JOHN M. WILLIS

DIRECTOR OF AI GOVERNANCE ENGINEERING & ADVANCED SYSTEMS ARCHITECTURE

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

Technical founder, research director and engineering architect who turns novel governance concepts into executable specifications, engineering methods and verifiable system designs. Leads original research in deterministic runtime governance, controlled AI-assisted engineering and high-assurance architectures; brings cross-disciplinary depth in complex integration, program delivery, secure release engineering and operational risk.

DISTINCTIVE EXPERTISE

- Technology strategy, architecture authority and multidisciplinary engineering leadership.
- Governance compilation, formal requirements, interface/schema specifications and testable invariants.
- Engineering-state controls, source integration, release qualification, traceability and evidence-backed acceptance.
- Federal identity modernization, security operations leadership, high-assurance platform architecture and assessment.

CURRENT ARCHITECTURE & RESEARCH

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

- Created the RGE approach and AGCP operating specification, including deterministically enforced proposal-to-commit separation and test-oriented conformance architecture.
- Sponsored the 2026 Carnegie Mellon University Heinz College capstone; provided architectural guidance and requirements for trusted-runner and cybersecurity operations use cases.
- Established a controlled AI-assisted SDLC framework with architecture decision records, requirements testing, diagnosis registers, canonical project state and regression verification.
- Created the PBSAI twelve-domain cybersecurity reference architecture; directs an engineering and research portfolio spanning secure AI and advanced technical systems.

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

- **U.S. Secret Service — through Zermount/TAS (Nov 2015–Feb 2021):** Led ICAM architecture and engineering coordination; approximately $8.3M P&L, staff/vendor oversight and reported $3M cost avoidance.
- **TSA — via Zermount (2021–Feb 2025):** Task Order Program Manager; led 50+ governance, risk and compliance personnel and advised on identity/Zero Trust strategy.
- **USPTO — via Zermount (Oct 2022–Feb 2025):** Reviewed cloud security architecture, HVA controls and performance/capacity tradeoffs; evaluated scale-up versus scale-out designs.
- **CMS — via CSC/GDIT (Oct 2014–Oct 2015):** Chief Security Architect; led technical analysis and recovery planning for SALARS, a critical enterprise audit-logging service.

EARLIER TECHNICAL & LEADERSHIP EXPERIENCE

- **CA Technologies / Layer 7 — employee (Feb–Sep 2014):** First CA professional services consultant for the acquired product line; standardized technical guidance and deployed secure XML/API/mobile gateway integrations.
- **DHS Science & Technology — via ICS (Aug 2013–Jan 2014):** Led assessment personnel, rebuilt security processes, and coordinated ATO/security review across government and national-laboratory systems.
- **U.S. Mint — via SupremeSoft/Lockheed Martin (Dec 2011–Dec 2012):** Program CISO; eight direct technical staff and broader engineering oversight; vulnerability reduction and NAC recovery.
- **Enterprise software systems:** General Dynamics MUOS installation/build automation (2007); AMD fab software release controls (2006–07); USAA WebSphere automation (2004–06); Vanguard source control serving approximately 800 developers (1997–99).
- **Earlier engineering:** GEC/Marconi avionics embedded systems and electro-optics (1978–86); MCI enterprise telecommunications systems and releases (1993–96).

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