CyberSecurity in the Federal Space

Reducing cybersecurity risks is essential to maintaining stable operations, protecting information, and assuring privacy.

VETS Core Competency Areas

Integrated Security
DevSecOps and Continuous Monitoring improve solution delivery of secure systems.

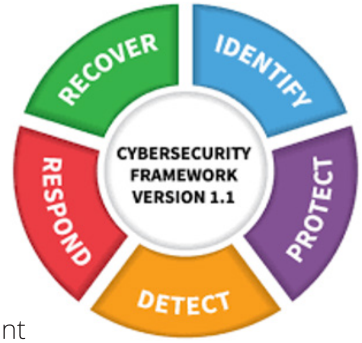
Hardening Solutions
Aligning to Federal cyber policies reduces vulnerabilities, attack vectors, and security events.

Security Playbook
Embedded offensive, defensive, and proactive security testing mitigate cybersecurity risks.

Cybersecurity Solutions

VETS is equipped to tackle the critical security challenges of our time. We bring a Top Secret (TS) Facility Clearance, staff with Public Trust, Secret and TS clearances, and more than a decade of experience protecting mission-critical infrastructures for our Federal customers. We execute cybersecurity functions that support Federal initiatives, including 24/7 risk analysis support, Command Cyber Readiness Inspections (CCRI), and FISMA compliance. Our approach integrates security with all facets of development and operations. We use a Continuous Integration and Continuous Delivery (CI/CD) framework to increase deployment frequency by using tool automation, Agile processes, DevSecOps, and cybersecurity best practices. We help Agencies shift traditional thinking from IT siloes towards distributed responsibility for cybersecurity, knowledge sharing, and effective use of CI/CD automation tools and processes.

Functional Expertise within a NIST Framework



VETS has improved our customers' security footprints, and we help them pass their FISMA audits, complete their security authorizations, and address their POA&Ms. We support Agency-wide initiatives, including:

- Federal Cyber Strategy
- Information Security Continuous Monitoring Mitigation
- Anti-Phishing & Malware Defense
- Risk Management Framework
- Identity, Credential, and Access Management
- Continuous Diagnostics and Mitigation

VETS Proven Experience

Disaster Credit Management System (DCMS) Support for the Small Business Administration (SBA) Office of Disaster Assistance (ODA)

Size: The SBA Consolidated Hosting Services contract is a single-award $19.4M TO.

Scope: The ODA provides financial support to small businesses in the event of a natural disaster. As the prime contractor, VETS is responsible for maintaining a fully functional system and supporting high user demand during emergencies. We provide network, system, and database administration services for all SBA environments; IT engineering and administration; support for IT security requirements across a broad spectrum of platforms and applications and facilities; Tier 2/3 Help Desk support; Information Assurance (IA), Disaster Recovery, and Continuity of Operations (COOP) support.

Complexity: We design, develop, implement, and support the infrastructure for ODA's applications, including 40+ Oracle and SQL-based databases, on premises and within the Microsoft Azure Cloud. We provide audit documentation and comply with FISMA guidelines; maintain security plans, policies, and procedures; and conduct security operations services such as vulnerability scanning, patching, and malware infection prevention.

Cybersecurity Expertise.

- Develop and maintain System Security Plan.
- Conduct Security Assessment and Authorization activities (e.g., risk assessment, vulnerability scans, penetration testing).
- Address POA&M items for tracking and resolution.

US Transportation Command (USTRANSCOM) Surface Deployment & Distribution Command (SDDC) Common Computing Environment (CCE)

Size: The SDDC CE contract is a single-award $24.6M Task Order (TO).

Scope: SDDC facilitates the Army mission by deploying and sustaining global forces. As the prime contractor, VETS managed the cloud-based and on-premises infrastructure that supports more than 10,000 world-wide users. We designed, implemented, maintained, sustained, and enhanced the Centralized Enclave (CE) domains (prod, staging, dev, training, COOP, AD, VDI), and provided enterprise Configuration Management (CM), migration planning and execution, Information Assurance (IA), and architecture planning support.

Complexity: The CE is comprised of enterprise hardware, software, communications, and network equipment that supports 40+ SDDC applications on 1000 VMs in a Veritas High-Availability (HA) or MS cluster configuration. We performed hardware and operating system upgrades, installed patches, maintained backup systems, authored system and other documentation, managed assets, maintained the Risk Management Framework certification, provided Tier 3 support, and conducted recovery operations.

Cybersecurity Expertise.

- Secure systems with DOD Security Technical Implementation Guides.
- Implement Continuous Monitoring for security events both on-premise and in AWS.
- Perform incident handling of security events.