

DAVID C. FLYNN

AI SECURITY ARCHITECT | AGENTIC AI | ZERO TRUST | LLM / MCP SECURITY

Laurel, MD 20708 | Local to Washington, DC and Baltimore | Remote / Hybrid / On-Site

301-367-5201 | davidflynn@eps-research.com | <https://www.eps-research.com> | GitHub: <https://github.com/eps-research/rag-corpus-series>

ORCID: <https://orcid.org/0000-0002-2768-6650> | CISSP (Active) | Able to obtain and maintain a U.S. security clearance

PROFESSIONAL SUMMARY

Cybersecurity and AI systems architect with 20+ years of experience across federal, financial, healthcare, cloud, and research environments. Currently Principal Investigator at EPS Research, an independent laboratory conducting applied research in AI systems, cybersecurity, and computational science. Proven record in NIST-aligned security architecture, Zero Trust, application security, cloud security, secure SDLC, vulnerability remediation, and enterprise risk. Hands-on AI specialization includes sovereign LLM infrastructure, RAG/CAG pipelines, agentic-AI evaluation, Model Context Protocol (MCP) security, semantic Zero Trust, persistent-agent risk, and multi-model validation. Published AI-security researcher and builder able to connect frontier AI capabilities with enforceable enterprise controls, auditability, and regulated-system requirements.

TARGET ROLES

Principal / Senior AI Security Architect | Cybersecurity AI Architect | LLM Security Architect | Agentic AI Security Lead | AI Red Team / Evaluation Lead | Zero Trust Architect | GenAI Risk and Governance Architect

CORE AI + CYBERSECURITY SKILLS

- AI / LLM Security: agentic AI, MCP hardening, prompt / tool-use risk, semantic policy enforcement, ontology and intent drift, model evaluation
- AI Engineering: Python, PyTorch, TensorFlow, scikit-learn, local LLM inference, quantization, RAG, CAG, embeddings, vector search, structured ingestion
- AI Infrastructure: sovereign AI, multi-node GPU/HPC systems, Blackwell and Ada GPUs, secure inference pipelines, Docker, Kubernetes, Ansible
- Cybersecurity Architecture: NIST CSF, SP 800-53, 800-171, 800-207, Zero Trust, microsegmentation, IAM, network and cloud security
- Application Security: Fortify, AppScan, Nessus, Qualys, secure coding, SAST/DAST, vulnerability triage, secure SDLC, DevSecOps
- Cloud / Platform: AWS, Azure, IBM Cloud Managed Services, SoftLayer, identity federation, encryption, logging, SIEM, infrastructure security
- Governance / Compliance: FISMA, CMMC, PCI, HIPAA, PII, security architecture review, risk assessment, ATO support, executive communication

SELECTED AI SECURITY & RESEARCH EXPERIENCE

Principal Investigator / AI Systems & Cybersecurity Architect | EPS Research

Laurel, MD | 2023-Present

- Designed and built a sovereign AI research environment using multi-node GPU systems for local inference, evaluation, scientific workloads, and security experimentation.
- Developed an AI-native Semantic Zero-Trust architecture for MCP tool use, including signed intent, hierarchical non-escalation, typed trust-labeled context, deterministic policy precedence, stateful risk memory, and separation of model planning from credential issuance.
- Built RAG/CAG and structured-ingestion pipelines using local LLMs, embeddings, vector search, Python, Langflow, Docling, Weaviate, and machine-readable JSON/JSONL outputs.
- Built and published the EPS Astro-RAG Platform and MCP Server, exposing five machine-readable research corpora through REST, semantic search, SSE, and Streamable HTTP for Claude, Copilot, and other MCP-compatible clients. Public implementation: <https://github.com/eps-research/rag-corpus-series>
- Developed cross-model evaluation methods for agentic behavior, refusal patterns, epistemic / ontology drift, persistent context, and heterogeneous multi-model review.
- Published peer-reviewed and preprint work spanning AI security, LLM evaluation, Zero Trust, MCP, HPC infrastructure, datasets, and computational astrophysics; maintains verifiable public artifacts through GitHub, ORCID, Zenodo, and arXiv.
- Built secure and reproducible AI workflows that combine model inference, tool access, scientific code, data provenance, adversarial validation, and explicit failure logging.

PROFESSIONAL CYBERSECURITY EXPERIENCE

Senior Cybersecurity Architect | ARMAVEL / U.S. Department of Veterans Affairs

Remote | 2023

- Authored Protective DNS architecture and guidance aligned with VA Directive 6403, CISA, and NSA direction.
- Produced Zero Trust and microsegmentation analysis based on NIST SP 800-207A and SP 800-204A/B patterns.
- Delivered CISSP-level training and architecture guidance for secure modernization initiatives.
- Participated in the Tier 4 Public Trust investigation process.

Senior Application Security Engineer / SME | Leidos / Social Security Administration

Woodlawn, MD | 2017-2018

- Led a remediation program addressing 32 million reported CVE findings through JRE modernization, Nessus/IAVA alignment, and coordinated application testing.
- Managed testing and implementation decisions across 62 stakeholders and multiple development teams.
- Performed architecture and secure-configuration reviews using Fortify, Nessus, secure coding standards, and federal security requirements.

Cybersecurity Architect | CenturyLink

Herndon, VA | 2016-2017

- Designed enterprise security solutions for cloud, network, application, DDoS, PCI, HIPAA, and PII requirements.
- Led customer-facing architecture reviews and integrated security capabilities from RiskSense, Imperva, ThreatConnect, QRadar, firewall, and IAM platforms.

Cloud / Application Security Architect | IBM - Federal and Commercial Programs

Washington, DC Metro / Remote | 2013-2016

- Delivered cloud and application security architecture across AWS, SoftLayer, IBM Cloud Managed Services, Oracle, and Watson Health environments.
- Led Platform IT security planning for U.S. Air Force civil-engineering systems spanning more than 80 bases, including industrial-control and IoT considerations.
- Designed LDAP federation, IAM, encryption, secure application architecture, and security-test strategies for federal and regulated clients.
- Performed and directed AppScan, Qualys, code-security, compliance, and cloud-control assessments; trained technical teams in secure development and CISSP domains.

Cybersecurity Project Manager / Security Lead | Business Integra / Internal Revenue Service

Washington, DC | 2013

- Managed a 12-person penetration-testing and code-analysis team supporting IRS security requirements and NIST SP 800-115-based test planning.
- Produced staffing, risk-mitigation, work-order, scope, and level-of-effort plans for red-team and blue-team security activities.

Security Consultant | U.S. Department of Commerce, OCIO

Washington, DC | 2013

- Developed enterprise risk-analysis processes, testing criteria, security metrics, mitigation plans, and FISMA / NIST SP 800-53A-aligned assessment workflows.
- Assessed applications, infrastructure, networks, telecommunications, and external services; authored practical security guidance and checklists.

EARLIER SECURITY, ENGINEERING & TESTING EXPERIENCE

Additional roles with General Dynamics, SAIC, Digex, Perot Systems, MCI Metro, Trusted Information Systems, Department of Labor, DHSS, Bureau of Engraving and Printing, Office of Inspector General, and commercial clients. Experience includes penetration testing, vulnerability management, secure SDLC, federal certification and accreditation / ATO documentation, application and database security, test automation, performance engineering, systems integration, and technical leadership.

SELECTED RESULTS

- Reduced or reconciled 32 million reported vulnerability findings during a major SSA Java modernization program.
- Created security architecture and policy deliverables for VA, SSA, IRS, Department of Commerce, Air Force, NARA, healthcare, financial, and Fortune 500 environments.
- Designed and operated sovereign AI / HPC infrastructure supporting local large-model inference, RAG/CAG, data engineering, and security research.
- Published 18+ research outputs and software / dataset records, including peer-reviewed astrophysics and current AI-security work.
- Taught cybersecurity, computer systems, orbital mechanics, robotics, and STEM programs at collegiate and continuing-education levels.

EDUCATION & CREDENTIALS

- M.S., Computer Science - Loyola University Maryland
- M.A., Catechetics - Christendom College Graduate School of Theology
- CISSP - Active
- IBM Cloud Architect | AWS Certified Solutions Architect - Associate (previous; recertification planned)
- Former Vice President, ISSA Baltimore Chapter

SELECTED PUBLICATIONS & TECHNICAL WORK

- Semantic Zero-Trust for Model Context Protocol (MCP), 2026 - agentic AI security control-plane architecture.
- Cognitive Integrity Security: Securing Human-AI Interaction in Large Language Model Systems, 2026.
- The Pathway to Implementing Zero Trust: Why Microsegmentation Remains the Critical Barrier, 2026.
- High-Performance Dual-Node AI Infrastructure for Astrophysics and Cybersecurity, 2025.

David C. Flynn | AI Security Architect | Laurel, MD 20708

- A New Empirical Fit to Galaxy Rotation Curves, Frontiers in Astronomy and Space Sciences, peer reviewed.
- GitHub / MCP implementation: <https://github.com/eps-research/rag-corpus-series>
- Complete publication record: <https://orcid.org/0000-0002-2768-6650>