



Controlled Work

Your CUI stays within the systems your security team approves. We still do the work.

Federal paperwork does not become your team's problem again when it contains controlled information. Gesso brings a versioned Controlled Work operating package into the environment your security team approves, configures the approved runtime and tools, then performs the controlled portions of responses, recurring reports, and past-performance records there.

Gesso delivers the response and reporting workflows approved for your controlled boundary. Your Gesso lead still coordinates contributors, drafts the work, asks focused follow-up questions, runs the checks, and prepares the finished files for your review.

What Gesso can do with controlled data

Responses and proposals

We build controlled response sections and, when the approved workflow calls for it, the complete package from the solicitation, contract, evidence, and working rules. Your company reviews and submits.

Recurring contract reports

We collect approved contributor updates, ask for missing facts and metrics, check the work against the contract, and prepare the report for review.

Past-performance records

We preserve approved metrics and evidence while they are fresh so your team is ready for the next RFI, RFQ, proposal, or recompete.

One service, two working boundaries

BOUNDARY	WHAT BELONGS THERE	HOW GESSO WORKS
Standard Work	Work that does not contain CUI, covered defense information, export-controlled technical data, or classified information	The ordinary client-approved Gesso workflow
Controlled Work	The named CUI or covered defense information approved for a specific client and scope	Gesso configures the versioned operating package inside the client-owned or client-licensed environment and uses only the processing route and access rules the security team approves

Controlled content does not move into Gesso's standard email, storage, local workspace, or ordinary commercial accounts.

Export-controlled technical data uses Controlled Work only after separate written authorization and approval of the U.S.-person, location, system, and access restrictions. Classified information is excluded.

How setup works

1. **Name the first job and its rules.** Tell us the first controlled workflow, the governing contract or flowdown, the data involved, and who owns the contract and security decisions. Do not send controlled files yet.
2. **Agree on the boundary.** We prepare the scope, preliminary data flow, responsibility split, and intended processing route. Both sides sign the Controlled Work Schedule before Gesso receives access.
3. **Authorize setup.** Your security owner approves invented-data setup in writing, and your team provisions named access to the blank approved environment.
4. **We inspect, configure, and prove the service.** Gesso inventories the environment, reports any gaps, and configures the workspace, procedures, checks, records, and handoffs. Using invented files, we test the exact processing route, file intake, extraction, editable documents and spreadsheets, PDF rendering and inspection, approved source access, logs, and client handoff required by the scope. Every required function needs a tested primary implementation and evidence. If the service relies on a fallback, we test it; otherwise we record the stop path. Missing functionality or output below Gesso's quality bar stops launch.
5. **Approve live use.** Gesso begins handling controlled data only after the exact processing route, required capabilities, security tests, and quality benchmark pass and your security owner issues written live approval.

What your security team receives

- a defined work scope and data-flow diagram;
- a responsibility matrix naming Client, Gesso, and provider duties;
- the exact people, accounts, locations, services, endpoint, model, and region proposed for the work;
- access, logging, retention, incident, change, and offboarding rules;
- a release manifest and client change record;
- a capability matrix and acceptance record showing that every required part of the workflow works;
- a direct answer to every open requirement or a named blocker that must be resolved before activation.

Clear ownership

Your company governs the environment

Your company governs the contract's required status and flowdowns, the working environment and approved services, identities and access, security approval, export-control approval, and the incident plan and external contacts. The signed responsibility matrix and contract assign every reporting duty.

Gesso runs the paperwork

Gesso configures the service inside the approved boundary, runs drafting and contributor follow-up, performs the checks, prepares the deliverables, keeps work and release records, and immediately uses your approved incident route if a boundary event is suspected. The signed responsibility matrix records any more detailed split.

Straight answers

Is Gesso Federal CMMC Level 2 certified?

Gesso can handle CUI through Controlled Work for a named contract and approved scope. Gesso does not claim a blanket CMMC Level 2 certification. We use client-issued access and only the systems and processing routes your security team approves. If the contract requires Gesso to hold its own CMMC status, or the required processing route cannot pass approval, work does not begin.

Can Gesso work with export-controlled technical data?

Only after your export-control owner confirms in writing the classification, U.S.-person and location restrictions, any required registration or authorization, and the approved systems and access path. Controlled Work does not itself authorize export-controlled work.

Can Gesso handle classified information?

No. Gesso does not handle classified information.

Does signing the agreement open controlled intake?

No. The signed agreement defines the scope. Controlled intake opens only after the exact route, every required capability, security test, quality benchmark, and complete end-to-end process pass with invented files, and your security owner issues the live approval record.

Start with the work and the requirement

Start with a 20-minute fit call. Tell us the first controlled job and who owns the contract and security decisions. We will prepare the specific follow-up, then handle the technical inventory, setup plan, and test record after the signed scope and written setup approval. Do not send controlled files before the approved workflow is live.

Book a Gesso Federal fit call