# JAMES SCOBEY

CISSP | MBA | M.Eng. Cybersecurity Policy & Compliance

james.scobey@s2i2.com | Crofton, Maryland | Active TS/SCI Clearance

## EXECUTIVE PROFILE

Senior cybersecurity executive with 25+ years building and leading enterprise security programs in highly regulated, mission-critical environments, including two federal financial regulators (SEC, PCAOB) and a global cybersecurity SaaS provider serving commercial and federal markets. Proven record establishing forward-looking cyber strategy, scaling high-performing security organizations, and translating cyber risk for boards, executive leadership, and external oversight bodies. Deep expertise in cloud-native security architecture, secure software development, security operations, and compliance across FedRAMP, FISMA, NIST 800-53, SOC 2, ISO 27001/27017/27018, IL-5, and CMMC.

## CORE COMPETENCIES

- Enterprise Security Strategy
- Regulatory & Audit Liaison
- Identity & Access Management
- Secure SDLC / DevSecOps
- Security Governance & Policy
- ISO 27001 / CMMC / IL-5
- Cloud Security (AWS, Azure)
- Cyber Risk & ERM Integration
- Security Operations & SOC
- Third-Party / Vendor Risk
- High-Availability Systems
- Budget & Vendor Management
- Board & Executive Reporting
- Zero Trust Architecture
- Incident Response & Forensics
- Data Protection & Encryption
- FedRAMP / FISMA / SOC 2
- Team Building & Mentorship

## PROFESSIONAL EXPERIENCE

**Chief Technology Officer & VP of Operations** Nov 2025 – Present

*S2i2, Inc. | Oakton, VA*

Drive enterprise technology, security, and operations strategy for an SBA 8(a) federal services firm holding TS facility clearance, CMMI ML3, ISO 9001/27001/20000, CMMC Level 2, and a GSA MAS contract; past performance across DISA/JSP, USACE, DLA, and PFPA.

- Established and operate a CUI enclave on AWS GovCloud (Amazon WorkSpaces, AWS Managed AD, Duo MFA, PreVeil, CrowdStrike Falcon) supporting DoD engagements under CMMC Level 2.
- Direct the enterprise security program covering governance, vulnerability management, endpoint protection, vendor risk, and incident response across federal and industry clients.
- Hold P&L accountability for the Operations division: budget forecasting, resource allocation, vendor and managed-services negotiations, and operational performance.
- Built and deployed an automated federal opportunity intelligence pipeline integrating multiple data APIs, reducing manual workload while improving competitive positioning.
- Maintain continuous authorization and compliance for systems under purview, ensuring adherence to federal and industry security standards.

**Chief Information Security Officer** Feb 2025 – Nov 2025

*Public Company Accounting Oversight Board (PCAOB) | Washington, DC*

Led the cybersecurity program for the Congressionally chartered nonprofit overseeing audits of US public companies, broker-dealers, and SEC-registered issuers. PCAOB Board members are appointed and overseen by the SEC.

- Established the enterprise cybersecurity program protecting non-public audit information, broker-dealer inspection findings, and investor protection data.
- Developed risk assessment frameworks and implemented control sets calibrated to the sensitivity of audit oversight data and regulatory expectations.
- Briefed the PCAOB Board and executive leadership on cybersecurity posture, emerging risk, and program maturity.

**Chief Information Security Officer** Oct 2024 – Feb 2025

*Keeper Security, Inc.*

Owned global cybersecurity strategy for a leading commercial and federal password management and privileged access SaaS provider serving millions of users and federal agencies.

- Maintained continuous compliance and authorization across SOC 2, ISO 27001/27017/27018, FedRAMP, StateRAMP, and DoD IL-5.
- Led security governance, secure SDLC integration with engineering, and product security authorization activities for new market entry.
- Built and mentored cross-functional security, compliance, SecOps, and DevSecOps teams; established executive-level security metrics and reporting.
- Managed relationships with external auditors, certification bodies, regulators, and federal customers.

**Chief Information Security Officer** Aug 2022 – Oct 2024

*United States Securities and Exchange Commission (SEC) | Washington, DC*

Led cybersecurity strategy and operations for the federal regulator of US securities markets, protecting market-critical infrastructure, non-public filing data, and PII for a 10,000+ user enterprise across headquarters, datacenters, and regional offices.

- Directed the Commission's comprehensive information security program in compliance with FISMA, NIST 800-53, and federal cybersecurity directives.
- Defined and executed the SEC's Zero Trust strategy aligned to OMB M-22-09 and CISA Zero Trust Maturity Model pillars.
- Led modernization of the Security Operations Center to address advanced persistent threats and nation-state actors, introducing new detection, automation, and response capabilities.
- Partnered with Enterprise Risk Management, Internal Audit, OIG, and GAO to identify, evaluate, and report organizational-level cyber risk within tolerance.
- Managed federal employees and contractors across cybersecurity engineering, operations, and policy/compliance functions; led talent strategy and team scaling.
- Served as primary security liaison to Commission leadership, Congressional staff, and oversight bodies on cyber posture and incidents.

**President & CEO** Feb 2022 – Aug 2022

*SigmaCyber LLC*

Cybersecurity consulting firm advising federal civilian and defense clients on cybersecurity engineering, incident response, security assessment and authorization, information assurance, and secure solution delivery.

**Chief Technology Officer** Sept 2021 – Feb 2022

*United States Securities and Exchange Commission (SEC) | Washington, DC*

- Set technical strategy and roadmap for the Commission's enterprise IT estate in partnership with the Chief Enterprise Architect.
- Drove adoption of modern security capabilities and emerging technologies, including hybrid multi-cloud and DevSecOps methodologies.
- Managed IT service delivery, vendor relationships, and shared services across the agency.

**Assistant Director, Cybersecurity Operations** Nov 2018 – Sept 2021

*United States Securities and Exchange Commission (SEC) | Washington, DC*

- Founded and led the SEC Cloud Center of Excellence; established cloud security strategy, reference architectures, and implementation standards for agency-wide cloud adoption.
- Ran cybersecurity operations for a 10,000+ endpoint enterprise; designed and deployed technical controls protecting sensitive market data and non-public filing information.
- Redesigned the SEC SOC to address nation-state and insider threats; implemented new detection capabilities and automated incident response workflows.

**Cyber Performance Systems Engineer** Oct 2017 – Nov 2018

*The MITRE Corporation*

- DevSecOps lead on the National Background Investigation System (NBIS) for DISA; designed and deployed a pre-deployment development test environment for code and component security validation of a national security system.

- Architected the cybersecurity lab integrating the MITRE ATT&CK framework for threat actor identification and containment planning; conducted cyber tabletop exercises.
- Designed a DevSecOps toolchain automating evaluation and deployment through CI/CD; secured DISA Risk Management Executive Approval to Operate.
- Recipient of the MITRE Director's Award and Officer's Award for distinguished service.

**Chief Information Security Officer** May 2016 – Oct 2017
*S2i2, Inc. | Pentagon Force Protection Agency*
Operations Manager and CISO for the Pentagon Force Protection Agency (PFPA), responsible for all IT service delivery supporting physical and cyber protection of the Pentagon.

- Led PFPA through the agency's first successful DISA Command Cyber Readiness Inspection (CCRI) through proactive cyber infrastructure improvements and a new vulnerability remediation process.
- Architected and deployed a highly available IaaS/PaaS hybrid cloud (VMware ESXi 6.5 / Microsoft Azure) and migrated all systems; deployed ACAS, ePO, and STIG compliance via domain policy.
- Designed multi-site clustered failover for physical security applications using application and storage-based replication; deployed enterprise DR with VEEAM.
- Deployed Splunk for log management and event correlation; implemented real-time response process for findings.

**Founder & Chief Technology Officer** June 2006 – May 2016
*Federal Data Systems (FEDDATA)*

- Co-founded and led a federal systems integrator with TS facility clearance serving Defense and Intelligence community customers; built and operated the internal cybersecurity program protecting CUI based on adversary TTPs.
- Coordinated with the Pentagon Computer Incident Response Team (PENTCIRT) on detection and response across classified and unclassified systems; served on multiple formal IR teams for classified intrusions.
- Operations Manager for the Pentagon Computer Services Room and tenant application migration to the Pentagon Enterprise Datacenter; Lead Architect for the DoD Continuity of Operations Integrated Network (DCIN).
- Designed the integrated server, storage, and virtualization environment for 7,000 Mark Center tenants; raised agency cybersecurity posture from borderline compliance to over 95% through vulnerability remediation and automation (PowerShell, PowerCLI, Python).

**Earlier Career** 1997 – 2006
*Director and engineering roles in federal IT and enterprise infrastructure*

- Director of Technology Integration, USmax Corporation: built NOAA's first Security Operations Center and led the cyber detection and response team.
- Director of Federal Services, By-Light: primary solution and cybersecurity designer for USSOCOM SCAMPI WAN upgrades; led DISA Tier III support lab implementation.
- Senior Systems Architect, SMS Data Products Group: deployed the first enterprise firewall in the Pentagon; designed IP transport for the 30,000+ user Pentagon network. Earlier engineering roles at SANrise, Worldstor, Fleetmark, Xerox Connect, and Stream International.

## EDUCATION

**M.Eng., Cybersecurity Policy & Compliance** • *George Washington University* 2020
**Master of Business Administration** • *University of Maryland Global Campus* 2014
**B.S., Computer and Information Science** • *University of Maryland Global Campus* 2012

## CERTIFICATIONS & CLEARANCE

Certified Information Systems Security Professional (CISSP) #358739 • AWS Certified Solutions Architect – Associate • AWS Certified Cloud Practitioner • VMware VCP – Network Virtualization and Desktop Mobility • Active TS/SCI Security Clearance