

# KETRICA R. GREEN

Dallas-Fort Worth, TX · 254-702-2582 · ketrica2002@yahoo.com

linkedin.com/in/ketrica-green-71112916 · ketricagreen.com

C|CISO · CISM · CISA · PMP · U.S. ARMY VETERAN

---

## SECURITY EXECUTIVE — DEPUTY CISO / HEAD OF INFORMATION SECURITY

*Regulated & Federal Environments · AI Risk & Governance · M&A Security · Enterprise Vulnerability Management*

---

### EXECUTIVE PROFILE

Security executive with 15 years across federal healthcare, defense, financial services, and telecommunications — including a sitting CISO role at Engility and vCISO / Trusted Advisor mandates at AT&T. Builds security functions where none exist: process, governance, tooling, and the executive reporting line that makes risk decisions possible.

Most recent proof point is operational, not advisory. Inherited an enterprise Azure estate carrying 223,596 open vulnerability findings and no remediation process of any kind — no intake, no triage, no ownership, no risk-acceptance path. Built the program from zero, wrote the Python tooling the team runs on, and dispositioned the entire baseline to zero.

Governs AI as a security discipline rather than a policy exercise. Designed and enforced an approval gate that blocks any local LLM from processing PHI until five mandatory controls pass, keeps cardholder data out of the model path entirely through tokenization and a broker pattern, and folds AI risk into existing HIPAA, HITRUST, SOX, and CMMC obligations instead of running a parallel program.

---

### LEADERSHIP SCOPE AT A GLANCE

**Team leadership** — Seven direct reports as CISO at Engility; an eight-person team at T-Mobile; a six-engineer vulnerability engineering team at Brillio.

**Program ownership** — Built and ran enterprise vulnerability management for a regulated Azure estate: 1,975 assets across 12 categories, monthly CIO reporting.

**Executive & board reporting** — Monthly technology risk and financial performance reporting to CIO, senior technology leadership, and audit committees across T-Mobile, Cognizant, and Brillio.

**Regulatory range** — NIST CSF & RMF, ISO/IEC 27001 & 42001, HIPAA, HITRUST, PCI-DSS, SOX, CMMC, GLBA, EU AI Act. Certified as both an ISO 27001 Lead Implementer and a PCI Qualified Security Assessor.

**Transaction security** — Cyber due diligence, integration, and separation across seven named transactions at four enterprises — from 200-employee carve-outs to T-Mobile's \$4.4B UScellular acquisition. IAM workstream ownership on both an acquisition and a divestiture.

**Federal & defense** — 150+ VA healthcare systems accredited under NIST RMF with ATOs achieved; DoD security control assessment at AAFES; A&A artifact development at Lockheed Martin; CMMC-CCP and CMMC-AB Registered Practitioner.

**Executive accountability** — CISO for a federal and defense services organization operating across a \$2.08B contract portfolio, leading a team of seven direct reports with security ownership spanning VA delivery task orders valued at \$15M–\$65M.

---

### PROFESSIONAL EXPERIENCE

**BRILLIO** | Frisco, TX · 2026 – Present

#### **Cybersecurity Principal Consultant — Vulnerability Management & AI Governance**

- Lead a six-engineer vulnerability engineering team owning end-to-end vulnerability management across endpoints, servers, cloud platforms, containers, and applications for a regulated Azure estate — discovery, triage, risk-tiering, remediation, verification, and exception handling.
- Dispositioned a 223,596-finding baseline across 1,975 assets to 100% closure: 129,825 remediated and 55,532 formally risk-accepted at CVE-asset grain, each with a documented compensating control, named owner, and scheduled re-review.
- Designed and secured formal adoption of the enterprise remediation RACI spanning Vulnerability Engineering, Application Teams, and Azure subscription owners — relocating accountability for unremediated risk from the security team to the asset owner, and producing the two-track routing model still in operation.
- Established KEV-first prioritization as the governing rule over raw CVSS. Of 787 CVEs in the baseline, 421 were retired through decommission of end-of-life virtual machines rather than consuming patch cycles; the remaining 366 were triaged, with the 126 KEV-rated CVEs expedited ahead of higher-scoring findings.
- Drove a region-wide AKS node-image update with Microsoft to clear cluster vulnerabilities that could not be self-patched; implemented ownership and environment tagging across AKS resources to make previously unassignable container findings routable.
- Rebuilt executive reporting on disposition, velocity, and KEV posture from a single governed source with data-integrity checks applied before publication; briefed the CIO monthly, including the capacity recommendation against a rising inflow rate.
- Design and audit cybersecurity frameworks for the medical sector, integrating secure healthcare AI and process automation under formal AI governance, with IT audit against HITRUST, SOX, NIST, and CMMC.

**T-MOBILE** | Frisco, TX (remote) • 2024 - 2025

**Senior Cybersecurity Lead — IT Risk & Financial Programs**

- Led a team of eight delivering enterprise IT audit and cybersecurity advisory programs aligned to the NIST Framework, measuring enterprise systems against external authorities and setting program maturity roadmaps.
- Executed end-to-end control mapping of 200+ regulatory requirements across NIST RMF, SOX, and ISO into ServiceNow for acquired entities, establishing a single source of truth for compliance and eliminating parallel compliance tracking across the combined estate.
- Owned the identity and access management workstream for the \$4.4B UScellular acquisition — T-Mobile's largest transaction since Sprint — directing identity and entitlement integration from announcement through close in August 2025.
- Directed enterprise vulnerability and audit programs on Nessus (Tenable) and Qualys; performed technical assessments of enterprise network security posture to confirm audit readiness.
- Operated SentinelOne as the enterprise EDR platform, integrating endpoint control evidence into audit programs and reconciling endpoint telemetry against scanner findings to establish true exposure.
- Reported technology risk and forecasted financial performance to senior technology leadership and executive audiences to guide strategic planning.

**COGNIZANT** | Dallas, TX (remote) • 2021 - 2023

**Senior Cybersecurity Program Manager — Mergers, Acquisitions & Divestitures**

- Led global client engagements across GRC, M&A, divestitures, and incident response, setting audit objectives and scope for rapid cybersecurity risk assessments of transaction targets and surfacing the critical gaps that informed deal decisions.
- Owned the IAM separation workstream for the Austin CSI divestiture, directing identity and entitlement disentanglement from the parent environment; also supported the One Source and TQS divestitures.
- Automated IT General Controls testing and continuous monitoring in ServiceNow, accelerating audit evidence collection by 40% and reducing exposure to control failures during transaction execution.
- Delivered executive-level ServiceNow dashboards for real-time risk posture and ITGC compliance reporting to senior leadership and audit committees.
- Directed incident response for a 2023 unauthorized data disclosure inside an acquired healthcare payer-services entity — inherited transaction risk materializing post-close. Ran accelerated compromise assessment, integrated continuous threat monitoring, and isolated the acquired entity's networks, directory services, and shared privileged accounts behind Zero Trust access boundaries to block lateral movement into the parent environment.
- Contained credential-harvesting exposure across 12,000+ exposed identity records to fewer than 75 actually compromised accounts, and cut mean time to contain from 72 hours to under 4 hours.
- Commanded incident response for a ransomware event in a PCI environment delivered through an over-permissioned third-party guest identity in SharePoint — validated segmentation as the first action and confirmed the cardholder data environment was unaffected, isolated 600+ privileged directory accounts to cut off lateral movement, held the infection to 15 development endpoints, and contained surgically rather than halting the collaboration platform. Closed the root cause through external-identity governance across the tenant.

**AT&T** | Dallas, TX (remote) • 2018 - 2022

**Senior Information Security Consultant | Trusted Advisor & vCISO**

- Served as Trusted Advisor and virtual CISO to enterprise clients, translating business drivers into security program roadmaps and developing courses of action for embedded cybersecurity challenges.
- Built the cross-functional coalition — IT operations, development, and compliance — required to deliver Zero Trust across an estate where no single team owned it, sequencing delivery to lead with identity and access management before micro-segmentation and continuous monitoring rather than attempting simultaneous enterprise rollout.
- Provided cyber due diligence and advisory support to Sysco Foods' Mexico joint venture divestitures, applying NIST, ISO, HITRUST, and SOX to shape security policy and program maturity.
- Scoped a security framework overhaul with client audit teams and executed plans for advanced SIEM and Zero Trust deployment.

**ENGILITY** | Irving, TX • 2016 - 2017

**Chief Information Security Officer**

- Held full CISO accountability for a federal and defense services organization operating across a \$2.08B contract portfolio, leading a team of seven direct reports with security ownership spanning VA delivery task orders valued at \$15M-\$65M across Health IT and EHR modernization, cybersecurity and compliance, and enterprise program management.
- Led technical security architecture for HIPAA and PCI-DSS compliant payment processing across 1,200+ global retail locations, implementing AES-256 encryption, tokenization, and secure transmission channels.
- Architected an enterprise-wide Third-Party Information Security Risk Assessment program with automated risk scoring and vendor questionnaires aligned to NIST 800-53 and ISO 27001.
- Directed enterprise audit and vulnerability programs on Nessus and Qualys, orchestrating remediation that cut critical vulnerabilities by 85%.

## SELECTED PROGRAM ENGAGEMENTS

---

**AI Governance Framework** — Designed and implemented an AI governance framework for rapid AI/ML adoption: model risk management protocols, ethical deployment guidelines, and data privacy safeguards. Built a mandatory approval gate requiring five P1 controls before any local LLM processes PHI — endpoint authentication, attributable audit, no PHI in logs, retrieval authorization, and model weight provenance — with additional controls gating agentic deployments. Result: 100% of AI models governed, 25% improvement in threat detection, and PCI scope held stable while AI capability expanded.

**Security Tooling Development** — Designed and wrote Sentinel, a Python application built from scratch to close a gap no vendor product addressed: automated playbook generation, KEV-based prioritization applied automatically, and compensating-control recommendations feeding the GRC risk-acceptance path. Encoded senior judgment into the tool so junior engineers started from correct prioritization, enabling a six-engineer team to execute 129,825 remediations and 55,532 governed risk acceptances.

**Zero Trust Framework Implementation** — Implemented Zero Trust across key operational areas for enterprise clients — establishing the asset, data-flow, and vulnerability baseline first, because a Zero Trust program built on incomplete asset knowledge produces expensive partial coverage. Delivered a 40% reduction in unauthorized access attempts, a reduced attack surface, and a scalable governance model that outlasted the implementation.

**ISO 27001 GRC Build** — Advised a financial services institution operating with no formal GRC framework. Led gap analysis against ISO 27001/27002 and built the framework ground-up — 40% reduction in audit findings and 100% ISO 27001 alignment.

**API-Powered Threat Detection** — Architected API-driven security integrations across multi-cloud (AWS and Azure) and GRC platforms, using RESTful APIs for real-time data exchange, automated risk scoring, and continuous compliance monitoring — cutting latency and unifying posture management across previously disconnected systems.

**Third-Party Risk Automation** — Architected an API-driven TPRM platform integrating vendor assessments, risk scoring algorithms, and compliance tracking workflows — 60% reduction in manual assessment time across 500+ financial services suppliers evaluated annually.

**Multi-Agent Security Systems** — Architected and built three multi-agent AI systems with defined authority boundaries and per-agent framework citations: 16-agent vulnerability management, 14-agent threat research anchored to MITRE ATT&CK/ATLAS and NIST SP 800-115, and 13-agent AI governance validated at 100% pass across a 41-test UAT. Also delivered CyberPulse, a CMMC Level 2 / NIST SP 800-171 compliance console taken through a 94-case UAT with zero open Critical/High defects at launch.

## EARLIER CAREER

---

**Santander Consumer USA • 2017** — Senior Information Security Consultant | IS Project Manager. Implemented a vendor risk governance framework on Shared Assessments, NIST 800-53, and GLBA; drove remediation cutting critical vulnerabilities 85%.

**Lockheed Martin • 2018** — Senior Information Security Consultant (contract). Developed Authorization & Accreditation artifacts; quantified cost and benefit of security functions to inform engineering trade-offs and risk treatment.

**Citi • 2014–2016** — Senior Cyber Security Engineer | Third Party Risk Manager. Built due diligence frameworks incorporating technical security review, SOC 2 Type II analysis, and penetration testing requirements for enterprise third-party integrations.

**AAFES • 2013–2014** — Senior Information Assurance Engineer | Accreditation Project Manager. Security control assessment of vendor solutions against DoD requirements; BC/DR architecture sustaining 99.9% availability for critical retail and financial systems.

**Department of Veterans Affairs • 2011–2013** — Senior Information Assurance Analyst | System Certification Project Manager. Architected and executed A&A certification packages for 150+ VA healthcare information systems under NIST RMF, achieving ATOs for applications managing veteran health records and benefits data.

## EDUCATION & CREDENTIALS

---

**Master of Information Technology, Project Management** — American InterContinental University

**Bachelor of Information Technology, Computer Forensics** — American InterContinental University

**Security leadership:** Certified Chief Information Security Officer (C|CISO) • Certified Information Security Manager (CISM, #2161093) • Certified Information Systems Auditor (CISA, #2117585) • Project Management Professional (PMP, #3397459)

**Assurance & privacy:** PCI-DSS Qualified Security Assessor (PCI-QSA) • ISO/IEC 27001:2022 Lead Implementer (BSI) • Certified Data Privacy Solutions Engineer (CDPSE, #2005804) • Certified CMMC Professional (CMMC-CCP) • CMMC-AB Registered Practitioner

**Technical:** AWS Certified Security – Specialty • Microsoft Azure AI Engineer (AI-102) • Splunk Core Certified User • CompTIA Security+ • Six Sigma

## TECHNICAL DEPTH

---

**Frameworks & regulation:** NIST CSF, RMF, AI RMF • NIST SP 800-53 / 800-171 • ISO/IEC 27001 & 42001 • HITRUST • HIPAA • PCI-DSS • SOX • CMMC • GLBA • EU AI Act

**Cloud & infrastructure:** Microsoft Azure • AWS • Google Cloud • Kubernetes / AKS • Docker • Terraform • multi-cloud architecture

**Security tooling:** Wiz • Nessus (Tenable) • Qualys • Microsoft Sentinel • Splunk • QRadar • SentinelOne • CrowdStrike • Tanium • CyberArk • Zscaler

**GRC platforms:** ServiceNow (GRC / VR / ITGC) • Archer • XACTA • AuditBoard

**Engineering & AI:** Python • PowerShell • SQL • REST API integration • multi-agent architecture • local LLM deployment • RAG • MITRE ATLAS • OWASP LLM Top 10