# Gino Pepenella, CISSP

Cloud and Infrastructure Security

g.pepenella@gmail.com | (352) 650-0088 | Orlando, FL | linkedin.com/in/ginopepenella | github.com/ginopepenella | portfolioxp.com

## WORK EXPERIENCE

**Cole Engineering Services, Inc.** Oct. 2024 - Present
*Senior Cyber Systems Security Engineer* *Orlando, FL*

Senior Engineer for the Persistent Cyber Training Environment (PCTE), U.S. Cyber Command's multi-tenant globally distributed training platform and the world's largest cyber range. Scaled the platform from 3 to 10 enterprise enclaves during tenure.

- Led zero-trust security architecture during expansion of VMware Cloud Foundation (VCF) and AWS GovCloud cyber training platforms.
  - Stack: VCF 9.0; AWS; NSX-T; Elastic SIEM; Tenable; Trivy; F5 WAF/IPS; Ansible; RHEL; PKI; SSO; Red Hat IdM/IAM; Red Hat Satellite; Cisco IOS/NX-OS; Cisco ISE.
- Conduct security architecture reviews for new platform capabilities and tenant onboarding, setting risk-based design requirements before deployment.
- Built automation and tooling that reclaimed engineering capacity and compressed audit cycles.
  - Ansible compliance auditing automation across Linux and Cisco fleets reclaimed roughly 40 engineering hours per week.
  - Containerized, PKI-enabled application consolidates thousands of system control checklists, cutting pre-audit prep by 40%.
- Authored the RMF accreditation package for the platform's AWS expansion: SecCONOPS, Incident Response (IR), Change Management (CM), BC/DR, and Control Implementation Policy (CIP).
- Owned platform vulnerability management using Tenable Security Center, prioritizing remediation by CVSS and asset criticality.
- Audited the entire infrastructure stack (VCF, Linux, Cisco, Kubernetes) and made risk acceptance and mitigation decisions.
- Mentored junior engineers; authored a process knowledge base adopted as the team's standard repository.

**Scientific Research Corporation** Oct. 2023 - Sep. 2024
*Cyber Systems Security Engineer* *Charleston, SC*

- Earned project ownership within six months after developing a pipeline to cut compliance scan time from 8 hours to 30 minutes.
- Owned one of the program's six system accreditation packages, including all system and control audit documentation.
- Authored the program's foundational security policies, defining implementation standards across all NIST 800-53 control families.
- Embedded shift-left gates (SAST, secrets scanning, SCA) into CI/CD pipelines, reducing post-release vulnerabilities.
- Automated Body of Evidence collection, cutting pre-audit prep by over 30% and saving hundreds of hours per quarter.

**United States Air Force** Jan. 2020 - Jan. 2024
*Cybersecurity Engineer, Network Control Squadron* *Oklahoma City, OK*

- Conducted 750+ security control inspections across mission-critical systems, shaping unit-wide hardening standards.
- Drafted Standard Operating Procedures (SOPs) and Contingency Plans (CP), formalizing unit-wide response and recovery procedures.
- Stood up Tenable Security Center, designed the network scanning process, and remediated findings with patching.
- Engineered network and host security controls across classified and unclassified systems.

**PEO Exchange (acquired by Alkeme Insurance)** Jul. 2018 - Nov. 2019
*Business Risk & Cyber Consultant* *Tampa, FL*

- Assessed 200+ enterprise vendors for data-protection controls, regulatory posture, and breach exposure.
- Advised clients on vendor risk strategy, reducing supply-chain risk exposure across their portfolios.

## EDUCATION

**University of South Florida** Tampa, FL
*M.Sc., Cybersecurity Intelligence and Information Security*

**Western Governors University** Salt Lake City, UT
*B.Sc., Business Administration (IT Management)*

## TEACHING

**ECPI University, Adjunct Professor of Cyber and Network Security** Nov. 2024 - Mar. 2026

Designed and taught Advanced Cybersecurity Lab, Governance Risk and Compliance, and Cloud Security college-level courses; coached students through Security+, CISSP, and CGRC certification tracks.

## CERTIFICATIONS & SKILLS

**Certifications:** CISSP (ISC2); CGRC (ISC2); CompTIA Security+ CE

**Technologies:** AWS GovCloud; VMware vSphere/VCF; NSX-T; Kubernetes; Docker; RHEL; Linux; Terraform; Ansible; Trivy; Python; Bash; PowerShell; Elastic SIEM; Splunk; Tenable/Nessus; F5 WAF/IPS; CrowdStrike; Microsoft Defender; IPsec

**Skills:** Security Architecture; Zero Trust (NIST 800-207); NIST 800-53 / RMF; FedRAMP; SOC 2; ISO 27001; CMMC; STIG/SCAP; CIS Benchmarks; Vulnerability Management; DevSecOps; Threat Modeling; Incident Response; MITRE ATT&CK; PKI; Third-Party Risk Management

## CLEARANCE

Top Secret/SCI (TS/SCI) Clearance