# LARRY PESECKIS

Greenwood Village, CO | larry.peseckis@gmail.com | linkedin.com/in/larry-peseckis | github.com/larrypeseckis | larrypeseckis.ai |
**DoD Cleared**

**Frontier Cyber Risk | AI Security & Cyber Safety Evals | Cloud Security | Defense & Aerospace**

## PROFESSIONAL SUMMARY

Cybersecurity and cloud security professional with 30+ years securing mission-critical defense, aerospace, cloud, Linux/Solaris, and multi-network environments, including current TS/SCI-cleared work supporting U.S. government satellite programs. Focused on building the connective tissue between cloud security, red team operations, blue team detection, DevSecOps, and LLM security. Public portfolio work includes a frontier cyber risk taxonomy, a 57-prompt cyber safety eval set, LLM-as-judge/human pilot results, LLM attack mapping, ML supply-chain security controls, and documented red/blue/cloud/LLM security labs. Known for translating complex technical risk into frameworks, controls, evaluations, evidence-based findings, and repeatable operational processes.

## SELECTED AI SECURITY & FRONTIER CYBER RISK WORK

- Developed and published a four-tier Frontier Cyber Risk Evaluation Taxonomy for AI-assisted cyber requests, classifying model-output risk by uplift, autonomy, authorization verifiability, and cumulative capability transfer.
- Built a companion 57-prompt Frontier Cyber Risk Eval Set spanning allowed, dual-use, high-risk, and disallowed tiers, with over-refusal traps, boundary cases, multi-turn assembly tests, and metrics for tier adherence, false refusal, reframing resistance, and incremental capability transfer.
- Ran a pilot cyber-safety evaluation against a frontier model using cross-family LLM-as-judge scoring and blind human grading; identified zero measured over-refusal on the pilot set, descriptive-label drift at boundary cases, and a content-triggered judge-abstention failure mode on severe Tier 4 prompts.
- Maintained public red team, blue team, cloud, and LLM security lab writeups documenting attack paths, defensive observations, tooling decisions, detection opportunities, and lessons learned to ground model-policy analysis in realistic cyber workflows.
- Developed AI security portfolio work including an LLM attack atlas, a Burp Suite Community REST API bridge validated across 7 PortSwigger labs, AI-assisted cyber risk analysis, and an ML supply-chain integrity gate using model scanning, safer artifact formats, signing/provenance concepts, and CI/CD enforcement.

## CORE COMPETENCIES

| | |
|---|---|
| **AI & Model Risk** | Frontier cyber risk, model policy, cyber safety evals, dual-use risk, LLM security, prompt injection, AI-assisted cyber misuse |
| **Security Operations** | Threat modeling, vulnerability management, detection and response, purple team operations, incident-style analysis, evidence reporting |
| **Cloud & Infrastructure** | AWS GovCloud, EC2, ECS, S3, VPC, IAM, RDS, Lambda, CloudTrail, CloudWatch, Security Hub, Linux/Solaris, VMware |
| **Governance & Execution** | FedRAMP, DoD STIG, RMF/NIST 800-53, Zero Trust, SOPs/runbooks, cross-functional coordination, Ansible/Bash/Python/Terraform |

## PROFESSIONAL EXPERIENCE

## Raytheon RTX | Aurora, CO

**Senior Principal Systems Administrator / Manager, Information Workplace Services** 2025 – Present

- Lead secure operations for mission-critical infrastructure supporting a U.S. government satellite program in TS/SCI/SAP environments, maintaining system integrity, privileged access control, operational continuity, and compliance across classified networks.
- Oversee administration of highly secure multi-network environments, including physical and virtual systems, privileged user workflows, classified infrastructure controls, and audit-ready operational processes.
- Coordinate across engineering, security, operations, and government stakeholders to resolve complex technical issues, manage risk, and sustain mission availability under high-stakes operational constraints.

**Principal Specialist, Information Workplace Services** 2021 – 2025

- Architected, deployed, and sustained the unclassified FORGE MDPAF environment, supporting 1,500+ Linux VMs, petabytes of storage, and 900+ users across geographically distributed government and military locations including Buckley AFB, the TAP Lab (Boulder), and DEV-C (Aurora).
- Automated multi-cluster deployments using Ansible and shell scripting, enabling parallel application versions and supporting a dozen teams with diverse operational requirements across classified and unclassified sites.
- Led patching, deployments, lifecycle management, troubleshooting, and high-tempo peer support across distributed teams as primary administrator for a large-scale mission-critical hardware and software ecosystem.
- Built and maintained technical documentation and repeatable troubleshooting procedures to improve consistency, reduce operational friction, and support cross-team execution in classified and unclassified environments.

**Senior System Integration Technologist II** 2019 – 2021

- Designed and prototyped secure AWS GovCloud environments for the GPS OCX program, enabling isolated lab infrastructure, automated deployment validation, and migration planning without introducing operational risk to production systems.
- Engineered and operated enterprise-scale AWS infrastructure using EC2, ECS, ELB, EBS/EFS, S3, VPC, IAM, RDS, CloudWatch, CloudTrail, Security Hub, SNS, and Lambda to meet strict FedRAMP and enterprise security requirements.
- Automated cloud provisioning, maintenance, teardown, cost tracking, and billing controls using AWS CLI, Lambda, and custom scripting to improve repeatability, visibility, and operational control.
- Designed and governed secure, compliant cloud architectures aligned with FedRAMP and enterprise security standards, including service classification, implementation guidance, logging, and monitoring controls.

**Senior System Integration Technologist I** 2016 – 2019

- Served as senior engineer on the GPS OCX support program, supporting configuration, integration, and deployment of mission-critical GPS satellite systems in partnership with DoD stakeholders during physical and security audits.
- Led administration of the GPS OCX System Integration and Transition Laboratory (SITL), maintaining a secure and stable environment supporting satellite operations and testing.
- Implemented DoD-compliant STIGs and physical hardening controls across Linux/Solaris and lab environments, improving security posture and audit readiness.
- Coordinated with VMware, IBM, and Dell to diagnose and resolve complex hardware and software issues, sustaining operational readiness across critical systems.

## General Dynamics | Pittsfield, MA

**Surface Ship Combat and Weapons System Engineer II** 2009 – 2015

- Led integration, deployment, and validation of naval combat systems across lab simulators and active U.S. Navy shipboard environments, managing end-to-end test cycles including planning, test procedure authoring, execution, and Navy-witnessed Level 1–7 acceptance testing.
- Served as Combat Management Systems (ICMS) Subject Matter Expert integrating complex interfaces including SeaRAM, SeaGiraffe AN/SPS-77, ESM 3601, SAFIRE III, Bofors 57mm Mk110, and LCS Mission Packages.
- Performed Linux/Solaris administration, system imaging, software deployment, troubleshooting, security remediation, and operational validation for mission-critical combat systems within a CMMI Level 5 environment.
- Applied DoD STIGs, DOORS-based requirements verification, and IBM Rational Change defect tracking to maintain security posture, traceability, and audit evidence across the system lifecycle.

- Briefed Navy and industry leadership on technical risks, installation strategies, execution status, and validation outcomes; earned the U.S. Navy LCS Bull Rider Award for technical expertise and program contribution.

**Additional Experience:** *Network Engineer & Systems Administrator, L&P Media | Systems Administrator, 5points.net, LLC | System Administrator, PSINet | Head Technician / System Administrator, CapitalNET / PSINet*

## CERTIFICATIONS

**AI / Cyber / Security:** CompTIA SecAI+, SecurityX, CySA+, PenTest+, Security+, Cloud+, Project+, Network+, Server+, A+ | ISC2 CC, SSCP, CISSP (exam scheduled July 2026) | CyberSec First Responder (CFR-410)

**Infrastructure / IT / Labs:** ITIL 4 Foundation | Linux Professional Institute Linux Essentials | TryHackMe SEC1, PT1, SAL1, AI1 | HackTheBox CJCA

## EDUCATION

**B.S., Cybersecurity and Information Assurance** — Western Governors University (expected Dec. 2026)

*Excellence Awards: Applied Cybersecurity (D333) | Legal Issues in Information Security (D828)*