USCYBERCOM Capability Summary: PacketViper OT / Cyber-Physical Critical Infrastructure

Non-proprietary. Response to USCYBERCOM Command Challenge Problems (Edition 3). ≤2 pages.

1. Company Name: Viper Network Systems, LLC d.b.a. PacketViper, LLC **2. Company Website:** https://packetviper.com **3. Company POC Name:** Francesco Trama, Founder & CEO **4. Company POC Email:** frank.trama@packetviper.us **5. Company POC Phone:** 412-368-2077 **6. Company Overview:** PacketViper is a U.S.-based (Pittsburgh, PA) cybersecurity company and originator of Automated Moving Target Defense (AMTD, IP since 2011). It delivers preemptive, inline defense for IT and OT in a single agentless appliance, protecting operational technology and cyber-physical systems without installing anything on the protected devices.

7. Capability Name: PacketViper OT / Cyber-Physical Critical Infrastructure Protection (OT360 / Remote Security Units)

8. Capability Overview: PacketViper deploys as an agentless Layer-2 transparent bridge (no IP on the wire, hardware fail-open) in front of OT/ICS assets, PLCs, RTUs, HMIs, DCS, and inspects industrial protocols at the command/register level. It allows legitimate reads and authorized operations while blocking unauthorized or malformed **write/control** commands that would create cyber-physical effects (e.g., unauthorized pump start/stop, chemical-injection change, or traffic-signal/DMS manipulation). A positive-security trust model permits only defined systems to issue defined commands to each asset; deviations are blocked or alerted, surgically scoped to the source so a defensive action never causes an outage. Ruggedized Remote Security Units enforce autonomously at unattended/air-gapped sites and continue operating through network outages.

9. Capability / Technology Area Keywords: OT/ICS security; cyber-physical protection; critical infrastructure (CIKR); agentless transparent bridge; command/register-level protocol inspection (Modbus, DNP3, S7COMM, EtherNet/IP, BACnet, OPC-UA, NTCIP); Zero Trust for OT; virtual patching; passive asset discovery; SCADA; ICS deception.

10. Capability Availability: Available now (0 months; fielded). Orderable via Carahsoft **ITES-SW2 (W52P1J-20-D-0042, through ~March 2027)** and GSA Schedule. Hardware-agnostic and software-defined, deploys as a PacketViper ruggedized DIN-rail fanless edge appliance or rack appliance (TPM 2.0 hardware root of trust, measured boot, UL/IEC 61010 safety), as a virtual/cloud instance, or on customer-provided hardware, well suited to field cabinets, substations, and tactical-edge sites.

11. Technical Readiness Level: TRL 9 for fielded OT protection (proven in operational use; validated in a documented military-installation critical-infrastructure test, below); the NTCIP command-level enforcement module is TRL 6 (demonstrated on test bench / lab).

12. Applicable CYBERCOM Command Challenge Problems (CCP): - **CCP 1.2, Strengthen the Security of Critical Networks** *(primary):* Recognizes unexpected activity within CIKR control systems that can create cyber-physical effects. Command/register-level inspection of Modbus/DNP3/S7/EtherNet-IP and NTCIP-over-SNMP detects and (in enforce mode) blocks unauthorized control writes to physical devices; passive per-asset baselining flags deviation. **Validated:** in a documented test against a representative forward-operating-base's four utility segments (power, water, fuel, HVAC) under live attack, run in multiple configurations, **4 of 4 runs fully contained, <2 ms inline block, 4:12 average fabric-wide isolation, 99% alert reduction (312 events → 3 needing analyst action), 0% false positives, 47 unauthorized write commands blocked.** - **CCP 2.1, Zero Trust (for OT):** Positive-security "trusted partner" model, only defined sources may issue defined commands to each asset; agentless enforcement on legacy devices that can't host ZTA agents; micro-segmentation and source-scoped blocking. Results mapped against the **DoD Zero Trust for OT Activities & Outcomes framework (Nov 2025)** and **MITRE ATT&CK for ICS**. - **CCP 6.4, Critical Dependency Analysis:** Passive asset discovery, trust mapping, and Purdue-level classification produce an authorized-communication/dependency map across power and water assets, visibility that feeds dependency analysis.

13. What similar technologies exist today? OT monitoring/visibility tools (Claroty, Dragos, Nozomi, Armis) and traditional IT/OT firewalls. These are predominantly detect-and-alert or require SIEM/SOAR orchestration; most do not enforce inline at the command level, and agent-based tools cannot run on legacy PLCs/RTUs.

14. Differentiator / what is innovative: PacketViper is agentless and non-intrusive (transparent bridge, hardware fail-open, never a single point of failure), inspects OT protocols at the command/register level (not just port/5-tuple), and **blocks unauthorized control commands inline** rather than alerting after the fact. It adds active deception, virtual patching for unpatchable devices (~3,000 ICS CVE signatures), a software data diode for one-way enforcement, and cyber-physical correlation (physical door/motion/camera events fused with network events). It operates fully offline / air-gapped with local autonomy, built for contested, disconnected critical-infrastructure sites.

15. Compliance: a. **NIST 800-53 Rev 5 / 800-171 Rev 2:** Maps to / provides evidence across AC, AU, CA, CM, CP, IA, IR, PE, PM, RA, SA, SC, SI (incl. SC-26, SC-30, PM-8 Critical Infrastructure Plan) and 800-171 3.1/3.3/3.4/3.5/3.6/3.7/3.10/3.11/3.12/3.13/3.14. Also **IEC 62443**, **NERC CIP (incl. CIP-015-1 INSM)**, NIST 800-82. Structured for SCA / Authorizing Official review and cATO evidence. b. **CMMC:** PacketViper's built-in Compliance module maps **control-by-control to CMMC 2.0 Levels 1, 2, and 3**, generating live evidence (one framework within a 665-control / 29-framework mapping engine). Viper Network Systems meets CMMC control requirements and will pursue formal certification if required, for example in support of an Authorizing Official (ATO) process. c. **NIAP / NIST-FIPS:** PacketViper embeds FIPS 140-2 cryptography and operates in FIPS mode (self-contained, no external crypto dependency), using a FIPS 140-2 validated cryptographic module (validated OpenSSL + kernel crypto API; FIPS-mode toggle blocks non-validated algorithms). No separate product-level CMVP certificate; NIAP: not currently held. d. **CSfC:** Not applicable. PacketViper is an inline defense / AMTD / deception platform, not a commercial encryption or VPN component (the categories CSfC covers). Not listed on

the NSA CSfC Components List. e. **FedRAMP:** Not applicable. PacketViper is an on-premises, customer-controlled appliance (air-gap capable), not a cloud service offering. f. **DoD Impact Level:** Not separately authorized. DoD Impact Levels (IL2-IL6) apply to cloud service offerings under the DoD Cloud Computing SRG; PacketViper deploys on-premises inside the customer's own authorization boundary and operates at the impact level of the environment in which it is accredited. g. **Foreign ownership / export control:** Viper Network Systems, LLC is 100% U.S.-owned and staffed by U.S. citizens, no foreign ownership, control, or influence (FOCI). Commercial cybersecurity product; export governed under EAR (not ITAR/USML).

16. Currently in use by U.S. Government (examples): Available to Army, DoD, and Federal agencies via Carahsoft on Army CHESS **ITES-SW2 (W52P1J-20-D-0042)**. Production commercial critical-infrastructure deployments include remote water / pump-station protection and cabinet-level protection of 200+ legacy traffic controllers.