on request from OSP, the department, or the PI to provide estimated Azure GCC High costs to inform proposal budgeting and for feasibility assessment.		
Step 1 — Proposal review/submission to sponsor <i>Dept./PI build CUI requirements into the proposal budget, timeline, and workflow planning and mark MyFunding submission as “yes” to CUI.</i>					
Once MyFunding proposal is received to OSP Specialist and as able, ensures proposal language reflects safeguarding obligations. Triggers ORSTC and Pitt Digital review at proposal stage if CUI scope is evident. Documents CUI indicators in MyFunding via triggering “response required” ancillary reviews to ORSTC and Pitt Digital.	Advises PI on required workflows, restricted tools, safeguarding obligations to be listed in the proposal, and GCC High planning. Flags compliance concerns with the proposal as written. Coordinates with OSP on feasibility of proposed approach as needed.		Available on request to advise on GCC High compatibility of proposed workflows during proposal development.		
Step 2 — Contract review/ <i>OSP, ORSTC, and Pitt Digital review the award to confirm whether CUI obligations apply.</i>					
Identifies CUI-related clauses during contract negotiation and award processing. Sends clarifying questions to sponsor regarding CUI applicability. Routes record to ORSTC and Pitt Digital in MyRA for compliance review via “response required” ancillary reviews. If CUI applies or cannot be removed and ORSTC and Pitt Digital have cleared their ancillary reviews, refers the award to Senior Leadership Review (SLR) prior to agreement signature; the agreement is not signed until SLR approval is received. Documents SLR decision within MyRA (via Private OSP Comment). If SLR does not approve, OSP updates the PI/department and sponsor.	Reviews full agreement, statement of work, and deliverables. Determines whether CUI applies or is reasonably anticipated. If confirmed: schedules required PI intake meeting before award activates. Documents determination.		Receives an ancillary review assignment through MyRA once CUI is flagged.		
COMPLIANCE SETUP					
Step 3 — PI intake meeting <i>ORSTC briefs the PI on all CUI obligations before the award is signed. Award is on hold until this gate is cleared.</i> ★ Decision gate					
Award signature is paused until ORSTC confirms the intake meeting has occurred and the PI has agreed to proceed. OSP does not sign until ORSTC and Pitt Digital provide written clearance (via	Leads intake meeting. Briefs PI on: what information is CUI, GCC High requirements, personnel eligibility rules, publication constraints, physical space needs, onboarding timeline, and cost model. Collects PI's personnel list, work locations, computing needs, and planned collaborators. PI must		Clears MyRA ancillary review.		

OSP Office of Sponsored Programs	ORSTC Research Security & Trade Compliance	Pitt Digital + Summit 7 IT provisioning & technical support
clearing ancillary reviews in MyRA) and SLR approval has been provided.	confirm intent to proceed before process advances. Clears MyRA ancillary review.	
Step 4 — Technology Control Plan (TCP) <i>ORSTC and the PI document exactly who can access CUI, where, and how.</i>		
	Works with PI to confirm CUI type and deliverables in scope. Documents approved personnel roster with need-to-know justifications, approved physical locations, approved workflows, and approved tools. TCP is project-specific and distinct from the GCC High system SSP managed centrally by Pitt Digital. Obtains PI signature and approves TCP before access request proceeds. Notifies OSP that TCP has been completed.	Consulted by ORSTC to confirm proposed workflows and tools are supported within the GCC High environment before the TCP is finalized.
Step 5 — Personnel screening and training <i>Every person on the access roster must pass screening and complete all required training before any access is requested.</i>		
	Performs restricted party screening on all personnel. Coordinates HR identity verification. Confirms eligibility requirements (e.g., U.S. Person status if required). Tracks completion of all required training for every user: DoD Cyber Awareness Challenge, DoD Mandatory CUI Training, Insider Risk Training (delivered by Pitt Digital via KnowBe4), Rules of Behavior signature, and ORSTC project onboarding session. No access request is submitted until all items are verified for every user on the roster.	
Step 6 — GCC High access provisioning <i>Accounts are created in Pitt's secure GCC High environment. CUI work may not begin until this gate is cleared. ★ Access gate</i>		
	Compiles validated access request package (project details, approved user roster, completed TCP). Submits to Pitt Digital Technology Help Desk. Verifies provisioning aligns with approved TCP upon Pitt Digital confirmation. Notifies PI that access is active and CUI work may begin.	Reviews ORSTC access request package for completeness and compliance. Coordinates with Summit 7 to provision user accounts in GCC High tenant. Sets up MFA enrollment (Microsoft Authenticator required). Summit 7 confirms completion to Pitt Digital; Pitt Digital confirms to ORSTC.
ACTIVE PROJECT		
Step 7 — Day-to-day CUI work <i>The project is active. ORSTC monitors for compliance; Pitt Digital maintains the enclave.</i>		
	Monitors active projects for changes requiring TCP amendments. Available to answer PI questions on permitted tools, workflows, and collaboration. Serves as primary point of contact throughout project life. Conducts check-ins as appropriate for project risk level.	Summit 7 maintains the Azure GCC High environment and security controls; Pitt Digital is alerted to security incidents. If researchers need assistance — including password resets, MFA issues, or environment access — ORSTC submits a Pitt Digital Help Desk ticket (helpdesk@pitt.edu), and Pitt Digital coordinates with Summit 7 as needed. Reports technical anomalies to ORSTC.
Step 8 — Managing changes <i>Any change to personnel, locations, or tools requires prior ORSTC review and written approval.</i>		
Reviews personnel change requests against award language. Sends to sponsor and/or Dean's area for approval, as needed.	Evaluates all change requests: new personnel (screening and training required before access), new work locations, new tools or workflows. Amends TCP as needed. Sends personnel change requests to OSP to ensure sponsor approval is not needed. Provides written confirmation of approved changes to PI. Submits updated access requests to Pitt Digital for personnel additions or removals.	Adds or removes GCC High user accounts per ORSTC-submitted requests only; Summit 7 executes account changes based on Pitt Digital's submitted requests. Does not accept direct requests from the PI or project team. All account changes

OSP <i>Office of Sponsored Programs</i>	ORSTC <i>Research Security & Trade Compliance</i>	Pitt Digital + Summit 7 <i>IT provisioning & technical support</i>
		route through ORSTC. Confirms implementation back to ORSTC.
Step 9 — Offboarding and closeout <i>Access is removed and the TCP is closed out when the project ends or personnel leave.</i>		
Signs applicable award closeout documents or sends to other central offices for signature/review as needed.	Processes all personnel departures. Submits account deactivation requests to Pitt Digital. Confirms final disposition of CUI held by the project team, consistent with University Data Retention requirements for CUI. Closes out TCP. Coordinates with OSP on award closeout if relevant. Documents project closure in compliance records.	Summit 7 disables and removes GCC High accounts per ORSTC-submitted deactivation requests, executed through Pitt Digital. Accounts are soft-deleted before permanent removal. Accounts inactive for 90+ days are automatically deactivated per enclave policy. Confirms deactivation to ORSTC.

⚠ Step 10 — Incident Reporting: applies at every stage ⚠		
<i>If CUI may have been mishandled, lost, or accessed by an unauthorized person — Stop. Preserve all evidence. Do not delete anything. Report immediately to Pitt Digital Help Desk AND ORSTC.</i>		
Informed if the incident affects award terms, sponsor notification obligations, or contract compliance requirements. Does not contact the sponsor directly — sponsor notification for the incident occurs through Pitt Digital's certified DoD report. If contacted by sponsor directly, does not reply, but rather forwards communications to Pitt Digital for response.	Coordinates response across offices. Oversees documentation and reporting. Works with Pitt Digital on scope of exposure and containment. Relies on Pitt Digital's certified report as the formal channel to notify the sponsor; does not contact the sponsor independently during an incident.	Leads technical incident response and investigation. Determines scope of any exposure. Executes containment and remediation. Reports technical findings to ORSTC. Preserves logs and evidence for compliance documentation. With ORSTC's approval, rapidly reports the incident to DoD via DIBNet (dibnet.dod.mil) within 72 hours of discovery, per DFARS 252.204-7012. Only two designated Pitt Digital staff hold the required DoD-approved medium assurance certificate needed to submit this report, making Pitt Digital the sole point of formal contact with the sponsor during a cyber incident.