Angela Horga
Cloud & DevOps Projects | AWS | Terraform | RHEL Hardening | Security & Compliance (RMF, DoD)

◆ Mobile: (904)-327-9831 ◆ Pepperell, M A ◆angyhorga@gmail.com
https://www.linkedin.com/in/angela-a-horga/
https://medium.com/@angela.a.horga1

PROFESSIONAL SUMMARY

Results-driven IT professional with hands-on experience as an ISSO supporting DoD systems, seeking a role as a Cloud DevSecOps Engineer. Skilled in establishing continuous monitoring processes, implementing security best practices per NIST Risk Management Framework, and ensuring compliance with DISA STIGs. Adept at advising on cybersecurity policy, integrating secure practices across the system lifecycle, and supporting DevSecOps and Agile environments. Active Secret Clearance with proven success in risk management and secure cloud adoption.

PROFESSIONAL CERTIFICATION

- CompTIA Security+ CE | CompTIA CySA+ CE | AWS Certified Cloud Practitioner
- ACAS Operator & Supervisor Certified

SECURITY CLEARANCE: Active Secret Clearance

CORE COMPETENCIES & TECHNICAL SKILLS

- Cloud Computing Platforms: AWS (IAM, EC2, S3, VPC, GuardDuty, NATs, IP Gateway, Lambdas)
- Cloud Governance & Compliance: RMF, NIST SP 800-53, DISA STIGs, ATO documentation
- Systems & Networks: Windows & Linux (RHEL) admin, networking, RBAC/IAM, Active Directory
- Security & Monitoring: ACAS (Tenable.sc/Nessus), Splunk, CloudWatch, Security Hardening, Vulnerability Management, Incident Response.
- DevOps & CI/CD: Understanding of CI/CD pipelines, automation scripting (Bash)
- Infrastructure as Code: Terraform, Docker Compose, Kubernetes, CloudFormation

- **Infrastructure as Code:** Designed secure, reusable Terraform and CloudFormation templates to automate AWS deployments, reducing manual setup by 80%.
- **Containerization:** Built and deployed a hardened, Dockerized web app, demonstrating cloud-native security best practices.
- **Microservices Architecture:** Implemented an Auto Scaling Group and Load Balancer to showcase system resilience and elasticity.
- **Linux Automation:** Automated RHEL user account provisioning and file permission management with Bash.
- **IAM Security:** Authored a deep dive on IAM policy evaluation and cross-account role usage to strengthen least-privilege access.

PROFESSIONAL EXPERIENCE

Raytheon **April 2025 - Present**

IT Internal Auditor

- Conduct IT risk-based audits to evaluate security controls, system availability, and compliance posture.
- Collaborate with technical staff to recommend process improvements that improve system reliability and audit readiness.
- Deliver detailed compliance and risk reports to support executive decision-making.

Raytheon ◆ Andover, MA **July 2023 – April 2025**

Information System Security Officer (ISSO)

- Performed weekly system and security audits using Tenable.sc and Splunk, improving compliance and operational visibility.
- Developed and maintained Plan of Actions and Milestones (POA&Ms), System Security Plans (SSPs), and Risk Assessment Reports aligned with RMF and NIST SP 800-53 guidelines.
- Evaluated and approved hardware/software change requests to maintain system integrity and alignment with enterprise risk management protocols.
- Performed vulnerability scans, STIG reviews, and continuous monitoring with Splunk and ACAS, improving visibility and security posture.
- Managed end-user accounts, RBAC, and access controls, ensuring compliance with security and operational requirements.
- Supported ATO package reviews in eMASS, reducing review cycles by 25%.
- Performed continuous monitoring with Splunk to detect anomalies and strengthen security posture.

United States Navy ◆ Various Locations **April 2015 – June 2023**

Aviation Maintenance Administrator

- Administered configuration, deployment, and maintenance of Windows Servers in a secure operational environment.
- Maintained comprehensive IT asset documentation and responded to Tier I/II technical support tickets with a 95% resolution rate.
- Assisted end-users in troubleshooting hardware and software issues, providing timely resolutions and documenting incidents in accordance with Navy protocols.
- Managed technical publications, aircraft records, and engine logbooks to ensure regulatory accuracy and compliance.
- Utilized NALCOMIS (Naval Aviation Logistics Command Management Information System) to track maintenance events and analyze aircraft reliability trends.
- Controlled user account permissions, system configurations, and implemented access policies based on operational security standards.

EDUCATION

University of Maryland Global Campus ◆ Adelphi, MD August 2020 – December 2022

Bachelor of Science

- Computer Networks and Cybersecurity