BALD MAN TECHNOLOGIES, LLC

Cybersecurity & Network Engineering Services

SDVOSB Pending • 8(a) Applied • Hispanic-American Owned • Minority-Owned • Veteran-Owned • Tampa, Florida

UEI: U5DFU7U8GA54
CAGE: 1ZVH6
SAM.gov: Active

CORE COMPETENCIES

Cybersecurity Engineering & Compliance

Risk Management Framework (RMF) implementation, Authority to Operate (ATO) lifecycle support, NIST SP 800-30/37/53/137 control assessments, FIPS 140-3 validation, STIG hardening, ACAS vulnerability assessments, and continuous monitoring program development.

Penetration Testing & Offensive Security

External, internal, web application, and assumed-breach engagements aligned to NIST SP 800-115 and OWASP methodology. Rules of Engagement and authorization documentation, findings mapped to NIST SP 800-53 controls, executive briefings with technical appendices, and evidence packages suitable for A&A and POA&M ingestion.

Network Architecture & Secure Infrastructure

Enterprise network design and deployment including next-generation firewall (NGFW) configuration, high-availability (active/passive and active/active) architectures, IPSec site-to-site VPN with FIPS-validated cryptography (DH Group 21, SHA-512, AES-256-GCM), dynamic routing (BGP, OSPF, EIGRP), MPLS, QoS, VLAN segmentation, and PKI integration.

CMMC Readiness & Compliance Support

Cybersecurity Maturity Model Certification (CMMC) Level 1 and Level 2 readiness assessments, gap analysis, System Security Plan (SSP) development, POA&M management, and SPRS score support.

Cloud & Hybrid Security

Multi-cloud security architecture across AWS, Azure, and GCP environments. Identity and access management (IAM) integration, infrastructure-as-code (Terraform, Ansible) for consistent provisioning, and SIEM integration for centralized monitoring.

Information Assurance & Security Operations

Vulnerability management across DoD network enclaves, packet analysis (Wireshark, tcpdump) for incident response, custom automation development (Python, PowerShell, Bash) for compliance reporting and patch deployment, and security control implementation across classified and unclassified environments.

DIFFERENTIATORS

- **Active TS/SCI clearance** (next investigation 2027), eligible for sponsored work in classified environments
- **9+ years** of cybersecurity and network engineering experience across DoD, federal civilian, and commercial sectors
- **Senior offensive security credentialing**: GPEN, GXPN, GX-PT, and GCIH, an uncommon stack for a small business
- **28 active industry certifications** spanning cybersecurity, networking, cloud, and program management
- **Tampa Bay-based**, proximity to MacDill AFB, USCENTCOM, USSOCOM, and the regional defense industrial base
- **Hands-on engineering principal**, every engagement is led and executed by a senior-level engineer
- **Multi-category socioeconomic eligibility**: SDV, Hispanic-American, Minority-Owned, Veteran-Owned
- **Federal-side experience** across NIPRNET, SIPRNET, CENTRIX-K, and JWICS environments

PAST PERFORMANCE

Senior Information System Security Engineer

DoD Sensitive Information Networks • March 2024 – June 2025

ATO lifecycle support across **27 standalone classified environments**. Conducted semiannual continuous monitoring per NIST SP 800-137, executed RMF activities aligned with NIST SP 800-30/37/53, and remediated POA&M items in coordination with ISSOs and ISSMs. Designed and accredited a remote functional testing environment with FIPS-validated IPSec tunneling, internally maintained PKI, and physical/logical network segmentation. Developed Python, PowerShell, and Bash automation for STIG enforcement and ACAS-based vulnerability auditing.

Cybersecurity Engineer

Federal Aviation Training Systems • July 2022 – March 2024

Designed and implemented secure network architectures supporting aircraft training device development for federal customers. Deployed Cisco enterprise networking with EIGRP, DMVPN, and integrated NGFW solutions with custom Snort inspection profiles, AVC, and IPS. Built virtualization-based security suites on Hyper-V and ESXi with centralized logging, IAM via LDAP and SAML, automated patching, and high-availability configurations. Performed ISSE lifecycle activities under RMF in accordance with NIST SP 800-160.

Information Assurance Analyst

U.S. Army, 20th CBRNE Command • May 2017 – July 2022

Supported accreditation under DIACAP and RMF frameworks across **NIPRNET, SIPRNET, CENTRIX-K, and JWICS** environments. Maintained compliance posture across **250+ computer systems** through coordinated vulnerability scanning (ACAS), STIG enforcement, and patch management. Conducted risk assessments for network-wide implementations and automated data collection and patch deployment via custom PowerShell scripting.

CERTIFICATIONS

Cybersecurity (Senior/Expert)

GIAC Security Expert (GSE) • GIAC Security Professional (GSP) • CISSP • GIAC Strategic Planning, Policy & Leadership (GSTRT) • GIAC Defensible Security Architect (GDSA)

Cybersecurity (Specialist)

GIAC Security Essentials (GSEC) • GIAC Certified Incident Handler (GCIH) • GIAC Certified Intrusion Analyst (GCIA) • GIAC Python Coder (GPYC) • GIAC Penetration Tester (GPEN) • GIAC Exploit Researcher and Advanced Penetration Tester (GXPN) • GIAC Experienced Penetration Tester (GX-PT) • GIAC Experienced Incident Handler (GX-IH) • GIAC Experienced Cybersecurity Specialist (GX-CS) • GIAC Experienced Intrusion Analyst (GX-IA)

Networking & Infrastructure

Cisco Certified Network Professional - Enterprise (CCNP Enterprise) • CCNP Security • CCNA • CompTIA Network+ • CompTIA A+ • CompTIA Security+

Cloud & Linux

AWS Certified Solutions Architect - Associate (AWS SAA) • Red Hat Certified System Administrator (RHCSA) • Red Hat Certified Engineer (RHCE)

Program & Project Management

Project Management Professional (PMP) • GIAC Certified Project Manager (GCPM) • Certified Scrum Master (CSM)

Donovan Rodriguez
Founder & Principal Engineer
donovan@baldmantech.com
786-519-7464 • baldmantech.com

PRIMARY NAICS: 541512
Computer Systems Design Services
Secondary: 541519, 541513, 541611, 541990
PSC: DJ01, DG01, DE01, 7J20, 7G20