

# Paul A. Haake, CSEIP

Senior Federal Security / Electronic Security Solutions Architect  
Access Control | Video | Intrusion | ESS Design, Integration & Commissioning

Merritt Island, FL 32953 | (760) 585-6485 | pahaake@gmail.com

## Professional Summary

Senior federal electronic security systems engineer with more than 20 years of experience designing, integrating, troubleshooting, testing, and supporting enterprise access control, video surveillance, intrusion detection, perimeter security, and associated server, storage, workstation, and network infrastructure. Experienced supporting federal and secure-facility projects from requirements development and site assessment through design documentation, integration planning, installation oversight, testing, commissioning, final acceptance, and operational turnover.

Strong background coordinating with customers, architects, engineers, cybersecurity teams, integrators, manufacturers, contractors, and project stakeholders. Recent work has included HSPD-12/FICAM-aligned PACS, PIV/CAC credentialing, STIG-aligned infrastructure, cybersecurity remediation, system migrations, complex integrations, and federal technical documentation.

Known for translating complex federal requirements into practical, supportable designs for agencies, integrators, partners, and high-compliance environments. Strong ability to connect physical security, IT infrastructure, cybersecurity, product behavior, field deployment realities, and sales strategy into solutions that can actually be deployed and defended.

## Core Expertise

Federal PACS architecture | HSPD-12 / FICAM | PIV / CAC / TWIC / PIV-I | Gallagher Command Centre | Controller strategy | HBUS | Mercury / LenelS2 / AMAG | IP video | Intrusion | Perimeter security | PSIM | RFID / RTLS | Data center security | Technical sales engineering | Takeoffs and estimating support | RFI/RFP response support | Competitive positioning | AWS / Azure concepts | NIST cybersecurity framework and RMF concepts | NIST SP 800-53 control alignment | STIG implementation and remediation | Cybersecurity coordination for physical security platforms | SOC 2 and cloud security/compliance concepts | Windows Server | Linux | VMware / Hyper-V / Proxmox | Cisco / Meraki | SQL Server | Docker | MQTT | Grafana | Splunk | ELK Stack | Python | OpenSSL research | Local AI tooling | Device schedules | Risers and one-line diagrams | Point lists | Integration matrices/interfaces | Enterprise storage architecture | NAS / SAN / DAS | NetApp and EMC environments | RAID and high availability | Backup, recovery and replication

## Professional Experience

### Gallagher Security — Riverside, MO

#### Senior Systems Engineer, Federal Solutions

March 2023 – Present

Support Gallagher's federal business through technical architecture, customer engagement, partner support, competitive positioning, product explanation, and opportunity strategy for federal, state, tribal, defense, and high-security customers.

- Design and support HSPD-12 certified access control solutions for federal, state, and tribal government agencies.
- Translate customer requirements into practical access control architectures covering controllers, readers, credential validation, integrations, cloud-readiness, and operational constraints.
- Support complex integrated solutions for national laboratories, defense environments, and high-compliance government facilities.
- Interface with hardware, software, cybersecurity, and product teams to identify defects, improve reliability, and communicate federal customer requirements back into engineering.
- Develop technical positioning around Gallagher Command Centre, Controller 6000 / Controller 7000 strategy, HBUS monitoring, reader lifecycle, secure controller architecture, and high-security credential migration.
- Support discussions involving AWS, Azure, FedRAMP sponsorship considerations, air-gapped deployments, and agency-specific security constraints.
- Create federal technical documentation, comparison material, RFI/RFP language, product positioning notes, and internal guidance for sales and engineering teams.
- Prepared and reviewed system architecture, device schedules, integration requirements, network and server dependencies, migration documentation, test procedures, and technical guidance for federal ESS deployments.
- Supported factory, site, and integrated system testing; diagnosed deficiencies across controllers, readers, credentials, databases, video systems, networks, and third-party interfaces; and drove issues through final resolution and acceptance.

**Selected impact:** Supported strategic federal conversations and opportunities involving CBP, GSA, SOCOM, USCIS, Department of State, Fish & Wildlife, DHS, FBI, national laboratories, and defense-related programs. Helped refine federal technical documentation covering Mercury comparisons, controller lifecycle positioning, C6000 / C7000 strategy, RFI responses, and Gallagher differentiation.

## LenelS2 — Rochester, NY

### **Senior Manager, Government Solutions**

April 2021 – February 2023

Managed and supported government security solutions for LenelS2, focused on FICAM / HSPD-12 certified access control deployments, federal customer requirements, cloud-hosted environments, and cybersecurity remediation.

- Managed and maintained FICAM / HSPD-12 certified GSA solutions for federal customers including VA, DoD, and civilian agencies.
- Created, updated, and managed physical and cloud-based AWS and Azure installations aligned with applicable Security Technical Implementation Guides.
- Provided subject matter expertise to cybersecurity teams to identify, remediate, and correct defects in government-facing product lines.
- Supported federal product strategy, customer requirements, solution validation, and technical documentation for government access control deployments.
- Applied NIST, STIG, FICAM, HSPD-12, and agency-specific cybersecurity requirements to physical security system architecture, infrastructure, interfaces, and remediation activities.

## Stanley Security — Fishers, IN

### **Manager, Sales Engineering**

May 2019 – April 2021

Provided technical leadership and subject matter expertise to sales personnel, national sales engineering resources, and government end users across electronic security technologies. This role was the point where earlier infrastructure, networking, and physical security experience converged into disciplined sales engineering, including technical design, takeoffs, estimating support, and federal access control solution development.

- Served as SME for IP video surveillance, electronic access control, intrusion detection, perimeter protection, and related security technologies.
- Designed HSPD-12 certified electronic access control solutions for federal government customers.
- Developed practical takeoff, estimating, and system-design discipline across complex access control, video, intrusion, and integrated security opportunities.
- Provided leadership, technical guidance, and field support to a national sales engineering team.
- Supported customer discovery, system design, proposal support, and technical sales strategy.

## Earlier Career Foundation

Before Stanley, built the technical foundation behind current federal physical security work through roles in infrastructure, networking, Cisco switching, video transport, IP surveillance, access control, PSIM, RFID/RTLS, customer consulting, project delivery, and hands-on systems work. Physical security became a primary focus during the Red River period, while the underlying Cisco/network/server work became essential to understanding how large security systems deploy, scale, and fail in the field.

Architected, staged, deployed, and commissioned enterprise-scale storage infrastructure supporting high-volume video and security workloads, including high-density disk arrays, storage servers, RAID, fiber and Ethernet connectivity, capacity planning, rack integration, system configuration, performance validation, and operational turnover.

Performed infrastructure sizing, rack elevation planning, rack-and-stack, server and storage configuration, network integration, burn-in testing, performance validation, troubleshooting, commissioning, and customer turnover.

- **KPH Communications — Solutions Architect, 2017 – April 2019:** Security consulting, cloud-enabled network design, project management, deployment, and training for education, financial, and commercial customers.
- **Red River Computer Company — Solutions Architect, 2014 – 2017:** Physical security SME for federal and commercial customers including DoD, VA, healthcare, banking, and retail; supported IP video, CCTV migration, access control, perimeter security, RFID, RTLS, PSIM, vendor coordination, and RFP responses.
- **Additional earlier roles:** Practice Lead, Physical Security, GTRI; Solutions Architect, Native Security Solutions; Consulting Sales Engineer, Iron Bow Technologies; Engineering Manager, Technology Integration Group; Network Services Manager, Nuera Communications; Manager of Technical Services, RF Microsystems; Programmer / Analyst II, University of California, San Diego.

## Independent Technical Work

Maintain an active lab environment for security monitoring, automation, video analytics, infrastructure testing, access control research, and AI-assisted technical workflow development. Current and recent work includes PIV/CAC/TWIC/PIV-I registration concepts, OpenSSL validation research, commodity data diode testing, MQTT and VMS automation, BLE beacon testing, Frigate/Home Assistant/Grafana/Splunk dashboards, and local AI tooling using Ollama, OpenWebUI, OpenClaw, and local model evaluation.

## Education & Certifications

**MBA** — University of Phoenix | **BA** — University of California

**Certifications:** CSEIP; HID pivCLASS Certified; Lenel OnGuard Professional; AMAG Symmetry 8 Certified; Axis Certified Professional; Vidsys Certified Engineer; Bosch

Certified Intrusion Expert; CompTIA Security+; Microsoft MCSA / MCSE; Cisco CSE / CCNA / IPTOS / CCVP; Check Point CCSA / CCSE

## Professional Style

Strong preference for live demonstration, practical architecture discussion, and direct customer discovery over generic slide decks. Effective with engineers, integrators, federal customers, executives, and field technicians because explanations stay connected to what can actually be deployed, supported, and defended.