CASE STUDY · AUGUST 2025

Defense Contractor Strengthens NIST 800-171 Readiness in Three Weeks

An anonymous defense contractor deployed Microsoft 365 GCC High, strengthened endpoint controls, and documented its security approach in three weeks, reporting retention of a critical client contract.



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

How Microsoft 365 GCC High helped retain a critical contract and strengthen cybersecurity. The contractor and client are anonymous. Outcomes are reported in the supplied August 4, 2025 project account; no independent assessment, certification, or guarantee of compliance is established by that account.

A defense contractor needed to meet NIST 800-171 requirements to retain a major Fortune 500 client contract. With sensitive projects and future defense opportunities at stake, the organization faced an urgent need to strengthen its security controls and document its compliance approach.

In three weeks, the contractor implemented a Microsoft 365 GCC High environment, strengthened endpoint protection, and completed supporting compliance documentation. The engagement helped retain the client contract and established a foundation for future CMMC readiness.

At a glance

Category	Details
Industry	Defense contracting
Business requirement	Meet NIST 800-171 requirements tied to a Fortune 500 client contract
Solution	Microsoft 365 G5 in GCC High, Intune, Defender for Endpoint, and CIS v8 controls
Timeline	Three weeks
Reported results	Meeting the contractor’s NIST 800-171 requirements, contract retention, stronger security, and progress toward CMMC readiness

The challenge

The contractor supported sensitive projects for U.S. government and private sector clients, but its existing IT environment lacked the security framework and compliance alignment required for a critical client engagement.

The immediate concern was retaining a Fortune 500 defense client contract. Beyond that deadline, gaps in standardized security controls created cybersecurity exposure and threatened the organization’s eligibility for future Department of Defense opportunities.

The contractor needed to address these gaps quickly while preparing for future CMMC requirements. Technology deployment needed to be supported by security configuration, control alignment, and documentation.

The solution

The engagement combined a migration to Microsoft 365 GCC High with device management, endpoint protection, and compliance support.

Workstream	Documented approach
Microsoft 365 G5 in GCC High	The contractor migrated to an environment supporting its security and compliance objectives.

Workstream	Documented approach
Microsoft Intune	Policy-based device management and compliance enforcement brought greater consistency to endpoint configuration.
Microsoft Defender for Endpoint	Integrated endpoint defenses and Microsoft security policy guidance strengthened protection across managed devices.
CIS v8 security controls	Controls mapped to NIST 800-171 requirements provided a structured basis for security hardening.
System Security Plan support	Assistance with drafting and validating the SSP helped document the environment and its implementation of required controls.

The reported outcomes

Accelerated NIST 800-171 alignment

The contractor reported meeting its NIST 800-171 compliance requirements within three weeks. This is a source-reported outcome, not an independent determination that every applicable control was assessed or certified. Platform selection alone does not establish compliance.

Critical contract retained

The supplied account reports that the organization satisfied the compliance requirement tied to its major Fortune 500 client contract, protecting an important business relationship.

Foundation for CMMC readiness

The engagement established security controls and documentation to support future CMMC preparation. The account does not establish achieved CMMC certification or a completed CMMC assessment.

Stronger cybersecurity posture

Hardened endpoints, centralized device policies, and integrated defenses improved the organization’s ability to protect its environment.

A foundation for future defense opportunities

The contractor addressed an urgent compliance requirement while improving the security of its Microsoft 365 environment. By connecting platform configuration, endpoint controls, and supporting documentation, the engagement helped protect an existing contract and prepare the organization for future defense-sector opportunities.