



Bespoke cybersecurity solutions crafted to meet your unique digital challenges

FEIN: 46-2221006 DUNS: 080198593 UEI: QMGZDKJ78G96 CAGE Code: 7NLF0

CAPABILITY STATEMENT

InterSec focuses on protecting your business's digital assets and infrastructure from ever evolving cyber threats. Our cybersecurity solutions are tailored for smooth integration with your existing systems and processes, combining advance security measures with expert tradecraft for robust resilience and operational efficiency.

Our services significantly reduce cyber risk, comply with industry regulations and mandates, strengthen your operations, maintain reputation , and provide uninterrupted business continuity.

Threat & Vulnerability Management

- Threat Modeling and Attack Simulation
- Secure SDLC
- Application Security
- Penetration Testing
- Vulnerability and Risk Assessment
- Cyber Supply Chain Risk Management

Security Architecture & Engineering

- Zero Trust
- Secure By Design
- Secure AI
- Data Loss Prevention
- Mobile Device Security

Governance, Risk, & Compliance

- NIST Risk Management Framework
- FedRAMP
- NIST 800-171 / CMMC / ISO 27001 /
- NIST CSF
- High Value Asset Assessment
- Security Awareness Training
- Phishing Simulation

Advisory and Consulting

- Cyber Program Development
- vCISO
- Managed Security Services
- Cyber Workforce Development
- Cyber Staffing Solution
- ISSO

Differentiators

At InterSec, we prioritize your security, tailoring cybersecurity solutions to your specific business needs through strong client relationships. Our team's diverse expertise across consulting, digital solutions, and engineering ensures comprehensive, integrated cybersecurity responses.

Since 2013, our proven track record of delivering quality, cost-effective services underscores our commitment to your long-term security. Embracing a collaborative culture, we integrate our services with your operations, aligning with your business goals for enhanced effectiveness.

Contract Vehicles

Prime Vehicles : GSA 47QTCA19D00EG, GENEDGE CMMC BPA, VRS PENTESTING BPA
Sub Vehicles : Oasis+ 47QRCA25DSE20 (JV), CIO-SP3, 8(a) STARS III, GSA SCRIPTS BPA

Socio-Economic Designations

Minority Owned, SBA SDB
NMSDC MBE, MD MBE
VA, OH DBE

Quality Certifications

ISO 27001:2022, ISO/IEC 42001:2023
ISO 9001:2015

Industry Certifications

CMMC RPO, CISSP, CAP CCSP, CISM, CISA, CDPSE, LPT ECSA, CHFI, CTIA, CEH

Memberships

OWASP-NoVa, ISC(2)-NoVa, NVTC, The Cyber Guild

NAICS Codes

541511, 541512, 541513, 541519, 541611, 541612, 541618, 541690, 541990

Technology Partners



Our Clients



Business Contact

- 📞 +1-571-765-4235, 📧 inquiries@intersecinc.com
- 📍 13800 Coppermine Road, Herndon, VA 20171 | Work Area: Nationwide
- 🌐 www.intersecinc.com

Scan the QR code to book a 30-min no obligation call





Past Performances

| Title | Enhancing C-SCRM Compliance | Advancing Cybersecurity and Risk Management |
|--------------------|---|---|
| Client | Department of the Interior | Department of Army |
| Project Overview | As the prime contractor, InterSec Inc partnered with Exiger Government Solutions to help the Department of the Interior (DOI) meet EO 14028 on Cybersecurity Supply Chain Risk Management (C-SCRM). The goal was to streamline data collection for third-party vendor profiles to support cyber risk analysis. | As a subcontractor, InterSec Inc supported the Department of the Army in cyber and risk management, liaising up to the CIO/G6 level. The focus was on enhancing software security and mitigating ERP system risks to align with strategic goals. |
| Solutions Provided | <ul style="list-style-type: none"> Conducted Vendor, HBOM, and SBOM analyses to ensure genuine hardware and software use. Complied with OMB Memorandum M-22-18. Offered real-time risk monitoring and secure information sharing. Integrated C-SCRM capabilities with DOI's existing systems. | <ul style="list-style-type: none"> Strengthened software development security per DoD directives. Mitigated ERP system risks. Applied FinOps principles for cost-effective disaster recovery and business continuity. Managed global cloud-based ERP systems efficiently. |
| Results | <ul style="list-style-type: none"> Met federal cybersecurity mandates. Strengthened supply chain risk management. Improved DOI's overall cybersecurity posture. | <ul style="list-style-type: none"> Reduced security risks in software and ERP systems. Enhanced operational capabilities aligning with strategic objectives. Achieved cost savings in disaster recovery planning. Optimized global cloud resource management. |

| Title | Securing Information Systems | ISSO Services to CMS Marketplace |
|--------------------|--|---|
| Client | Administrative Office of The US Courts | Centers for Medicare & Medicaid Services |
| Project Overview | As a subcontractor, InterSec Inc provided Red Teaming and Penetration Testing services for multiple U.S. Courts systems, including 22 subsystems for case management and communications. | As a subcontractor to VETS, LLC, InterSec Inc provided AppSec, Penetration Testing, Secure Software Development, DevSecOps services for the CMS Marketplace systems for Federally Facilitated Exchange systems. |
| Solutions Provided | <ul style="list-style-type: none"> Implemented advanced security protocols. Ensured compliance with federal standards and Section 508. Provided cybersecurity training for court staff. Performed continuous risk assessments and maintained authorization to operate. | <ul style="list-style-type: none"> Provided compliance with EO 14028 in Zero Trust and Supply Chain Security. Assisted with CMS's Expedited Life Cycle (XLC) gate reviews. Ensured compliance with CMS Security ARS and Privacy Act requirements. Supported various assessments and audits (SCA, GAO, OIG, IRS, DHS RVA, CDM). Updated key documents: CMP, CP, and AMP annually. |
| Results | <ul style="list-style-type: none"> Significantly improved risk posture of US Court systems Achieved full compliance with federal security mandates. Meet DOJ security compliance requirements | <ul style="list-style-type: none"> Improved continuous ATO for CMS systems. Reduce risk of CMS HVA and FISMA High systems Ensured ongoing regulatory and EO compliance. Strengthened CMS's overall security posture. |

Business Contact

