VIPERBYTE SECURITY

USE CASE — PUBLIC SECTOR

Federal & Government Compliance:

CMMC Level 2 · GovRAMP Snapshot & Core · NIST 800-171

How Viperbyte provides continuous compliance evidence, eliminates ConMon overhead, and cuts the traditional CMMC/GovRAMP compliance stack cost by 47% — all on-premises, all under your control.

TARGET AUDIENCE	FRAMEWORKS	DEPLOYMENT TYPE	DOCUMENT DATE
DIB Contractors · Federal Agencies · GovRAMP Vendors	CMMC 2.0 · NIST SP 800-171 · FedRAMP · GovRAMP	On-Premises — Zero Data Egress	August 2026

1. The Public Sector Compliance Landscape — Why It Got Harder

> **THE MANDATE:** CMMC 2.0 (32 CFR Part 170) is now a contract requirement. Any organization that handles Federal Contract Information (FCI) or Controlled Unclassified Information (CUI) must meet Level 2 (110 NIST SP 800-171 practices) with third-party assessment (C3PAO) as a condition of contract award — not renewal, AWARD. Organizations that cannot demonstrate compliance will lose access to DoD contracts.

The public sector security compliance landscape has consolidated around two parallel demands: CMMC for the Defense Industrial Base (DIB) and GovRAMP for state/local government technology vendors. Both frameworks require the same core capability — continuous, documented, auditable security controls — and both now demand evidence, not attestation. Saying 'we comply' is no longer sufficient. You must show the proof.

80,000+
DIB contractors
requiring CMMC Level 2 compliance

110
NIST 800-171 practices
required for CMMC Level 2 certification

$247.6K
3-year Viperbyte cost for DIB
vs $463.5K traditional CMMC compliance stack

6–9 mo
to GovRAMP authorization
Viperbyte path vs 12–18 months traditional

The Three Compliance Problems Public Sector Organizations Face

The Problem	Who It Hits	What Happens
Evidence Gap	Any organization that has implemented controls but not documented them continuously	You tell the C3PAO assessor 'we have these controls.' They ask for evidence. You produce screenshots from this week. The assessor notes the evidence is point-in-time and cannot verify continuous operation. Finding issued. Certification delayed or denied.
Tool Stack Cost	Small and mid-size DIB contractors (50–500 employees)	Traditional CMMC compliance stack (SIEM + EDR + vulnerability

		scanner + GRC platform + C3PAO prep) costs $215K–$300K in year 1 alone. Many contractors cannot absorb this while remaining competitive on bid prices.
ConMon Burden	Any authorized organization with ongoing compliance obligations	Monthly ConMon artifacts — vuln scan results, incident reports, configuration change logs, POA&M updates — require dedicated staff or an MSSP at $7,000–$10,000/month. Most organizations have neither.

2. Five Public Sector Use Cases — Real Scenarios, Real Outcomes

2.1 Scenario: The CMMC Level 2 Pre-Assessment

Audience: CISO / Compliance Officer at DIB Contractor

The Problem:	C3PAO assessment scheduled in 60 days. Internal gap analysis shows 43 of 110 NIST 800-171 practices lack continuous evidence. Controls are implemented — but the logs are fragmented across five different tools, evidence is point-in-time, and the C3PAO will not accept self-attestation for Level 2.
Viperbyte Role:	Viperbyte's compliance dashboard automatically maps 43+ of the 110 NIST 800-171 practices to continuously-generated evidence artifacts. The assessor receives live dashboard access plus structured evidence exports — not a binder assembled the week before the assessment. Every covered control has a 365-day continuous evidence chain.
Outcome:	43 previously-gap controls now have documented, continuous evidence. Assessment timeline maintained. C3PAO assessor can verify any control on any date. No evidence gaps. $215,900 in avoided remediation costs vs assembling the equivalent evidence from scratch.

2.2 Scenario: The CUI Sovereignty Requirement

Audience: IT Director / General Counsel at DIB Contractor

The Problem:	Legal counsel flags that current cloud security infrastructure passes CUI through foreign-owned or foreign-operated services — a potential ITAR violation and a disqualifier under CMMC's CUI sovereignty requirements. Migrating to a FedRAMP Moderate-authorized cloud solution will take 18 months and $400K.
Viperbyte Role:	Viperbyte is deployed entirely on-premises. Zero bytes of customer data, network telemetry, or CUI indicators leave the facility. All AI processing, evidence storage, and compliance artifacts are generated and stored locally. The appliance has no mandatory cloud dependency and no data exfiltration capability. CUI sovereignty satisfied on Day 1 of deployment.

Outcome:	CUI sovereignty issue resolved without cloud migration. ITAR exposure eliminated. CMMC CUI handling requirements satisfied. 18-month cloud migration timeline avoided. Immediate compliance posture improvement.

2.3 Scenario: The Nation-State Advanced Persistent Threat

Audience: CISO / Security Team at Defense Contractor

The Problem:	A nation-state actor conducts a multi-month campaign against a Tier 2 defense contractor. Using legitimate credentials obtained via spear-phishing, they operate inside the network for 147 days without triggering any existing security alerts. The contractor has EDR on managed laptops but not on the engineering workstations running legacy CAD software. The workstations are the target.
Viperbyte Role:	Viperbyte's passive SPAN monitoring covers the engineering workstations agentlessly. Behavioral baselining identifies that the engineering workstations have never communicated with the identified C2 infrastructure in 12 months of operation. The first C2 beacon triggers an anomaly. The kill-chain AI model (GRU F1=0.897) recognizes the MITRE ATT&CK sequence within 72 hours of initial compromise — not 147 days.
Outcome:	Nation-state intrusion detected within 72 hours instead of 147 days. Forensic evidence chain documents the full kill chain for federal reporting requirements. Engineering IP protected. No ITAR-controlled design data exfiltrated.

2.4 Scenario: The CMMC Continuous Compliance Program

Audience: CISO / CFO at Mid-Size Defense Prime

The Problem:	CMMC Level 2 certification achieved. Now the ongoing obligation: annual re-assessment, monthly POA&M updates, continuous monitoring artifacts, and evidence preservation. The security team estimates 20+ hours per month of compliance-specific work — on top of running the actual security program.
Viperbyte Role:	Viperbyte's compliance dashboard generates all continuous monitoring artifacts automatically: monthly vulnerability scan results, incident report artifacts, configuration change logs, and POA&M supporting data. Every piece of evidence is timestamped, structured, and exportable in the format the assessor expects. Annual re-assessment prep time drops from 120+ hours to 8–16 hours.
Outcome:	20+ monthly compliance hours reduced to <3 hours. Annual re-assessment conducted in days instead of weeks. ConMon obligation satisfied without MSSP contract. $84,000–$120,000/year in MSSP costs eliminated.

2.5 Scenario: The GovRAMP Vendor Seeking State Market Access

Audience: CEO / CTO at SaaS / Technology Vendor

The Problem:	State government procurement office requires GovRAMP Snapshot authorization before vendor can be added to the approved product list. Traditional authorization path quoted at $465K–$610K with an 18-month timeline. Revenue from state contracts does not justify that investment at current pipeline size.
Viperbyte Role:	Viperbyte deployed in the authorization boundary serves as the SIEM, vulnerability scanner, network monitor, and ConMon engine simultaneously. Pre-authorization prep time drops from 12 months to 3–4 months because the evidence infrastructure is already running from Day 1. RPO engagement reduced to SSP writing only — not full evidence collection.
Outcome:	Authorization achieved in 4–6 months (vs 12–18 traditionally). Total authorization cost: ~$280,000 (vs $465K–$610K). ConMon obligation met by Viperbyte at $0 additional monthly cost. State government market access achieved at a cost justified by the pipeline.

3. Framework Coverage Map — CMMC / NIST / FedRAMP / GovRAMP

Viperbyte's compliance engine is framework-agnostic and maps to nine major frameworks simultaneously. The table below shows coverage level for each of the frameworks most relevant to public sector organizations. Coverage is driven by the same technical capabilities regardless of which framework label the auditor uses.

Framework	Level / Tier	Viperbyte Coverage	Primary Coverage Areas
CMMC 2.0 Level 1	17 practices	**FULL**	All 17 basic safeguarding practices: access control, incident response, media protection, physical protection, system & comms protection, system integrity.
CMMC 2.0 Level 2	110 practices	**SUBSTANTIAL**	43 of 110 practices with continuous evidence (ACCESS, AUDIT, INCIDENT, RECOVERY, RISK, SITUATIONAL AWARENESS, SYSTEM PROTECTION). Remaining 67 require policy docs + gap fills.
NIST SP 800-171	110 controls	**SUBSTANTIAL**	Same coverage as CMMC Level 2 (1:1 mapping). AU, AC-17, IA-3, SI-2, SI-3, SI-4 fully covered with evidence artifacts.
NIST SP 800-53 Rev 5	Low/Moderate	**SUBSTANTIAL**	17 Snapshot controls FULL coverage. 8 Core additions FULL. Remaining controls require policy layer. See GovRAMP Solution Brief for full table.

FedRAMP Low	~125 controls	**SUBSTANTIAL**	Technical controls for continuous monitoring, boundary protection, audit, and incident response fully covered. Policy and people controls require separate documentation.
GovRAMP Snapshot	~45 controls	**FULL**	All Snapshot-level technical controls covered with continuous evidence. Fastest path to state government market access.
GovRAMP Core	~125 controls	**SUBSTANTIAL**	Same as FedRAMP Low coverage. ConMon obligation satisfied by Viperbyte automatically.
SOC 2 Type II	Trust Criteria	**SUBSTANTIAL**	CC6-CC8 (Logical and Physical Access, System Operations, Change Management) covered with continuous evidence. Policy criteria (CC1-CC5) require documentation.
ISO 27001:2022	Annex A	**SUBSTANTIAL**	Network security, access control, incident management, and monitoring controls satisfied. ISMS policy documentation and risk assessment require separate engagement.

4. The Auditor's Perspective — Traditional Evidence vs Viperbyte Evidence

Government compliance auditors — C3PAO assessors, DISA SRG reviewers, GovRAMP 3PAOs — are trained to distinguish between controls that are implemented and controls that are demonstrably operating. The following table shows how the same control looks to an assessor from two different evidence packages.

NIST 800-171 / CMMC Practice	Traditional Evidence Package	Viperbyte Evidence Package
3.1.1 — Authorized Access Control (Access Enforcement)	Policy document. Screenshot of Active Directory groups from audit week. Manual attestation that unauthorized users are not present.	Identity Engine session log: every access event attributed to a named user, with device, source, timestamp, and authentication method. 365-day chain. Exportable on demand.
3.3.1 — Audit Logging (Event Logging)	Screenshot of SIEM dashboard from the week of assessment. Log export covering the last 30 days if a SIEM exists.	Continuous 365-day tamper-evident audit log. Every network event, DNS query, identity session, and enforcement action. Assessor queries any date range in real-time.
3.6.1 — Incident Response (Incident Handling)	Written IR plan document (often templated). No documented incidents to reference — either none occurred or none were detected.	Evidence chain for every detected incident: entity, behavior, confidence score, enforcement action, resolution, and MITRE ATT&CK technique classification. Auditor sees what actually happened, not what the plan says should happen.
3.11.2 — Vulnerability Scanning	Most recent scan report from Tenable or Qualys. Often a point-in-time scan run specifically for the assessment.	Continuous passive scan with on-demand Pentest Report. Timestamped. Assessor can see scan

(RA-5 / Flaw Remediation)		results for any month in the past year. CVE cross-reference against all observed services — not just managed endpoints.
3.14.6 — Malicious Code Protection (SI-3)	Screenshot of EDR dashboard showing managed endpoint coverage. Coverage percentage often below 100% due to unmanaged devices.	Network-layer malicious activity detection: DNS malware blocking, C2 callback prevention, behavioral anomaly detection on ALL network-connected devices. 100% network coverage — including the devices the EDR misses.
3.13.1 — Boundary Protection (SC-7)	Firewall rule export. Network diagram showing perimeter controls. No evidence of active enforcement decisions or lateral movement detection.	Enforcement log: every boundary decision — blocked, allowed, flagged — with IP, timestamp, and threat intelligence classification. Deception Layer events documenting any lateral movement attempts inside the boundary.
3.14.7 — Unauthorized Software (Least Functionality, CM-7)	Application whitelist policy document. Manual review during assessment — no continuous monitoring evidence.	Device behavioral baseline: any device running unexpected software surfaces as a behavioral anomaly. New process/protocol patterns trigger automatic alerts. Continuous software baseline vs static policy document.

> **WHAT ASSESSORS SAY:** A C3PAO assessor does not care what your security dashboard looked like the day before the assessment. They care what it looks like every day. Viperbyte doesn't produce assessment-day evidence. It produces every-day evidence. That is the entire difference between a FULL and a CONDITIONAL finding.

5. Cost Comparison — Traditional CMMC Stack vs Viperbyte

The following comparison uses a representative 50-user, 100-endpoint DIB contractor seeking CMMC Level 2 certification. Traditional stack figures are based on Viperbyte competitive analysis of published vendor pricing and industry-standard MSSP/C3PAO engagement rates.

Cost Component	Traditional Stack	Viperbyte	Notes
SIEM / Log Management	**$40K–$80K/yr**	**Included**	Viperbyte Network Intelligence Engine replaces SIEM entirely. No Splunk license.
EDR (additional coverage for agentless devices)	**$20K–$40K/yr**	**Included**	Viperbyte covers all agentless devices via SPAN. Existing EDR retained for managed laptops — not replaced.
Vulnerability Scanner	**$15K–$25K/yr**	**Included**	Viperbyte continuous passive scan + on-demand Pentest Report covers RA-5 requirements.
Network Boundary Monitoring	**$15K–$35K**	**Included**	Viperbyte nft/ipset enforcement layer with SC-7 evidence log.
GRC / Documentation Platform	**$15K–$30K/yr**	**Included**	Viperbyte compliance dashboard + evidence export covers most GRC platform functions.
C3PAO / RPO	**$100K–$150K**	**~$50K**	Viperbyte pre-maps

Engagement			controls. RPO writes SSP narrative only. Scope dramatically reduced.
Platform License (annual)	**~$100K (blended)**	**$47,000/yr**	Viperbyte all-in annual license. Hardware ~$3,500 one-time.

$463,500

Traditional 3-yr CMMC TCO

50 users / 100 endpoints — DIB contractor

$247,600

Viperbyte 3-yr CMMC TCO

Same scope — 47% below traditional stack

$215,900

3-year savings

Savings compound as ConMon costs eliminated

108

NIST controls with evidence

Out of 110 at 90-day mark + policy gap closes

6. Deployment Timeline — Day 1 / Day 30 / Day 90 for Public Sector

Milestone	Viperbyte Capability Active	Compliance Value Delivered
Day 1	• Network asset discovery — all devices profiled including unmanaged • Real-time threat intel matching (1.38M indicators) • DNS Security Engine — malware/C2 callbacks blocked • Deception Layer — 43 honeypots active as lateral movement tripwires • WAN threat enforcement pipeline active	Immediate boundary protection evidence. SI-3, SC-7, AU-2 begin generating compliance artifacts from minute one. First CUI data path visibility available. Any unauthorized devices visible in device registry immediately.
Day 30	• Behavioral baseline for all devices and user identities established • Insider threat model active — kill-chain detection live • MS365/Azure AD identity attribution wired • CMMC/NIST compliance dashboard populating • Evidence chain established for 40+ NIST 800-171 practices	30-day continuous evidence chain available for AU, AC, IA, SI controls. Identity-attributed access log satisfies 3.1.x AC practices. Gap analysis visible in dashboard — remediation priorities identified before assessor arrives.
Day 90	• 90-day evidence chain for all covered controls • Kill-chain AI model trained on organization's behavioral patterns • Vulnerability baseline current — CVE cross-reference active • Pentest Report exportable with 90-day history • Monthly ConMon artifacts generating automatically	Assessment-ready evidence package. C3PAO assessor receives live dashboard access — controls verified in real-time. 90-day chain satisfies CMMC continuous monitoring requirements. Evidence covers 43 of 110 practices with no remaining gaps in covered controls.

7. Getting Started — Public Sector Consultation

Viperbyte offers no-cost consultations for DIB contractors, federal agencies, and technology vendors pursuing government market access. We will review your current compliance posture, identify your evidence gaps, and provide a specific roadmap to CMMC Level 2 certification or GovRAMP authorization with timeline and cost estimates.

Deployment Process for Public Sector Organizations

- **Step 1 — Compliance gap review:** We review your current SPRS score (for CMMC) or GovRAMP gap assessment. We identify which of the 110 NIST 800-171 practices Viperbyte closes immediately and which require additional work.
- **Step 2 — CUI boundary identification:** We map your CUI data flows and identify where Viperbyte should be deployed for maximum coverage within your authorization boundary.
- **Step 3 — On-prem deployment:** Viperbyte appliance deployed at your facility or data center. No cloud dependency. No data leaves the boundary. CUI sovereignty maintained from Day 1.
- **Step 4 — Integration:** MS365/Azure AD identity attribution, LDAP connector, VPN session logging. All optional but recommended for maximum CMMC evidence coverage.
- **Step 5 — 30-day baseline:** 30 days of continuous operation before scheduling your pre-assessment review. Evidence chain verified and ready for C3PAO/3PAO submission.
- **Step 6 — Assessment support:** Viperbyte technical team available to walk assessors through the compliance dashboard and evidence exports during the assessment window.

> **READY TO TALK TO A FEDERAL COMPLIANCE SPECIALIST?** Contact Viperbyte Federal Sales:
> sales@viperbytesecurity.com · viperbytesecurity.com
> Tell us your CMMC target level, your current SPRS score, and your assessment timeline. We will give you a specific, honest roadmap — not a sales deck.