InterSec
Ignite . Inspire . Innovate

CONTRACT VEHICLES

Prime: GSA 47QTCA19D00EG, GENEDGE CMMC BPA, VRS PENTESTING BPA

Sub: Oasis+ 47QRCA25DSE20 (JV), CIO-SP3, 8(a) STARS III, GSA SCRIPTS BPA

INDUSTRY CERTIFICATIONS

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

QUALITY CERTIFICATIONS

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

MEMBERSHIPS

OWASP-NoVa, ISC²-NoVa, NVTC, The Cyber Guild

NAICS CODES

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

SOCIO-ECONOMIC

Minority Owned · SBA SDB · NMSDC MBE · MD MBE · VA / OH DBE

TECHNOLOGY PARTNERS

Microsoft · box · PREVEIL · virtru · EXIGER

BOOK A CALL

30-min consultation

Scan to book
www.intersecinc.com

BUSINESS CONTACT

+1 571 765 4235
inquiries@intersecinc.com
www.intersecinc.com
13800 Coppermine Rd
Herndon, VA 20171 · Nationwide

Cost-Effective CMMC Compliance for the Defense Industrial Base

FEIN 46-2221006 **DUNS** 080198593 **UEI** QMGZDKJ78G96 **CAGE** 7NLF0

Our deep engagement with the DoD, Cyber-AB, nationwide APEXs, MEPs, industry groups, partners, and vendors uniquely positions us to understand the precise requirements for achieving CMMC compliance, for both DIBs and Federal Contractors. Our bespoke CMMC solutions streamline your path to compliance, saving time and costs while ensuring you meet all necessary standards efficiently.

170+
NIST 800-171 SSP, POA&M, and SPRS

200+
CMMC Level 1 Advisory

50+
CMMC Level 2 Advisory & MSSP

CMMC Service Lifecycle

01 Rapid CUI Scoping
Rapidly assessing your organization's CUI scope, security posture, and unique challenges to tailor your CMMC compliance efforts effectively.

02 CMMC Gap Assessment
Pre-audit to baseline existing cybersecurity readiness & map your existing processes to CMMC controls, identifying gaps.

03 Remediation, Documents & Audit Prep
Deep technical remediation expertise and audit-ready artifacts — swift system upgrades, policy drafting, and team training to meet CMMC standards.

04 Continuous Support & Maintenance
Ongoing support to ensure CMMC compliance, enhance cybersecurity resilience, and adapt to evolving threats and requirements.

Differentiators

Proven expertise and mature cyber services capabilities to meet your CMMC compliance needs.

- ✓ Cyber-AB RPO with seasoned CMMC SMEs.
- ✓ Dedicated security professionals throughout the entire compliance process.
- ✓ Strategic partnerships with vendors for turnkey, cost-effective solutions.
- ✓ Multiple service & price models customized to your needs.
- ✓ Technical guidance, policy, and staff training under one umbrella.
- ✓ 6–18 months to compliance, tailored to your scope.

Our Clients

BCF solutions · EFINEA *Capabilities Beyond Infinity* · SHOREPOINT · CYBERBAHN · IntellectFaces · ARRIKAI LLC

CYBER-AB CREDENTIAL
Registered Practitioner Organization

BPA AWARDEE
Manufacturing & Higher Education
GENEDGE · University of South Carolina · George Mason University

InterSec
Ignite . Inspire . Innovate

CMMC ENGAGEMENTS

Active CMMC Level 2 readiness programs for Navy ship repair, specialty metals, and defense R&D, delivered against the November 2026 enforcement deadline.

SERVICE AREAS

Supply Chain Risk Management, Application Security, Penetration Testing, ISSO Services, DevSecOps, Red Teaming, Risk Management, FinOps

FRAMEWORKS

CMMC, NIST 800-171, NIST 800-53, FedRAMP, FISMA, EO 14028 (Zero Trust & Supply Chain), Section 508

COMPLIANCE & AUDITS SUPPORTED

SCA · GAO · OIG · IRS · DHS RVA · CDM · DOJ · CMS Security ARS · Privacy Act

QUALITY CERTIFICATIONS

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

SOCIO-ECONOMIC

Minority Owned · SBA SDB · NMSDC MBE · MD MBE · VA / OH DBE

BOOK A CALL

30-min consultation

Scan to book
www.intersecinc.com

BUSINESS CONTACT

+1 571 765 4235
inquiries@intersecinc.com
www.intersecinc.com
13800 Coppermine Rd
Herndon, VA 20171 · Nationwide

CMMC engagements with the Defense Industrial Base

Naval Ship Repair Contractor

Marine boilers & pressure vessels · Founded 1986 · 5 active Navy ports

CMMC L2 · GCC HIGH · 5 SITES

CHALLENGE

SPRS score of **−203** at kickoff. Decentralized IT, mixed physical-access systems, and a workforce of direct, contractor, and temporary labor spread across **five active Navy ports** on the East and West coasts.

APPROACH

Five parallel workstreams on a biweekly cadence with a co-managed MSP partner. Standardized physical security across all locations, full hardware re-inventory with on-site validation, and migration to **GCC High** for CUI segregation.

OUTCOME

SPRS climbed from **−203 to −78** in four months. **GCC High live**, vulnerability scanning active, artifact gaps closing, and pre-assessment scheduled with the C3PAO. Shared-responsibility matrix is auditor-ready.

−203 → −78	5	GCC High	Pre-assessment
SPRS gain in 4 months	Naval port sites	CUI environment live	C3PAO scheduled

Specialty Alloys Manufacturer

Aerospace, defense, electronics & medical alloys · Founded 1965 · 4 facilities

CMMC L2 · MSP TRANSITION · GCC

CHALLENGE

Incumbent MSP could not produce the evidence assessors require — change logs, incident-response procedures, SIEM configurations — and a concurrent multi-site consolidation was moving the network footprint underneath the program.

APPROACH

InterSec called the MSP transition decisively, onboarding a CMMC-capable partner mid-engagement with SentinelOne EDR, RocketCyber SIEM, and ConnectWise change management. Rationalized 200+ artifacts in IntelliGRC and mapped the client's existing quality processes to NIST SP 800-171 controls.

OUTCOME

MSP transition **complete**. Clean CUI architecture: **4 dedicated workstations on an isolated VLAN**, GCC for email and storage, USB blocking, no physical media. Auditable evidence in place across change, incident, and log management.

MSP transition	4 users	200 → priority set	3 stacks
Complete & integrated	VLAN-isolated CUI	Artifacts rationalized	EDR · SIEM · change mgmt

Navy Calibration & Fabrication Contractor

Calibration, machine work, fabrication near Norfolk Naval Station · Self-assessment path · No internal IT

CMMC L2 · SELF-ASSESSMENT · LEAN SCOPE

CHALLENGE

Active Navy contract with a CMMC requirement, no prior cybersecurity program, no dedicated IT staff, and a tight budget. A two-person client team running a hands-on industrial business needed an auditor-ready program that would not overwhelm daily operations.

APPROACH

Right-sized the path: self-assessment, minimal CUI footprint, milestone-based pricing tied to SPRS score gates. Hands-on technical enablement on Nessus, OpenSCAP, PowerShell CMMC scripts, and WatchGuard, transferring capability to the client team rather than holding it.

OUTCOME

Lean CUI architecture stood up: **2 encrypted laptops**, segregated Wi-Fi, GCC subdomain for CUI mail. Full policy suite drafted by the client with InterSec review. SSP and POA&M live in IntelliGRC. **SPRS submission of 100–110** on track ahead of November 2026.

100–110	2 laptops	Milestone-priced	Client-owned
Target SPRS, on track	Total CUI footprint	Pay on SPRS gates	Sustainable program