MICHAEL R. ROBINSON

Cloud Architect | DoD Cloud Modernization & Secure Architecture
St. Petersburg, FL | Remote / Relocation Eligible
727-313-1018 | michaelrobinsonjr@gmail.com
LinkedIn: linkedin.com/in/michaelrobinsonjr

CLOUD ARCHITECT SUMMARY

Cloud Architect with 15+ years supporting DoD mission environments and deep hands-on experience designing, delivering, and securing Azure Government cloud architectures at IL5/IL6. Proven leader in cloud modernization, DevSecOps enablement, RMF-aligned architecture, and ATO-ready cloud platforms. Trusted technical authority for senior government stakeholders, bridging mission requirements, security governance, and scalable cloud design across hybrid and multi-cloud environments.

CORE ARCHITECTURE & CLOUD SKILLS

Cloud Platforms

Azure Government (IL5/IL6) • AWS (Gov & Commercial) • OCI & GCP (Cloud One Exposure)

Architecture Domains

Enterprise Cloud Architecture • Secure Landing Zones • Network & Identity Architecture • Zero Trust Alignment • Hybrid & Multi-Cloud Design • Governance & Policy Architecture

DevSecOps & Automation

Terraform • ARM Templates • GitHub • Azure DevOps • Jenkins • CI/CD Security Integration • Infrastructure as Code (IaC) Governance • Secure Pipeline Design

Security & Compliance

RMF • ATO Support & Sustainment • DoD SRG • SCCA • NIST 800-53 • DISA STIGs • POA&M Management • Continuous Compliance Engineering

Leadership & Delivery

Technical Authority • Architecture Reviews • Trade Studies • White Papers • Senior Leadership Briefings • Agile / Kanban • Cross-Functional Engineering Leadership

---

PROFESSIONAL EXPERIENCE

Azure Cyber Security Principal

SAIC – Cloud One Program | Remote
2023 – Present

Serve as senior cloud and cybersecurity technical authority supporting the Cloud One Common Computing Environment, a globally distributed hybrid cloud hosting mission-critical USAF and Army workloads.

Architectural & Strategic Responsibilities

- Act as security and cloud architecture authority for Azure IL2/IL4/IL5

environments
- Define inheritable cloud security controls aligned to NIST 800-53, SRG, and RMF requirements
- Design secure-by-default cloud reference architectures adopted across multiple programs
- Partner with DevOps and platform teams to embed security into build and deployment workflows

Key Contributions

- Architected RMF-aligned cloud security patterns integrated directly into CI/CD pipelines
- Designed and implemented automated DISA STIG assessment pipelines leveraging Evaluate-STIG with ingestion into STIG Manager for continuous compliance visibility
- Implemented scalable STIG enforcement frameworks using DSC, GPO, Ansible, and Packer to support hardened golden images and repeatable secure deployments
- Improved vulnerability response workflows through integrated compliance telemetry and monitoring

---

Cloud Architect

SAIC – USCENTCOM J6 | MacDill AFB, Tampa, FL
2022 – 2023
Led a team of Cloud Engineers responsible for planning, designing, and implementing secure Azure Government IL5/IL6 cloud environments supporting CENTCOM modernization initiatives.

Architecture & Platform Leadership

- Designed secure landing zones including hub-and-spoke VNet architecture, segmentation, identity federation, and policy enforcement
- Implemented Zero Trust-aligned RBAC, encryption-at-rest/in-transit, and boundary control models
- Developed governance guardrails using Azure Policy and infrastructure validation pipelines

DevSecOps & Automation

- Architected DevSecOps ecosystems leveraging GitHub and Azure DevOps integrating security scanning and policy validation
- Developed reusable Terraform and ARM modules enabling standardized IL5/IL6 provisioning
- Embedded automated compliance validation within CI/CD workflows

Cloud Modernization & Analytics

- Spearheaded USCENTCOM's inaugural transition to Azure Government IL5/IL6
- Designed and implemented Azure Synapse Data Lakehouse architecture using medallion storage patterns
- Developed migration strategies for legacy systems transitioning to cloud-native

platforms

Governance & Accreditation

- Contributed to ATO documentation and authorization boundary definitions
- Conducted architecture trade studies and modernization briefings for senior leadership

---

Innovations Adviser – Cloud & Modernization

SAIC – USCENTCOM J6 | MacDill AFB, Tampa, FL
2020 – 2022

Served as strategic adviser within CENTCOM J6 Technology Innovation Branch guiding modernization initiatives across cyber, cloud, and network domains.

Strategic Modernization Advisory

- Evaluated emerging technologies for mission applicability, accreditation feasibility, and enterprise integration
- Conducted architecture trade studies assessing security, scalability, and sustainment risk
- Advised leadership on modernization roadmaps aligned to DoD enterprise strategy

Cloud & Security Alignment

- Ensured technology insertion complied with SRG, RMF, and SCCA governance
- Participated in Azure Government IL5/IL6 planning and accreditation activities
- Developed interoperability strategies for hybrid and coalition network environments

Executive Engagement

- Authored white papers and executive-level technical analyses
- Coordinated cross-functional planning sessions across cyber defense, network operations, and systems teams

---

Senior Cyber Infrastructure Analyst
Cyber Ops JRSS Migration Lead

SAIC – USCENTCOM | MacDill AFB, Tampa, FL
2017 – 2020

Led enterprise boundary defense operations supporting USCENTCOM HQ and theater components, ensuring operational resilience across mission-critical networks.

Architecture & Cyber Defense Leadership

- Designed and administered network boundary security architectures across HQ and deployed environments
- Evaluated emerging threats and implemented countermeasures aligned with operational and security mandates
- Interpreted and enforced DoD cybersecurity directives and operational cyber orders

Network Security Engineering

- Operated and optimized firewalls, IDS/IPS platforms, content filtering, and enterprise spam protection systems
- Recommended architecture modifications to mitigate risk while preserving mission availability
- Led multi-disciplinary engineering efforts supporting active and passive Computer Network Defense (CND) tool migration to JRSS stacks

Operational Impact

- Strengthened defensive posture across geographically dispersed mission systems
- Reduced operational risk through architecture-informed mitigation strategies
- Improved boundary visibility and cyber defense integration across HQ and theater operations

---

Network Operations SME – Senior

CACI / L3 NSS – USAF Southwest Asia AOR | Shaw AFB, SC
2011 – 2017

Served as senior technical lead supporting 17 Air Force bases across the Southwest Asia Area of Responsibility, delivering Tier 3 engineering, routing architecture, and enterprise security support for over 10,000 users.

Enterprise Network Architecture & Engineering

- Designed and maintained large-scale enterprise routing environments utilizing Cisco 7600/3900/2900 routers and Catalyst 6500 switching platforms
- Implemented and maintained BGP, OSPF, EIGRP, and MPLS-VPN routing architectures connecting remote bases and data centers
- Developed IP addressing schemes, VLAN segmentation models, and STP policies aligned to operational security requirements

Identity & Access Architecture

- Engineered Cisco ACS 5.3 environments supporting 802.1X RADIUS authentication and TACACS+ device administration
- Integrated Cisco ACS with Active Directory identity stores to enforce centralized authentication controls

Security & Infrastructure Operations

- Administered Nexus 7000/5000/3000 data center switches, ASA firewalls, EMC SAN, and UCS B/C series server infrastructure
- Managed McAfee Enterprise Firewall clusters in high-availability configurations
- Designed packet inspection rule sets and DNS zoning policies supporting secure enterprise operations

Operational Leadership

- Provided time-critical Tier 2/3 troubleshooting across WAN, data center, and VoIP environments
- Led engineering teams delivering resilient communications across geographically dispersed installations
- Proposed forward-looking technical solutions aligning near-term operational needs with long-term enterprise strategy

Network Operations Technician

L3 NSS – USAF Enterprise Network | Shaw AFB, SC
2010 – 2011

Provided enterprise-level operational support for WAN, server, firewall, and routing infrastructure supporting multiple Air Force installations.

- Delivered Tier 0–2 troubleshooting for WAN connectivity, firewall policy implementation, and server operations
- Configured and maintained DNS/BIND services across Microsoft and Unix environments
- Applied and troubleshot GPO changes within Active Directory domains
- Implemented DoD-approved hardening configurations for routers, switches, and Windows systems
- Provided remote network administration and firewall support across enterprise enclaves

---

EDUCATION

Bachelor of Science – Computer Engineering & Technology
Minor: Computer Science
Middle Tennessee State University

CERTIFICATIONS

- Microsoft Certified: Azure Solutions Architect Expert
- Microsoft Certified: Azure AI Engineer Associate
- ISC² Certified Cloud Security Professional (CCSP) – In Progress
- AWS Certified Solutions Architect – Associate
- CompTIA Security+
- Cisco CCNP / CCNA Security / CCNA Data Center
- ITIL v3 Foundation