

CASE STUDY · MAY 2026

Planning protected engineering desktops in Azure Government

An anonymized May 2026 SOW-based case study of proposed Azure Government virtual desktops, engineering application readiness, identity controls, and CUI protection planning.



Conceptual illustration only; not the customer's production environment.

Project snapshot

Detail	Documented scope
Customer	An organization supporting federal engineering workloads; customer anonymized
Project date	May 2026
Infrastructure plan	Azure Government tenant and Azure Virtual Desktop with dedicated and pooled desktops
Security objective	Support CUI handling and the customer's broader CMMC readiness program
Status represented	Proposed design, deployment, validation, and handoff; completion and results are not verified

This project case study is based on a supplied Statement of Work, not a completion report. Customer and third-party identities, deployment counts, commercial terms, and internal estimates have been omitted. Planned capabilities remain subject to licensing, cloud availability, architecture validation, and customer approval.

Executive summary

The SOW proposed an Azure Government environment for engineering users working with Controlled Unclassified Information (CUI). It combined virtual desktop design with identity, endpoint security, network access, data protection, and operational documentation.

Massive IT's proposed role was to build and configure the defined environment, validate representative workloads and access policies, and support the customer's wider compliance readiness program. The document does not establish a completed deployment, a CMMC certification, a customer FedRAMP authorization, or measured improvements in performance or security.

The planning challenge

Engineering applications such as AutoCAD, Autodesk tooling, and Visio require more than a generic desktop image. The design needed to account for application compatibility, graphics requirements, persistent user profiles, session concurrency, and access to approved data repositories.

At the same time, the customer wanted access and data controls aligned with its federal workload requirements. The plan therefore treated the desktop, identity, endpoint, network, and information-protection layers as connected workstreams rather than independent product installations.

Proposed architecture and cloud boundaries

Layer	Planned role
Azure Government	Subscriptions, management hierarchy, networking, role-based access, policy, and virtual desktop infrastructure
Azure Virtual Desktop	Dedicated desktops for persistent workloads and pooled session hosts for shared usage
Microsoft 365 GCC High	Relevant productivity, identity integration, device-management, and information-protection configuration
Approved CUI repository	Egnyte Gov designated in the SOW as the primary repository for CUI accessed through desktop sessions
Endpoint and access controls	Defender, Conditional Access, and proposed Cloudflare Zero Trust integration, subject to supported government-cloud capabilities

Azure Government and Microsoft 365 GCC High are distinct service environments, not interchangeable tenant labels. The SOW references both. Their identity relationships, administrative boundaries, service endpoints, licensing, and supported integrations would need confirmation during discovery.

Designating a repository and configuring network routes does not, by itself, establish compliant CUI residency or prevent every form of data transfer. The final design would require review of data flows, service authorizations, endpoint behavior, and the customer's applicable requirements.

Massive IT's proposed workstreams

1. Establish the government-cloud foundation

Provision and configure the Azure Government tenant, subscription structure, management groups, resource groups, virtual networks, subnets, network security groups, and DNS. Review site-to-site VPN or ExpressRoute connectivity as appropriate for the existing environment.

The scope also included role-based access control, privileged access configuration, and policy alignment with the customer's compliance program. These were configuration objectives supporting readiness, not guarantees that the organization would satisfy every CMMC or FedRAMP requirement.

2. Design dedicated and pooled engineering desktops

Use dedicated desktops where persistent, individually assigned environments were required, and pooled hosts where shared sessions were appropriate. Configure FSLogix profile containers and planned autoscaling to match the agreed usage pattern.

The SOW contains inconsistent concurrency assumptions and references both standard virtual machines and GPU-accelerated workloads. Host counts, graphics-capable SKU selection, quota availability, concurrency, and operating schedules would need reconciliation with the technical engineer and representative application tests. No final capacity or performance commitment is inferred here.

3. Prepare and document the desktop image

Build a master image with an appropriate supported Windows configuration, FSLogix, application-readiness validation, and image versioning guidance. Graphics drivers and GPU virtualization were proposed where required and supported by the selected hardware and government-cloud services.

Engineering application licenses were customer-provided. Procurement, activation, and vendor support for those applications were outside the engagement. Intune and GCC High integration requirements would need to be validated against the selected desktop and identity model.

4. Configure security monitoring and administrative access

The SOW proposed Defender for Endpoint Plan 2 onboarding for the scoped session hosts, security-baseline review, vulnerability findings review, and routing of critical or high-severity alerts to designated customer contacts. It also proposed Defender for Cloud Apps configuration and just-in-time administrative access where supported.

Government-cloud availability and licensing for each feature would need verification before implementation. Configuring alert routing is not evidence of a contracted 24/7 monitoring or incident-response service. Security work for unrelated commercial subscriptions and non-AVD workloads was excluded.

5. Stage identity-aware access controls

Plan Cloudflare Zero Trust organization setup, identity-provider integration, WARP deployment to user laptops, device-posture checks, and traffic routing. Validate the actual supported AVD connection path and government identity integration rather than assuming that an access application can gate every desktop protocol.

Conditional Access work would cover agreed user and device access requirements, MFA, compliance checks, and supported risk or session controls. The SOW called for customer-approved policy design, report-only validation before enforcement, and representative endpoint testing before phased rollout. Required Cloudflare licenses were the customer's responsibility.

6. Plan layered information protection

Design proposed DLP and sensitivity-label controls across applicable GCC High services, endpoint activity, and supported cloud-app sessions. The intended scope included reviewing unauthorized transfer scenarios and routing policy-match notifications to customer security or compliance contacts.

Built-in sensitive information types are not an automatic classifier for all CUI. Coverage, licensing, supported endpoints, and actual control behavior would require validation. The SOW called for initial audit

or simulation review before blocking, with refinement and customer approval. Custom classifiers and protection for unrelated workloads were outside scope.

Delivery sequence and ownership

Stage	Planned activity and dependency
Foundation	Confirm access and requirements; establish tenant, network, identity, and architecture
Desktop preparation	Resolve sizing and quota; build images, host pools, profiles, and engineering application readiness
Security configuration	Apply supported Defender, access, and data controls after licensing and integration validation
Pilot and enforcement	Test representative users and devices; review audit results before approved phased enforcement
Handoff	Deliver architecture, policy settings, image-update guidance, findings, enrollment procedures, and administrative documentation

The customer was responsible for timely system access, stakeholder input, required licenses, and policy approvals. Compliance-program direction remained with the customer and its compliance advisers. Scope changes, additional policy work, and unforeseen constraints required review through change control.

What the source establishes—and what it does not

The SOW establishes proposed workstreams, deliverables, responsibilities, and validation steps. It does not provide acceptance evidence, deployed configurations, successful user tests, a confirmed production cutover, or measured cost and performance results. Commercial and effort estimates are intentionally omitted; inconsistencies in the source are not resolved into new commitments.

The project takeaway is a structured planning approach: reconcile cloud boundaries and engineering requirements first, validate supported controls and data flows, pilot policies before enforcement, and document ownership. A government-cloud deployment can support a broader readiness program, but technology configuration alone is not certification or proof of compliance.