LOUGHTON BENNETT

Stuttgart, Germany | +1 (910)-999-7409 | loughton11@yahoo.com |
linkedin.com/in/loughtonbennett/ | github.com/Loughton03

INFORMATION SYSTEM SECURITY OFFICER | TS/SCI CLEARANCE | US MARINE CORPS VETERAN | RMF & NIST 800-53 | DISA STIGS | POLICY & AUDIT

PROFESSIONAL SUMMARY

Cleared security professional with a background in DoD and DoS environments, including 2.5 years assessing security controls in classified facilities. Assessed implementations against ICD 705 baselines, documented control deficiencies, and reported residual risk to system owners. Holds GSEC, GCIH, and GWAPT certifications, with GSEC meeting DoD 8140 IAT II requirements, plus an active TS/SCI clearance. Completed RMF Academy's ISSO Blueprint, including hands-on training in an eMASS emulator.

CORE COMPETENCIES & TECHNOLOGIES

RMF & Compliance: NIST SP 800-53, NIST SP 800-37 (RMF), ICD 705, DISA STIGs, NIST SP 800-171, NIST CSF, FISMA
Risk Management: Security Control Assessments, Continuous Monitoring, POA&M Development, Residual Risk Reporting, Corrective Action Tracking, SSP Support, ATO Package Preparation
Security Tools: eMASS, Tenable Nessus, Microsoft Sentinel, Microsoft Defender for Endpoint, Azure Monitor, Log Analytics
Cloud & Infrastructure: Microsoft Azure, Azure Bastion, Virtual Networks, NSGs, Azure Key Vault, Microsoft Entra ID, VMware, Oracle VirtualBox
Operating Systems: Windows 10/11, Windows Server, Linux (Ubuntu)
Technical Skills: KQL, PowerShell, Bash, Vulnerability Management, Threat Hunting, MITRE ATT&CK, Git, GitHub, Docker

EDUCATION

SANS Technology Institute - Bachelor of Science, Cybersecurity | Expected 2027
SANS Technology Institute - Applied Cybersecurity Certificate | 2026
American Military University - Associate of Arts, Interdisciplinary Studies | GPA: 4.0 | 2023

Certifications

- GIAC Web Application Penetration Tester (GWAPT) | April 2026
- GIAC Certified Incident Handler (GCIH) | November 2025
- GIAC Security Essentials (GSEC) - Meets DoD 8140 IAT II | April 2025
- GIAC Foundational Cybersecurity Technologies (GFACT) | December 2024

Professional Development

- RMF Academy | 5-Day ISSO Blueprint (Live Cohort) | June 2026
  Instructor-led RMF training with hands-on eMASS emulator: security control documentation, POA&M management, ATO package workflows, and continuous monitoring.

CYBER PORTFOLIO

Azure Honeynet — Microsoft Sentinel | NIST 800-53 | NIST 800-61

- Cut security events 85% on exposed Azure VMs. First captured a 24-hour baseline of 1,200+ malicious events, 800+ of them brute-force attempts. Then locked down the environment with NIST 800-53 controls: tightened NSGs, private endpoints, Key Vault private links, and Defender for Cloud.
- Analyzed privilege-escalation patterns in KQL and documented findings, aligning incident response procedures with NIST 800-61 to protect the environment's confidentiality, integrity, and availability.

Vulnerability Management — Tenable Nessus | NIST 800-53

- Ran authenticated Nessus scans on Windows 11 and found 25 critical and high vulnerabilities. Ranked each by CVSS severity and mapped them to NIST 800-53 RA-5, giving the system owner what they needed for POA&M tracking and remediation.

DISA STIG Remediation — PowerShell | DISA STIGs

- Achieved 100% remediation rate across 10 DISA STIG findings on Windows 11 by writing targeted PowerShell scripts and verifying each fix through registry inspection and post-remediation Nessus re-scans.

Threat Hunt — Microsoft Defender for Endpoint | KQL | MITRE ATT&CK

- Traced unauthorized TOR browser activity from download to outbound connection by building KQL queries across Defender for Endpoint telemetry sources, mapping the kill chain to MITRE ATT&CK and recommending endpoint isolation.

PROFESSIONAL & MILITARY EXPERIENCE

Construction Security and Reporting Technician *Aug 2023 – Present*

CACI (Dec 2025 – Present) · Amentum (Aug 2023 – Dec 2025) *Stuttgart, Germany & Sigonella, Italy*

- Tested physical and technical security controls at DoD sensitive compartmented information facilities against ICD 705 baselines, then monitored continuously to catch deviations from approved security plans.
- Wrote 200 security finding reports a year, 4 a week, covering control deficiencies, corrective actions, and residual risk.
- Flagged 8 findings a year for formal remediation and tracked each through closure.
- Briefed program managers across 5 stakeholder organizations on findings and residual risk, turning technical deficiencies into compliance guidance they could act on.

Cleared American Guard — U.S. Embassies *Aug 2020 – Aug 2023*

Coastal International Security / IDS *Iceland, Israel, Montenegro (return tour)*

- Inspected U.S. diplomatic facilities for security risks and enforced physical controls under Diplomatic Security Service standards, protecting classified operations.
- Assessed security for Site Security Managers, resolved compliance questions, and coordinated corrective actions with host-nation contractors.

Secure Storage Area Specialist *Jan 2020 – Aug 2020*

PAE *Frankfurt, Germany*

- Processed 500 supply manifests and 15 classified material shipments a month across multiple OCONUS locations, keeping chain-of-custody documentation and security compliance intact.

Cleared American Guard — U.S. Embassies *Feb 2016 – Dec 2019*

Coastal International Security *Chad, New Zealand*

- Ran 36 technical security examinations and risk assessments a year across OCONUS embassy postings, producing inspection reports under Diplomatic Security Service standards.

Marine Security Guard (MSG) / Training Manager *Aug 2011 – Nov 2014*

United States Marine Corps *Jordan, Pakistan, Brazil, Montenegro*

- Ran access control, personnel security, technical security device monitoring, and reaction force procedures at U.S. diplomatic facilities under Diplomatic Security operational control.
- Designed, coordinated, and led annual security training programs for MSG detachments, including continuous security education and drills that sharpened personnel readiness.