

NICHOLAS A. SOUTHERN

Cybersecurity Analyst · Governance, Risk & Compliance | Security Operations | AI Security

Greater Orlando, FL · 904-752-7085 · southerncybersolutions@protonmail.com

linkedin.com/in/nicholas-southern · cyber-southern.com · github.com/TheBaconSandwich

Active TS/SCI Clearance | DoD 8570 IAT II | GIAC GSEC | USAF Veteran

Open to contract, contract-to-hire, or direct · Available immediately · Remote, or hybrid/onsite in greater Orlando

Professional Summary

Cybersecurity professional with 6+ years spanning both sides of the security program: control assessment, risk management, and audit readiness on the governance side, and monitoring, incident response, and vulnerability remediation on the operations side. Federal and commercial experience across NIST 800-53 Rev 5 / RMF, NIST 800-171, NIST CSF, ISO 27001:2022, and SOC 2 Type II, including full authorization packages in eMASS and end-to-end GRC platform administration in Drata. Cleared the customer security attestations that unblocked \$1.2M+ in enterprise contracts within 30 days and cut audit preparation time by 40%. Four years of 24/7 DoD network defense for 3,000+ personnel across three Combatant Commands, including zero-day mitigation across 241 systems within 24 hours. Writes Python and PowerShell automation to replace manual evidence collection and compliance checking, and currently red teams large language models for prompt injection and adversarial risk. Active TS/SCI clearance.

Core Competencies

Governance, Risk & Compliance: NIST 800-53 Rev 5 · NIST 800-37 (RMF) · NIST 800-171 · NIST CSF · ISO 27001:2022 · SOC 2 Type II / AICPA Trust Services Criteria · CIS Controls · FedRAMP · HIPAA · DISA STIG · risk assessment & treatment · risk register & POA&M administration · gap analysis & remediation planning · control mapping, inheritance, tailoring & crosswalks · SSPs, control narratives & assessment reports · policy, standard & procedure authoring · continuous control monitoring · access recertification & periodic reviews · vendor & third-party risk (TPRM) · customer security questionnaires & attestations · auditor, assessor & customer inquiry response · security metrics & leadership reporting

Security Operations: SIEM monitoring & log analysis (Splunk dashboards, correlation rules, tuning) · endpoint detection & response · incident response, triage & escalation · threat hunting & root cause analysis · vulnerability management & scan validation (ACAS / Tenable Nessus) · STIG hardening & validation · zero-day response · indicators of compromise · audit log retention & dashboarding · 24/7 watch operations & shift handover

Platforms & Tools: Splunk · eMASS · Drata · ACAS / Tenable Nessus · McAfee HBSS · Active Directory · Microsoft Azure · Remedy / WebHelpDesk · Jira-style ticket workflows

Technical & Automation: Python · PowerShell · Bash · REST APIs · JSON / YAML · regular expressions · Git / GitLab · RHEL · Windows Server · IP networking · CI/CD and configuration-as-code review

AI Security: LLM red teaming · prompt injection defense · adversarial evaluation · model data-leakage testing · AI-assisted control and code review · local AI / security research lab

Professional Experience

Invisible Technologies

Dec 2025 – Present

AI Cybersecurity Specialist (Contract)

Remote

- Analyze emerging AI-driven attack vectors, focusing on prompt injection, jailbreak chaining, tool-use abuse, and adversarial manipulation of large language models, and document risk findings in artifacts consumable by both engineers and non-technical stakeholders.
- Conduct red team scenarios against model behavior to identify vulnerabilities, attack paths, and data-leakage vectors, then recommend and tune the controls that close them.
- Provide technical review of generated code and exploit paths, improving the reliability of AI-assisted threat analysis tooling; document methodology and results as reusable evaluation patterns other reviewers can apply.
- Author SOC and GRC scenario sets used to harden model behavior on incident response, NIST/ISO control mapping, and compliance reasoning tasks; translate operational security discipline (SIEM, IR, RMF) into evaluation rubrics and ground-truth signal.

ThreatLocker

Jan 2026 – Feb 2026

Cybersecurity Compliance Analyst, GRC (Contract)

Maitland, FL

- Unblocked \$1.2M+ in enterprise contracts (Visa, CIBC) within 30 days by aligning technical control implementations with client-facing attestation requirements and clearing the compliance findings holding up deal closure.
- Supported an active SOC 2 Type II and ISO 27001 program end to end: control design and documentation, evidence collection, and ongoing monitoring, producing attestation evidence on demand for enterprise customer security reviews.
- Served as primary Drata administrator from platform sourcing through rollout, building workspaces, program settings, and control mappings and replacing manual evidence gathering with automated collectors; shifted the organization from point-in-time auditing to continuous control monitoring and cut audit preparation time by 40%.
- Authored Python and REST API fetcher/validator scripts pulling configuration evidence from cloud and endpoint sources, normalized into platform-ingestible artifacts; decomposed NIST 800-53 Rev 5 controls into actionable engineering tickets with named owners and due dates, tracked to closure.
- Acted as liaison between leadership and external auditors, translating technical control implementations into client-facing assurance documentation; ran vendor security reviews (TPRM) against internal Zero Trust standards and supported the transition from FedRAMP readiness toward full authorization.

Lockheed Martin

Senior Information Security Analyst

Jun 2024 – Jan 2026

Jacksonville, FL

- Led control assessments across access management, change management, audit/logging, configuration management, and incident response; produced gap analyses with prioritized remediation plans and drove every finding to closure through formal POA&M governance.
- Authored full accreditation packages in eMASS, including system security plans, control narratives, assessment reports, and continuous monitoring plans, in the exact format the owning security organization and external assessors required.
- Onboarded new systems into an established, already-accredited program: determined which enterprise common controls could be inherited, then selected, tailored, and documented system-level controls only where inheritance was not available.
- Architected a new Information Assurance program from scratch for the customer Area of Responsibility, establishing baseline security protocols and governance documentation.
- Built continuous monitoring tying vulnerability scan output, configuration compliance status, and audit log retention into recurring leadership reporting, evidencing controls operating consistently across the monitoring period rather than at a single point in time.
- Engineered Splunk dashboards and correlation rules for real-time security event analysis, tuning detection logic to cut false positives and sustain 100% audit log retention; wrote Python and PowerShell utilities to automate compliance checks and evidence exports.
- Served as primary incident handler for system deviations and security alerts; executed vulnerability assessments and STIG hardening across RHEL and Windows fleets and enforced NIST 800-171 and 800-53 control implementation with system owners.
- Assessed account lifecycle and access review controls, verifying provisioning, transfer, and termination protocols were followed and documenting exceptions for remediation.
- Served as working liaison between engineering teams and the government security and assessment organization, answering control questions from primary sources and adapting implementations to assessor requirements; trained and mentored junior security administrators on RMF packages and standard operating procedures.

Five Stones Research Corporation

Information Assurance Analyst (Contract)

Sep 2023 – Nov 2023

Jacksonville, FL

- Supported ATO sustainment across approximately 200 servers and 2,000 workstations on classified networks; certified that baseline server and workstation images met NIST, ISO 27001, and HIPAA requirements before deployment, implementing STIG settings and back-out/recovery procedures as directed by DoD mandates.
- Configured and tuned McAfee HBSS for endpoint detection and compliance verification; performed forensic analysis of endpoint logs to identify indicators of compromise and managed incident response workflows under strict DoD reporting timelines.
- Supported IAVM vulnerability compliance scanning and mitigation planning.

United States Air Force

NOC Engineer & Systems Administrator

Apr 2019 – Jan 2023

Ramstein AB, Germany

- Managed 24/7/365 network defense operations for 3,000+ personnel across three Combatant Commands in a shift-based, globally distributed environment with formal watch handover; monitored, triaged, investigated, and escalated 1,000+ Tier 1/2 security and network incidents on JWICS/ISR classified networks.
- Mitigated zero-day vulnerabilities across 241 systems at 11 sites within 24 hours, completing RMF documentation that preserved accreditation with zero rework on the follow-up audit.
- Administered RHEL 6/7 and Windows Server 2012 R2/2016 and Active Directory for 500+ users at 99.9% uptime through patch management and proactive log monitoring; enforced DISA STIGs on GCCS servers and clients.
- Authored installation, use, and troubleshooting procedures adopted across the watch floor; modernized SOPs, trained new team members on physical and virtual server administration, and coordinated onboardings.

Automation Projects

Network Infrastructure Automation Suite

Python · github.com/TheBaconSandwich

2026

- Built a set of Python scripts against a multi-node lab network that inventory devices, poll availability, and dispatch SMTP alerts when a host stops responding.
- Integrated a REST ticketing API with token authentication to open and update tickets automatically on detected outages, with a shared helper module for reuse across scripts.
- Added DNS integrity checks that detect unauthorized zone changes, restore known-good records, and write status to a rolling log for review.

Education & Certifications

B.S., Cybersecurity & Information Assurance, Western Governors University

Expected December 2026

GIAC: Security Essentials (GSEC) · Foundational Cybersecurity Technologies (GFACT)

CompTIA: Security+ CE (DoD 8570 IAT Level II) · Network+ (N10-009) · A+

Service Management: ITIL 4 Foundation

Honors: USAF Distinguished Graduate, Cyber Systems Operations technical training, Keesler AFB (top 5%) · Honor Graduate, training flight (top 10%)

Languages: English (native) · Spanish (fluent)