NICHOLAS A. SOUTHERN

Governance, Risk & Compliance Analyst · Security Controls, Risk Management & Audit Readiness

Greater Jacksonville, FL · Remote · southerncybersolutions@protonmail.com · linkedin.com/in/nicholas-southern

Clearance: Active TS/SCI | Compliance: DoD 8570 IAT II

Professional Summary

GRC and compliance professional with 6+ years across risk assessment, control design, security assessment, and continuous monitoring in both federal (NIST 800-53 / RMF) and commercial (SOC 2 Type II, ISO 27001) environments. Experienced running controls through their full lifecycle — gap analysis, remediation planning, policy and narrative authoring, evidence collection, and finding closure through formal POA&M governance — and bringing new systems into established, already-authorized programs by determining what can be inherited and building only what can't. Hands-on GRC platform administration (Drata, eMASS) with Python/REST automation replacing manual evidence gathering. Proven as the working interface between engineering teams, leadership, and external auditors or assessment organizations.

Core Competencies

Frameworks & Standards: NIST 800-53 Rev 5 · NIST 800-171 · NIST 800-37 (RMF) · NIST CSF · ISO 27001:2022 · SOC 2 Type II / AICPA Trust Services Criteria · FedRAMP · DoD 8570

Risk & Governance: risk assessment & treatment · gap analysis & remediation planning · control mapping, inheritance & tailoring · crosswalks across frameworks · policy, procedure & control narrative authoring · POA&M / finding closure · audit & assessment support · vendor & third-party risk · continuous control monitoring

Control Domains: access management / IAM · change management · configuration management · logging & monitoring · incident response · vulnerability management · encryption & network boundaries · asset management

GRC & Security Platforms: Drata (administration, control mapping, automated evidence collectors) · eMASS · Splunk (SIEM) · ACAS · McAfee HBSS (EDR)

Technical: Python · Bash · PowerShell · REST APIs · JSON / YAML · Git · RHEL · Windows Server · Active Directory · Azure · CI/CD and configuration-as-code review

AI Security: LLM-assisted code and control review · prompt injection defense · red teaming

Professional Experience

Invisible Technologies Dec 2025 – Present

AI Cybersecurity Specialist (Contract) *Remote*

- Assess emerging AI-driven attack vectors (prompt injection, adversarial manipulation of LLMs) and document risk findings in artifacts consumable by both engineers and non-technical stakeholders.
- Conduct red team scenarios against model behavior to identify vulnerabilities and data-leakage paths, then recommend and tune controls to close them; provide technical review of generated code and exploit paths.
- Use AI-assisted tooling daily to search and interrogate source code and technical documentation, reading implementation directly rather than relying on summaries.

ThreatLocker Jan 2026 – Feb 2026

Cybersecurity Compliance Analyst – GRC (Contract) *Maitland, FL*

- **Compliance program support:** Supported an active SOC 2 Type II program end to end — control design and documentation, evidence collection, and monitoring — producing attestation evidence on demand to clear enterprise customer security reviews (Visa, CIBC).
- **GRC platform administration:** Served as primary Drata administrator from platform sourcing through rollout — workspaces, program settings, and control mappings — replacing manual evidence gathering with automated collectors.
- **Control mapping & remediation:** Decomposed NIST 800-53 Rev 5 controls into actionable engineering tickets, tracking owners and due dates through to closure.
- **Evidence automation:** Authored Python and REST API fetcher/validator scripts pulling configuration evidence from cloud and endpoint sources, normalized into platform-ingestible artifacts.
- **Auditor & executive interface:** Acted as liaison between leadership and external auditors, translating technical control implementations into client-facing assurance documentation.

Lockheed Martin Jun 2024 – Jan 2026

Senior Multi-Functional Information Security Analyst *Jacksonville, FL*

- **Risk & control assessment:** Led control assessments across access management, change management, audit/logging, configuration management, and incident response; produced gap analyses with prioritized, pragmatic remediation plans and tracked findings to closure through formal POA&M governance.

- **Authorization packages:** Authored full accreditation packages in eMASS — system security plans, control narratives, assessment reports, and ConMon plans — in the exact format the owning security organization and external assessors required.
- **Scope expansion into an existing program:** Onboarded new systems into an established, already-accredited security program — assessed which enterprise common controls could be inherited, then designed and documented system-level controls only where inheritance wasn't available.
- **Continuous monitoring:** Built recurring reporting tying scan output, configuration compliance status, and audit log retention together — evidencing controls operating consistently across the monitoring period, not just at point-in-time assessment. Wrote Python/PowerShell utilities to automate compliance checks and evidence exports; engineered Splunk dashboards supporting 100% audit log retention.
- **Primary interface role:** Served as working liaison between engineering teams and the government security and assessment organization, answering questions from primary sources and adapting controls to their requirements.

Five Stones Research Corporation Sep 2023 – Nov 2023
Information Assurance Analyst (Contract) *Jacksonville, FL*

- Configured McAfee HBSS for endpoint detection and compliance verification across classified networks; managed incident response workflows under strict DoD reporting timelines.

United States Air Force Apr 2019 – Jan 2023
NOC Engineer & Systems Administrator *Ramstein AB, Germany*

- Managed 24/7 network defense for 3,000+ personnel across three Combatant Commands; resolved 1,000+ Tier 1/2 incidents on JWICS/ISR networks and administered RHEL servers for 500+ users at 99.9% uptime.
- Mitigated zero-day vulnerabilities across 241 systems within 24 hours, preserving accreditation.

Education & Certifications

B.S., Cybersecurity & Information Assurance — Western Governors University Expected Dec 2026

Certifications: GIAC GSEC · GIAC GFACT · CompTIA Security+ CE (DoD 8570 IAT II) · Network+ · A+ · ITIL 4 Foundation