Dr. Matthew Hicks
5571 Kendrick Lane
Burke, VA 22015
mhicks4@cox.net
703-475-5269
DM • MBA • MS • C|CISO • CISSP • CISM • CRISC • PMP/RMP
PCI, HIPAA, NIST, FISMA, COBIT, GDPR, COTR/COR

Dear AOM

I have a Doctoral Degree in Management (Data Analytics), Master of Business Administration degree, and Master of Science degree in which I studied management of government, nongovernmental, nonprofit, and healthcare organizations. Also, I currently hold the C|CISO (EC-Council), CISSP, CISM, CRISC, PMP, and RMP certifications. I also have in-depth experience in HIPAA, PCI, NIST, FISMA, FRA, COBIT, ITIL and GDPR standards. I am an advisor to the ISSA board of directors and security executives from several organizations across different industries. I am a member of the AAR RISC group discussing cybersecurity and compliance issues with class 1 and other railroads.

I am an accomplished, results-oriented professional with extensive experience in creating and managing corporate-wide cyber security, compliance and risk management programs as well as having implemented these initiatives across global organizations. My background includes a proven track record of consistently establishing cost-saving efforts and offers a firm grasp of all aspects of compliance management and protection, including physical security, audit and compliance, and operational risk management for large organizations. Adept at utilizing broad-based skills to enable smooth collaboration among diverse facets, I have created more operationally efficient, secure, and synergistic organizations.

I have an extensive background and expertise in Cyber Security and Risk Management for hospitals (HIPAA, PHI) and federal/state agencies such as NOAA, FDA, Department of Transportation, and Department of Health and Human Services and the State of Maryland. I have served as an instructor and advisor specializing in HIPAA, FISMA, and NIST compliance. I have also worked with Contractor Officers reviewing and writing federal contracts to ensure adequate coverage of security concepts in the proposal and statements of work.

Please accept this letter and enclosed resume as an introduction to my skills and background. For a more detailed presentation of my offerings, feel free to contact me at your earliest convenience to schedule a conference. Thank you in advance for your consideration, and I look forward to our conversation.

Sincerely,
Dr. Matthew Hicks

Executive Summary

Highly accomplished Technology and Security Officer with proven ability to lead successful corporate information security and technology operations and facilitate corporate growth through technology-business alignment. Special expertise in cyber security, solution development, organizational excellence, program management, and process improvement. Doctoral, MBA and multiple certifications, including CISSP, CRISC, CISM, PMP/RMP, and ISSA member. Adept at directing multi-national teams and administering multi-million dollar budgets. Extensive familiarity with education, software development, transportation, health-care, financial, and technology sectors. Excellent presentation, problem-solving, and technical skills.

I am enterprising and innovative information compliance, security and technology leader with a With the talent in maintaining relationships, clients, vendors, and external business partners, I have identified and capitalized on technology and compliance trends to ensure that the organization performs at the top-tier of its industry while complying with regulatory standards. I have a motivational management style with a proven history of building, guiding, and retaining high-performance teams to develop and implement strategies for accelerated growth while ensuring security. I have also striven to optimize operations, reduce costs, and improve service quality while strengthening the bottom-line. Thus, I am a results-oriented technology industry leader and engineering principal, who has pioneered and managed complex compliance solutions involving cloud applications in the transportation, healthcare, and financial industries.

- Cyber-Law
- IT Governance
- IT Risk
- Cloud Security
- IT security
- Security Architecture Management
- Project/Program Management
- Threat & Incident Management
- Disaster Recovery / Business Continuity
- Strategic Planning
- IT Security Software Development
- Process Optimization
- Regulatory Compliance
- Technical Writing
- Cost/Budget Control
- Identity & Access Control
- Change Control Management
- Forensics
- E-Discovery

Technology and Security Leadership

Director, Information Technology and Security
Associate Professor
George Mason University - Fairfax, VA. 2019-present

Direct all facets of Information Technology and Security for the College of Health and Human Services (CHHS) at GMU. Collaborate with colleagues at GMU with research projects focused on healthcare initiatives. Peer review journal articles submitted for publication by GMU colleagues. Support of GMU curriculum to ensure program and student success

Senior Principal
National Railroad Passenger Corporation (Amtrak) – Washington, DC 2015–2019

Directed all facets of information security operations for Amtrak. The company's progressive workforce model is comprised of employees operating from several locations across the country. Responsibilities include cloud security, data security, security architecture, threat & incident management, compliance, risk management, compliance activities, identity & access control, change management, business continuity, disaster recovery, forensics, and legal discovery.

- Oversight and executive management of Amtrak's nationwide and enterprise Security Operation Center.
- Oversight of the Cyber Security Program including Governance, Risk, Compliance, Policy and Operations.
- Cyber Security Governance of Cloud services (AWS), IBM, AT&T, MuleSoft, and SCADA/ICS.
- Coordinated the implementation and management of SOC tools.
- Ensure compliance with Amtrak, federal, state, PCI, and NIST security standards and policies.
- Conduct compliance audits.
- Reduce Amtrak risk and exposure to malicious and hacking activity.
- Assist with managing IT Security budget and procurement of technology and training of staff.
- Successfully manage projects for Amtrak (valued 800K–1M).
- Advise the CISO on technical topics and Amtrak compliance to standards.
- Serve as a liaison with the AAR RISC, ISSA CISO, and external and internal teams to support troubleshooting, projects, and advanced cybersecurity opportunities.
- Manage vendor and contractor relations.
- Serve as point of contact with internal Amtrak teams and external agencies
- Work with Amtrak departments, groups, and projects to ensure compliance with Amtrak security policies.
- Interfaced with external and internal auditors.
- Conduct mainframe compliance audits for arrow and financial systems.

Council Member, Railroad Information Security Council (RISC)
American Association of Railroads (AAR) – Washington, DC

- Advise member organizations on CISO, cybersecurity, and information security risk and compliance.
- Reduce corporate risk and exposure to malicious and hacking activity.

Board Member
ISSA – CISO Advisory Council – Washington, DC

- Advise the ISSA Governing Board of Directors.
- Advise corporate security leaders, CISOs, VPs, and executives.
- Plan and coordinate cybersecurity conferences.
- Work with cybersecurity vendors.
- Reduce corporate risk and exposure to malicious and hacking activity.

NOAA Information Security Project Manager
MAXIMUS, NSOF – Suitland, Maryland 2015

Oversaw information security operations for NOAA. Managed NIST compliance. Planned and led complete engagements and supervised project teams.

- Ensure compliance with NIST and FISMA
- Conduct NESSUS scans of NOAA systems.
- Conduct risk and vulnerability analysis and assessment.
- Advise NOAA leadership on security issues.
- Manage all aspects of security for ESPC, GOES, POES, JASON2.
- Lead efforts to remediate POA&M ensuring the security of NOAA missions and systems.
- Manage security and system engineers.
- Work directly with NESDIS staff and contractors, including ISSO, management, and SES.

Information Security Director
Xerox State and Local Services – Elkridge, Maryland 2013–2015

Managed Cyber Security for the State of Maryland Children Services and Health Exchange agencies. Managed contractors and project teams.

- As the import-export and compliance officer ensuring ISO, NIST, PII and HIPAA standards.
- Designed, implemented, and managed data centers in Dallas, Indianapolis, and Baltimore.
- Operated the State of Maryland Department of Human Resources and the Health Benefit Exchange systems, providing security and privacy, while facilitating client transformation into the enterprise-class organization for maximum performance.
- Leveraged enterprise-wide information to re-engineer IT infrastructure, security, and team strategy into efficient alignment with core business priorities.
- Managed, a six-person security team, supporting two Maryland agencies to assimilate

innovative solutions rapidly and to maintain privacy and security.

- Managed contractors across multiple geographical locations.
- Directed and administered multimillion-dollar contracts, providing information technology and security services.
- Developed and executed plans for the State of Maryland to migrate 40 applications between data centers, including hosting on new server platforms.
- Introduced efficiently and integrated modern technologies to ensure the privacy and security of data.
- Managed third-party audits and assessments.
- Managed internal audits.
- Evaluate risks and acted expeditiously to make decisions and recommendations, while considering the technology environment, and the varying needs and viewpoints of a user community.
- Ensured mainframe systems audits and compliance.

Program Manager
Dakota Consulting, Silver Spring, Maryland

Contractor working with multiple consulting clients. Managed contractors and project teams.
2013–2013

- Worked with stakeholders to ensure compliance with NIST and FISMA.
- Spearheaded a focus on implementation and comprehension of relevant technology, while supporting tools for diverse applications and network vendors.
- Supervised six project managers in support of USDA technology and security projects.
- Developed solution roadmaps for diverse environments and architectures, improving client productivity and systems.
- Consulted with stakeholders on security, strategy, and infrastructure practices for USDA.
- Improved customer service benchmarks, collaborating with product management.

Program/Project Manager
DMI Consulting, Bethesda, Maryland 2012–2013

Contractor working with multiple consulting clients. Managed contractors and project teams.

- As a program manager, designed, implemented, and managed security solutions for DMI clients.
- Managed several projects for DOT, NIH, and FTC, ensuring on time and budget performance.
- Managed security programs for NIH grants management and payment systems.
- Spearheaded the development and implementation of compliance solutions for client systems.
- Developed and managed security certification processes.
- Improved the certification process, ensuring compliance with HIPAA, IRS, CMS, and NIST standards.

Associate
Booz Allen Hamilton, Mclean, VA 2010–2012

Contractor working with multiple consulting clients. Managed contractors and project teams.

- Designed, implemented, and managed a data center for the National Cancer Institute and the National Children's Study.
- Pioneered engineering solutions, and integrated IT, featuring the best-of-breed security technology for enterprise- level clients.
- Maintained subject matter expertise with two teams for system engineering overlay and expansive products.
- Provided technical and security support to NIH agencies.
- Increased the productivity of the development and deployment of client applications.
- Developed IT security and initiatives aligned with NIH vision, goals, and objectives.
- Established controls and reporting devices to monitor IT and security performance
- Assisted clients with compliance projects.

Director of Compliance and Security/CISO
Children's National Medical Center, Washington, DC 2001–2010

Directed corporate security operations for a National known hospital. Administered $5M+ budget. Oversaw information security, risk management, change management, compliance, threat/incident management, data security, business continuity, disaster recovery, forensics, and legal discovery.

- Import-export and compliance officer ensuring PII and HIPAA privacy standards.
- Designed, implemented, and managed three data centers.
- Transferred applications and systems from older to newer and larger data centers.
- Developed a backup data center.
- Created and directed the hospital information security program.
- Built and maintained the security architecture for all technology platforms.
- Maintained information security processes and security control standards to develop applications and deploy the technology.
- Evaluated a new security technology and conducted vulnerability assessments of hospital systems.
- Oversaw and managed 22 million dollars annual budget for information technology and the 100-technical staff.
- Established the hospital's Information Security Steering Committee and teamed with the internal audit department to define an IT security audit roadmap and strategy to address risks enterprise-wide.
- Gained a buy-in for the program across all levels, extracting the security organization from deep within the IT to direct awareness to executive levels.
- Security awareness training.
- Led and coordinated institutional responses to security incidents, providing timely reports during the event and intervention, and proposing solutions to prevent or mitigate future incidents.
- Provide leadership, guidance, and investigation regarding information security policy,

and security education and training.

Education

Doctor of Management, UMUC, Adelphi, MD – 2015
Dissertation Title: *Adoption of Knowledge Management Systems: The Impact of Organizational Cultural Factors*.

Master of Business Administration, UMUC, Adelphi, MD – 2011
Master of Science, Organizational Management, UMUC, Adelphi, MD –2010
Bachelor of Science, Public Administration (major), Information Systems (minor), George Mason University, Fairfax, VA –2003
Certificate, Organizational and Contract Management, Villanova, – 2010
Certificate, Six Sigma, Villanova – 2012

Certifications

C|CISO – Certified Chief Information Security Officer – EC-Council
CISSP (Certified Information Systems Security Professional) – ISC2
CISM (Certified Information Security Manager) – ISACA
CRISC (Certified in Risk and Information Systems Controls) – ISACA
PMP (Project Management Professional) – Project Management Institute
RMP (Risk Management Professional) – Project Management Institute
COTR (Contract Officer Technical Representative)

Additional Information

- Firewalls: CISCO ASA, Palo Alto, Check Point
- IDS/IPS: Palo Alto, Tipping Points, Snort
- SIEM: LogRhythm, QRADAR, Arcsight
- CrowdStrike
- Application testing
- Nessus
- IT audit and compliance management
- CMMI, ITIL, ISO 20000, SOX, PCI DSS, HIPAA, NIST, IRS, CMS, SSAE16, FedRamp, GDPR
- Security tools, processes, and policies
- Security incident response programs
- IT governance and best practices
- Global Project Lifecycle Management
- Information privacy and online safety
- Vendor and client management
- Mainframe systems, TPF, RACF
- Attachmate

Professional Organizations

- Project Management Institute (PMI)
- Information Systems Security Association (ISSA)®
  - CISO Executive Forum
  - CISO Advisory Council
- Information Systems Audit and Control Association (ISACA)
- The Academy of Management (AOM)
- Homeland Security Information Security Network (HSIN)
- American Association of Rail Roads (AAR) – Railroad Information Security Council (RISC)
- International Association of Privacy Professionals (IAPP)