

Luka Berg

Lead Cybersecurity Engineer

☎ (757) 555-0184 ✉ luka.berg@example.com 💼 linkedin.com/example/lukaberg 📍 Norfolk, VA 23510

SUMMARY

Lead Cybersecurity Engineer with seven years securing Navy training, simulation, shipboard, and integrated mission systems. Builds defense-in-depth architectures, RMF packages, A&A evidence, Cyber test procedures, and **Cyber Risk Mitigation Plans** aligned with **DoD Information Assurance**, DoDD 8115.01, **NIST SP 800-53 Rev. 5**, and NAVSEA business rules. Works directly with government stakeholders, IPTs, users, assessors, system administrators, and engineering teams to turn operational needs into secure, supportable system solutions. Hands-on work includes eMASS, ACAS, STIGs, SCAP content, **cross-domain interfaces**, system requirements, security specifications, vulnerability analysis, and authorization milestones. Holds a Bachelor of Science in Cybersecurity, Security+ IAT II, CAP, and an active Secret clearance. Ready to help protect mission-critical training systems through clear decisions, practical engineering, and accountable delivery.

EXPERIENCE

Lead Cybersecurity Engineer

Atlantic Mission Systems 📅 May 2023 - Present 📍 Virginia Beach, VA

Leads cybersecurity engineering for four Navy synthetic training system baselines, guiding architecture, RMF, vulnerability management, A&A, and government review activities. Mentors engineers and coordinates IPT decisions that keep accreditation evidence aligned with mission schedules.

- Led RMF execution across four Navy training baselines using eMASS and **NAVSEA business rules**.
- Built defense-in-depth diagrams for **sub-networks**, platform integration points, trust zones, and cross-domain interfaces.
- Traced **system requirements** to **NIST SP 800-53 Rev. 5** controls before authorization reviews.
- Created **Cyber test procedures** for boundary protection, accounts, audit events, and incident response.
- Converted ACAS findings, STIG gaps, and SCAP results into actionable **Cyber Risk Mitigation Plans**.
- Mentored three engineers through IPT sessions with government users, program managers, and software teams.

Cybersecurity Engineer

Bluewater Defense Technologies 📅 January 2021 - April 2023 📍 Newport News, VA

Managed cybersecurity execution for shipboard training subsystems across design reviews, testing, vulnerability remediation, and Assessment & Authorization. Maintained auditable RMF evidence and translated operator needs into security specifications for integrated engineering teams.

- Managed **eMASS** artifacts for system **security** plans, control statements, POA&Ms, and assessment evidence.
- Analyzed ACAS scans across Windows and network appliances, coordinating STIG remediation with infrastructure engineers.
- Documented operator needs as **system requirements**, scope statements, interfaces, acceptance criteria, and security specifications.
- Performed Cyber tests for segmentation, authentication, logging, and secure configuration across shipboard subsystems.
- Explained **DoD IA** policy implications during **IPTs**, helping users select practical security controls.
- Tracked retest status and technical evidence through recurring government **Assessment & Authorization** reviews.

Information Assurance Engineer

Coastal Integrated Systems 📅 September 2019 - December 2020 📍 Chesapeake, VA

Supported cybersecurity assessments for Navy training and simulation environments under senior engineering guidance. Organized evidence, prepared RMF artifacts, reviewed vulnerabilities, and documented system boundaries for design reviews and authorization milestones.

- Organized assessment evidence and validated control implementations for **Navy** training authorization milestones.
- Prepared eMASS **RMF** artifacts under senior guidance and aligned submissions with **DoD IA** policies.
- Reviewed ACAS output and component STIG requirements, separating false positives from remediation items.
- Created boundary, defense-in-depth, and cross-domain diagrams from configuration data and engineering drawings.
- Executed supervised Cyber tests for access control, audit logging, patch status, and boundary protection.
- Participated in integrated meetings with users, administrators, and stakeholders, recording risks and decisions.

PROJECTS

Navy Training RMF Modernization 📅 2025

Unified eMASS package maintenance, control traceability, ACAS review, STIG analysis, and authorization evidence for multiple Navy training baselines. Clearer ownership gave assessors faster access to defensible decisions.

Cross-Domain Defense Architecture 📅 2023

Mapped system boundaries, platform networks, sub-networks, trust zones, and cross-domain interfaces into practical defense-in-depth views. Diagrams gave engineering teams and government reviewers a shared basis for secure integration.

LEADERSHIP & AWARDS

- Cybersecurity Excellence Award, Atlantic Mission Systems, 2025
- Mission Assurance Peer Mentor Recognition, Bluewater Defense Technologies, 2022
- Dean's List, Old Dominion University, 2018

EDUCATION

Bachelor's Degree in Cybersecurity

Old Dominion University 🎓 GPA: 3.8 📅 2019 📍 Norfolk, VA

Coursework: Network Security, Risk Management, Secure Systems Design, Information Assurance

CERTIFICATIONS

- CompTIA Security+ (IAT II) 📅 2020
- Certified Authorization Professional (CAP) 📅 2022
- Active Secret Security Clearance 📅 2020

TECHNICAL SKILLS

- **RMF and Authorization:** Risk Management Framework, Assessment & Authorization, eMASS
- **DoD Compliance:** DoD Information Assurance, DoDD 8115.01, NAVSEA business rules
- **Security Frameworks:** NIST SP 800-53 Rev. 5, Security controls, Control inheritance
- **Vulnerability Management:** ACAS, Vulnerability scans, Finding remediation
- **Configuration Standards:** STIGs, SCAP content, Secure configuration
- **Security Architecture:** Defense-in-depth, System boundaries, Trust zones
- **Network Security:** Network segmentation, Platform networks, Sub-networks
- **Cross-Domain Engineering:** Cross-domain interfaces, Interface documentation, Boundary protection
- **Cyber Testing:** Cyber test procedures, Test evidence, Retest tracking
- **System Engineering:** System requirements, Security specifications, Acceptance criteria
- **Identity and Access:** Account management, Authentication, Access control
- **Audit and Monitoring:** Audit events, Audit logging, Incident response
- **Governance and Reviews:** IPTs, Working groups, Government stakeholder reviews
- **Platform Security:** Windows security, Network appliances, Patch status
- **Certifications and Clearance:** Security+, CAP, Secret security clearance

SKILLS

- | | | | |
|------------------------------|----------------------------|---------------------------------|---------------------------|
| • Risk Management Framework | • NIST SP 800-53 Rev. 5 | • STIG analysis | • Cross-domain interfaces |
| • Assessment & Authorization | • DoDD 8115.01 | • SCAP content | • System requirements |
| • DoD Information Assurance | • NAVSEA business rules | • Cyber test procedures | • Security specifications |
| • eMASS | • ACAS vulnerability scans | • Defense-in-depth architecture | |

PROFESSIONAL AFFILIATIONS

- Cybersecurity Engineering Mentor, Atlantic Mission Systems, 2024 - Present
- RMF Working Group Facilitator, Coastal Defense Cyber Forum, 2022 - Present
- Volunteer Presenter, Hampton Roads Cybersecurity Association, 2021 - Present

LANGUAGES

- English (Native)
- German (Intermediate)

ADDITIONAL INFORMATION

Work Status : Authorized to work in United States. No sponsorship required.

REFERENCES

AVAILABLE ON REQUEST