# JOHN M. WILLIS

## PRINCIPAL AI SECURITY & RUNTIME GOVERNANCE ARCHITECT

john@johnmwillis.me | +1 (240) 720-7515 | johnmwillis.me | linkedin.com/in/johnmwillis

github.com/jwillisSFT/agcp-spec | github.com/jwillisSFT/pbsai-reference-architecture | ORCID 0009-0007-5889-9628

## PROFESSIONAL PROFILE

High-assurance systems architect and creator of Runtime Governance Engineering (RGE) and the Agentic Governance Control Plane (AGCP). Designs deterministic execution-layer controls that independently evaluate whether proposed AI or programmatic actions are authorized, admissible, supported by current evidence, and consistent with governing invariants at commitment time. Combines original AI governance architecture with decades of federal identity, cloud and software assurance engineering.

## DISTINCTIVE EXPERTISE

- Deterministic policy enforcement at action/commit boundaries; machine identity, provenance, canonical state and audit evidence.
- AI/agent security integration: runners, harnesses, governance context and independently enforced execution gates.
- Zero Trust, ICAM/PIV/PKI, AWS/cloud security architecture, NIST SP 800-53, FedRAMP and high-value asset assessment.
- Systems architecture, formal requirements, secure SDLC, production recovery and controlled release engineering.

## CURRENT ARCHITECTURE & RESEARCH

### SUSTAINABLE FUTURE TECH, INC. | Founder & Chief Innovation Officer; Principal Architect | Aug 2024–Present

- Originated the AGCP open specification and directs a private Rust implementation; specifies proposal, evaluation and commitment separation: “AI proposes → AGCP evaluates → Enterprise commits.”
- Sponsored and guided the 2026 CMU Heinz College capstone on runtime governance for AI-driven cybersecurity operations, including trusted-runner integration and engineering evidence.
- Created the PBSAI twelve-domain, 72-agent reference architecture and research on governance compilation, conformance and execution assurance.

### TURNAROUND SECURITY | Founder; C2C Security Architecture Consultant | Nov 2019–Mar 2025

- Delivered independent enterprise and federal security architecture work through a C2C contracting entity; pursued security-control modeling and AI-assisted engineering research.

## SELECTED FEDERAL ENGAGEMENTS

- **USPTO — via Zermount (Oct 2022–Feb 2025):** Cloud Advisory Team architect; assessed AWS security designs, FedRAMP/NIST controls, HVA concerns and scale-up versus scale-out architecture.
- **TSA — via Zermount (2021–Feb 2025):** Task Order Program Manager and Zero Trust identity SME; led a 50+ person governance/risk/compliance support organization and contributed to DHS Zero Trust identity planning.
- **U.S. Secret Service — Zermount W-2, then Turnaround Security C2C (Nov 2015–Feb 2021):** ICAM program architecture and PIV enforcement across hundreds of applications; participated in DHS and federal identity standards groups; $8.3M P&L responsibility and approximately $3M cost avoidance reported.
- **Library of Congress / CRS — via Zermount (Jul–Sep 2020):** Led root-cause investigation into PIV authentication failure, identified CA server issues and prepared RCA and mitigation recommendations.

## EARLIER TECHNICAL & LEADERSHIP EXPERIENCE

- **CMS — via CSC/GDIT (Oct 2014–Oct 2015):** Chief Security Architect and Principal ISSE on a $450M federal healthcare program; led recovery planning for enterprise Security Audit Logging and Reporting System (SALARS).
- **CA Technologies / Layer 7 — employee (Feb–Sep 2014):** Senior Services Consultant; deployed enterprise API/XML and mobile security gateways; developed technical implementation guidance.
- **DHS Science & Technology Directorate — via ICS (Aug 2013–Jan 2014):** Chief Security Specialist leading security control assessors, RMF/ATO package reviews, Fortify source-code assessment and Nessus vulnerability verification.
- **U.S. Mint — via SupremeSoft, then Lockheed Martin (Dec 2011–Dec 2012):** Program CISO/security engineering leadership; led vulnerability remediation, Cisco NAC recovery and ADFS-based authentication integration.
- **Foundational systems engineering:** MUOS satellite control build automation (2007); AMD production change control (2006–07); USAA WebSphere release automation (2004–06); GEC/Marconi embedded real-time avionics engineering (1978–86).

## EDUCATION & PROFESSIONAL DEVELOPMENT

- **University of Sussex:** MSc with Merit, Sustainable Development (degree conferred 2023).
- **MIT Professional Education:** Applied Data Science Program (2024); built and compared CNN classifiers for malaria blood-smear imagery. Selected model achieved 98.27% accuracy on a 2,600-image held-out test set (academic capstone; not clinically validated).
- **Oxford:** AI Governance: Technology, Ethics and Institutions (2024); Senior Leadership Executive Program (2024).
- **Carnegie Mellon University:** CISO Executive Education and Certificate Program (2018).
- **ISC2 credentials earned:** CISSP (2008), CISSP-ISSAP (2016), CSSLP (2015), CCSP (2017).

## PUBLICATIONS, EVIDENCE & TECHNICAL PORTFOLIO

- **Author:** *Runtime Governance Engineering*, Vol. 1: Foundations and Architecture (2026), ISBN 979-8-9971149-0-9; Vol. 2: Secure-by-Design AI—Deterministic Runtime Governance (2026), ISBN 979-8-9971149-2-3.
- **Author:** *Hybrid Quantum AI Systems Engineering* (2026), ISBN 979-8-9971149-1-6.
- **Research:** Governance compilation, formal execution semantics and safety invariants, AI-assisted SDLC assurance, and sequential AI inference.

## PUBLIC TECHNICAL MATERIALS

**AGCP open specification:** github.com/jwillisSFT/agcp-spec
**PBSAI reference architecture:** github.com/jwillisSFT/pbsai-reference-architecture
**Research & publications:** orcid.org/0009-0007-5889-9628