## Contact

407-575-5781 (Mobile)
elvis.moreland@protonmail.com

www.linkedin.com/in/emoreland (LinkedIn)


## Top Skills

Creativity and Innovation

Problem Solving

Strategic Leadership

## Certifications

ISSEP - Information Systems Security Engineering Professional

CISSP - Certified Information Systems Security Professional

CGEIT - Certified in Governance of Enterprise Information Technology

CompTIA Subject Matter Expert

Certified Information Security Manager (CISM)

## Honors-Awards

Computerworld Premier 100 Leader

DOD Cyber Security Information Analysis Center (CSIAC) Subject Matter Expert (SME)

Atos Global Distinguished Expert, Data Security and Privacy Risk Management

FutureCon Award in Excellence Cyber Security Leadership

## Publications

G.E.A.R. U.P. Your Cyber Risk Management Program for DFARS, NIST, & CMMC

# Elvis Moreland CISSP-ISSEP, CGEIT, CISM

Virtual Chief Security Officer (CISO) | Strategy, Leadership, Vision | I Help Companies Use Best-of-Breed & DOD Secrets to Save 50% with GLBA, DFARS, NIST, & CMMC

Dallas-Fort Worth Metroplex

## Summary


An award-winning data security and privacy risk management executive with expertise in developing security and privacy programs for both private and public organizations within major critical infrastructure sectors. A security career that began in 1999 as the first command information security officer. A curious leader with proven management and operational expertise to:
-implement leading governance frameworks and GRC controls
-develop cyber risk management policy, process, and standards
-design enterprise security programs and system security plans
-assess and identify both data and privacy risks
-determine enterprise risk management priorities
-coordinate corrective actions and plans
-manage continuous diagnostics; and
-administer vendor relations

A strategic change agent and innovative problem solver in fast-paced and fluid environments. A team builder that mentors and empowers staff through vision, training, guidance, and motivation.

Professional certifications plus in-depth expertise in the following data security and privacy risk management domains: Governance; Engineering, Assessment (Audit); Risk Management, Compliance, and Continuous Quality Assurance. Specialization in developing quality-based management systems using NIST, ISO, and CERT/CC standards resulting in efficient and cost-saving risk management programs, policy, process, and capabilities.

Specialties include COSO, ERM, CMMC, FISMA, RMF, CJIS, HIPAA, CMS, FFIEC, SOX, GLBA, PCI DSS, IRS 1075, Systems

Security Engineering (ISSE) Process, NIST 800-18, NIST 800-34, NIST 800-39, NIST 800-53, NIST 800-171, and ISO 27001:2013.

## Experience

### Blue Cyren

Chief Information Security Officer (vCISO)
August 2020 - Present (2 years 10 months)
Dallas, Texas, United States

A business leader with data security and privacy risk management expertise. A leader with vision and innovation that builds high-impact programs and teams to continuously improve overall plans, processes, and cost.

Delivers guidance to organizations within the financial services, insurance, managed services, energy, and public sectors regarding prioritization of investments and projects that mitigate security risks, strengthen defenses and reduce vulnerabilities. Lead and inspire teammates responsible for security management, technical architecture, and operations with accountability for an effective and scalable cybersecurity control environment. Ensures continued compliance with statutory mandates and communicates major risks to executive management. Serves as an expert in security program best practices. Demonstrating advanced understanding of business processes, risk management, IT controls, and related standards. Deployed new and maintained current security program tools. Responsible for the creation and roll-out of security awareness and training company-wide. Collaborates cross-functionally, including with engineering, legal, and services teams, to build and strengthen security and privacy. Builds global awareness by training executives how to spot trouble and by using common sense metrics to track security and privacy risks.

### US Navy & Reserves

23 years 1 month

Fully Qualified Certification Agent / Auditor (INFOSEC)
October 2003 - December 2022 (19 years 3 months)

As a Fully Qualified Certification Agent (Auditor), I audited and validated programs and systems to ensure that: (i) risk-related considerations for programs and systems, to include authorization decisions, were viewed from an enterprise perspective with regard to overall strategic goals and objectives of the organization in carrying out its core missions and business functions;

and (ii) ensured programs and system-related security risk decisions are consistent across the enterprise, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success. I also coordinated and collaborated with senior executives to:
-Provide a comprehensive and holistic approach for managing risk—that provides a deeper understanding of the integrated operations
-Develop risk management programs with a strategic view of data security-related risks
-Facilitate the sharing of risk information among authorizing officials and other senior leaders
-Provide oversight for all risk management-related activities (e.g., security categorizations) to ensure consistent and effective risk management processes were implemented
-Ensure that authorization decisions considered all factors necessary for mission and business unit success
-Facilitate an open forum to consider all sources of risk (including aggregated risk) to operations and assets, individuals, other organizations, and the Nation
-Promote cooperation and collaboration among senior leaders and authorizing officials to include generate proper authorization actions requiring shared responsibility
-Ensure that the shared responsibility for organizational mission and business functions using external providers of information and services received visibility or elevated issues to the appropriate decision-making authorities; and
-Identify the organizational risk posture based on aggregated risk from the operation and use of the data and systems

### Information Security Officer / Information Security Manager
December 1999 - September 2003 (3 years 10 months)

-Reported to senior leadership at command and higher levels
-Managed organizational resources (time, money, personnel, etc.) to support security goals and policies
-Created and executed strategies to improve the reliability and security of IT projects
-Defined, implemented, and maintained corporate security policies and procedures
-Spearheaded vulnerability audits, forensic investigations, and mitigation procedures
-Responded immediately to security-related incidents and provided a thorough post-event analysis

-Managed a diverse team of security administrators, analysts and IT professionals
-Advised leadership on the organization's cybersecurity status
-Developed and deployed organization-wide training in security awareness, protocols and procedures
-Assessed, tested and selected new IT and security products

### Bank of America
#### Business Information Security Officer (BISO)
July 2019 - August 2020 (1 year 2 months)
Dallas/Fort Worth Area

Advised senior leaders and colleagues as a subject matter expert (SME) in federal statutory and regulatory compliance by utilizing codified protocols and standards such as NIST, FedRAMP, Financial Services Sector Coordination Council's (FSSCC) Cybersecurity Profile, Cybersecurity Maturity Model Certification - CMMC (built on NIST and ISO), and the OCC/FRB/FDIC mandated FFIEC Cybersecurity Assessment Toolkit (CAT). Worked cross-functionally with third-parties to develop, enhance, and execute data security, privacy, and risk management program requirements in information security policy, processes, procedures, and controls. Facilitated internal and external meetings to drive adoption of the firm's third-party risk program across service provider's enterprise standards and system-level capabilities.

As a proven professional in a cyber risk executive role adept at oversight and execution of critical assessments and reviews of third-party service providers by validating they:
-Developed and matured their Cyber Risk Management standards in policy, process, and controls that ensure the risk profiles are up-to-date with vendor contracts, risk assessments, and all pertinent vendor oversight details. This included collaborating with other stakeholders like vendor managers and procurement to ensure service providers are aware and compliant with the third-party risk program
-Implemented and integrated adoption of a risk framework based on NIST RMF, SSE, and CSF standards, including the implementation of policies, processes, and procedures for the third-party risk oversight program
-Educated and communicated best practices and standards for comprehensive policy, process, and procedures while reporting non-adherence during assessments in support of continuous monitoring
-Demonstrated in-depth expertise in enterprise and system-level Third-Party Cyber Risk Management standards

-Utilized management experience in designing, deploying, and delivering program oversight

### University of Central Florida - Office of Research & Commercialization

Program Manager, Data Security and Privacy Compliance (GRC)
October 2017 - July 2019 (1 year 10 months)
Orlando, Florida

Reported to the VP of Research as a research line of business Information security officer in the NIST Cyber Risk Executive role in order to provide a comprehensive, line of business approach to cyber risk management. Served as the common cyber risk management resource for senior leaders/ executives, research line of business managers, chief information officers, chief information security officers, system owners, common control providers, enterprise architects, security architects, systems security engineers, security managers/officers, and any other stakeholders having a vested interest in the line of business success. Coordinated with senior executives to:
-establish a clear line of business “cyber” risk management roles and responsibilities
-develop and implement a line of business cyber risk management strategy that guided business risk decisions (including how cyber risk is framed, assessed, managed, and monitored over time)
-established line of business forums to consider all sources of cyber risk (including aggregated risk)
-determined line of business cyber risk levels based on the aggregated risk from the operation of line of business systems and their respective environments of operation
-provided oversight for cyber risk management activities carried out to ensure consistent and effective risk-based decisions
-expanded stakeholder understanding of cyber risk with regard to the strategic and integrated operations
-established effective vehicles and served as a focal point for communicating and sharing cyber risk related information among key stakeholders internally and externally
-promoted collaboration among authorizing officials to include security risk authorization actions requiring shared responsibility
-ensured that security risk authorization decisions considered all factors necessary for success
-ensured accountability for supporting business functions received the needed visibility and were elevated to appropriate authorities

## Atos

### Sr. Director (Distinguished Expert), Data Security and Privacy Risk Management

May 2015 - July 2017 (2 years 3 months)

Dallas, TX

Recognized as a Global Distinguished Expert in Data Security & Privacy Risk Management while the Head of Consulting for North America. Built and directed a team of 18 security directors, consultants, and engineers. Provided security and risk management thought leadership to North American Operations while managing multiple initiatives and business process engineering. Collaborated with all levels of management and partners to assess client Information Security Risk Management (ISRM) and align program goals with appropriate regulatory mandates at the highest standards such as NIST RMF and the Cyber Security Framework. Managed efforts to mitigate Information Security Risk by planning, engineering, designing, assessing, deploying, evaluating, monitoring and/or administering policies, processes and standards. Provided Information Security Risk insight and guidance to senior management on risk and compliance issues and serves as a trusted advisor to executives, managers and the enterprise. Worked under minimal supervision on complex client requirements and developed appropriate solutions and problem resolutions.

## TISTA Science and Technology Corporation

### Chief Information Security Officer (CISO)

June 2013 - May 2015 (2 years)

Orlando, Florida Area

A Cybersecurity thought leader. Leading the Cybersecurity practice in standards for Governance, Engineering, Risk, and Operations by assisting with end to end assessment, design reviews, and management. A demonstrated leadership specific to business and security issues as well as the ability to manage and develop staff. I also:

-Maintained a working knowledge of advanced cyber threat actor tactics, techniques, and countermeasures

-Conducted risk assessments, audits and vulnerability tests with industry tools and techniques

-Documented and presented findings to executive and non-executive stakeholders

-Managed, mentored, and trained information security managers, engineers, and analysts

-Educated business leadership and regarding data security, privacy, and governance models
-Developed corrective action plans for implementing enterprise security plans
-Developed and deployed enterprise and system level security policies
-Partner with engineers and system owners to plan and implement secure road-maps
-Skilled and comfortable with change to actively drive innovation
-Leveraged expertise to resolve problems during system design, development, and testing processes
-Applied knowledge of national and international standards to produce new initiatives and solutions

### U.S. Department of Commerce

**Lead Information Systems Security Engineer, IT Management Specialist (INFOSEC)**

July 2012 - June 2013 (1 year)

Washington D.C. Metro Area

Team lead for Enterprise Information Security Engineering and Privacy Subject Matter Expert (SME). The Security Engineering Lead and Liaison for the Enterprise Change Management Program, Enterprise Change Advisory Board, Enterprise Engineering Review Board, Enterprise Private Cloud and Infrastructure as a Service (IaaS), Enterprise Development Environment, Enterprise High Performance Computing (HPC), Research Data Center thin client architecture, Enterprise Project Life Cycle (SDLC), SAS Center of Excellence, and Enterprise Risk Management Program.

Responsible for conducting information system security engineering activities. Information system security engineering is a process that captures and refines information security requirements and ensures that the requirements are effectively integrated into information technology component products and information systems through purposeful concept of operations (CONOPS), acquisition, security architecting, design, development, and configuration. Information system security engineers are an integral part of the acquisition and development team (e.g., integrated project team) designing and developing organizational information systems or upgrading legacy systems. Information system security engineers employ standards and best practices when implementing security controls within an information system including software engineering methodologies, system/security engineering methodologies, secure design, secure architecture, and secure coding techniques. System security engineers coordinate their security-related

activities with information security architects, senior information security officers (CSO/CISO), information system owners, common control providers, and information system security officers.

### United States Marine Corps

Lead Information Systems Security Engineer for Northrop Grumman / TASC, Inc.

August 2009 - January 2012 (2 years 6 months)

Orlando, Florida Area

The Lead Information Systems Security Engineer providing Information Assurance Analysis for multi-million dollar programs utilizing the Information Systems Security Engineering process, IEEE 1220 standards, the NIST Risk Management Framework and Life Cycle. Utilizing over 20 years of DOD experience in Operations Management, Network Operations, Information Security and Information Assurance to assist DOD commands plus their component structure to save millions of dollars by improving key business process efficiencies while delivering federal statutory and regulatory compliance.

### PremiereTec Companies

Interim Chief Information Security Officer (CISO)

November 2007 - July 2009 (1 year 9 months)

Responsible for the planning and development of an enterprise information security strategy and best practices in support of the enterprise*s information security architecture. Engineered compliance with PCI, FISMA and Florida IT security requirements. Collaborated with key business and IT leaders (CIO, Director Operations, etc.) to develop security and business continuance plans and standards. Directed all information security audits and tasks related to the integrity, confidentiality and to ensure availability of information to end users. Ensured that IT operations complied with existing state & federal laws and regulations. Responsible for ensuring that tools or technologies were implemented to reduce the risk of *denial of service* attacks or extrusions against systems. Acted as a corporate advocate for information security and business continuance best practices. Consulted with senior IT and business leaders regarding their information security risks and responsibility in minimizing those risks. Constantly keeping up-to-date, with information from state and federal government and across the relevant industries regarding the identification of new requirements, threats and vulnerabilities to information security.

### Supreme Court of the U.S.

Information Security Advisor

May 2007 - October 2007 (6 months)

Washington D.C. Metro Area

Utilized federally codified standards in planning, designing, developing, and deploying the court's first ever Cyber Security Incident Response Capability (CSIRC) and the CSIRC program concept of operations (CONOPS), policies, process, and procedures.

### FAA Telecommunications Infrastructure (FTI)

Deputy Chief Security Officer (CSO), Director of Security Operations for Harris Corp

October 2005 - May 2007 (1 year 8 months)

Designed, developed, and managed the 24/7 Security Operations Center (SOC) for the FAA Telecommunications Infrastructure (FTI) Program protecting the National Air Space services. Managed 26 Security Engineers and Analysts on multiple rotating schedules. Managed budget and network security operations for a wide area network with over 20,000 network devices and at over 6,000 sites across the country and internationally. Developed and managed the IT Security program and practices based on ITIL, IEEE 1220, IATF v3.1, NIST Special Publications, FIPS, OMB and DOD / NSA standards.

### JPMorgan Chase

Technical Manager

April 2003 - October 2005 (2 years 7 months)

Greater Chicago Area

Managed IT design, deployment and operations for government lockbox IT operations. Supervised and overseen projects and tasks for a specialized lockbox IT department. Assisted executives to define and implement life cycle processes to manage the IT-related line of business goals and requirements of the line of business. Created IT policies, process and procedures based ITIL and NIST standards.

---

## Education

### Regent University

Master's degree, Business Administration / Cyber Security Management · (December 2024)

### Oakland City University

Bachelor of Science (B.S.), Management

### Community College of the Air Force

Associate of Science (A.S.), Health Information Management

### SANS Technology Institute

Certificate, Information Security Management System ISO/IEC 27001/27002 Lead Auditor

### SANS Technology Institute

Certificate, Implementing and Auditing the Top Critical Security Controls In-Depth (GCCC)