CYTADEL
IT SOLUTIONS

Capability Statement

Secure The Way You Innovate

Company Overview

Cytadel is a veteran-led cybersecurity and technology firm built on two decades of direct experience inside national security and defense environments. Our leadership has served in uniform and continued that service in some of the most demanding federal and defense programs in the country.

We work with federal agencies, defense organizations, and regulated commercial clients on the security and technology challenges that carry the most operational weight. Our work is specific, deliberate, and built around what each client needs to protect and sustain their mission and operations.

Cybersecurity and Risk Management

Most organizations have controls in place. What they often lack is security that connects to how they actually operate. We work through the architecture, identify where controls are misaligned with real operational risk, and build programs that hold up outside the audit window. The work is specific, not templated.

Cyber-Physical Systems and Infrastructure Security

Operational technology, building systems, and industrial automation platforms are where digital vulnerabilities become physical consequences. We have worked inside these environments and understand what availability and continuity demand at the operational level. That changes how we assess risk and what we prioritize.

Technology Modernization

Legacy infrastructure does not age gracefully, and modernization projects have a way of introducing the exact vulnerabilities they were meant to eliminate. We stay involved through the transition, keeping security requirements connected to the work as platforms change, teams shift, and timelines compress.

Governance, Risk, and Compliance Advisory

We work directly with executives and program managers to make sure technical findings translate into decisions, not reports. That includes authorization support, audit preparation, and ongoing advisory work that keeps leadership informed without requiring them to become technical experts.

NAICS Codes

Primary—
541512 – Computer Systems Design Services
Additional—
541511 – Custom Computer Programming Services
541513 – Computer Facilities Management
541519 – Other Computer Related Services
541611 – Management Consulting Services
541330 – Engineering Services
541690 – Scientific and Technical Consulting
541715 – Research and Development in Emerging Technologies
561621 – Security System Services

Virginia Values Veterans
Official V3 Certified Company

SBA
U.S. Small Business Administration
SERVICE-DISABLED VETERAN-OWNED CERTIFIED

Company Data

Legal Name: Cytadel LLC
UEI: X1C2TNNFMQ33
CAGE Code: 115HH9
Entity Type: Virginia Limited Liability Company
Ownership Status: Service-Disabled Veteran-Owned Small Business (SDVOSB)
Website: www.cytadeltech.com
Email: info@cytadeltech.com
Primary Office: Richmond, VA

Strategic Differentiators

A Profile Built on Reinforcing Strengths

Our leadership brings together military service, national security execution experience, graduate-level strategic training, and industry-leading certifications earned in the field. Each of those elements makes the others more valuable. That combination is not something a competitor can replicate by adding a service line or making a hire.

Shaped by Environments That Demanded Excellence

Our leadership developed their practice inside military and federal defense programs where ambiguity was a liability, and the cost of poor judgment was measured in mission outcomes.Those standards travel. They shape how we scope work, what we flag as risk, and where we push back on assumptions.

Security Designed Around Operations, Not Around Frameworks

Governance structures and security architectures that ignore how an organization actually functions get worked around. We build programs that fit the operational reality of the client, not the theoretical baseline of a compliance document. One approach protects the audit. The other protects the organization.

Past Performance

Cytadel's foundation is more than two decades of direct operational experience supporting national security and enterprise programs at the federal level. Our leadership has worked directly with senior officials responsible for cybersecurity posture, system authorization decisions, and large-scale modernization efforts across mission-critical environments.

The work required more than technical knowledge. It required understanding how security risk lands at the leadership level and how to communicate it in a way that drives decisions rather than delays them. That included managing compliance readiness, preparing organizations for audits, evaluating emerging technologies before adoption, and keeping technical teams accountable to executive-level requirements.