Deputy Chief Information Security Officer Deputy Chief Information Security Officer Deputy Chief Information Security Officer - STATE OF TEXAS DEPARTMENT OF PUBLIC SAFETY Austin, TX CISSP, CISM, CRISC, and Security+ Certified Information Technology Leader skilled in securing information systems to achieve information confidentiality, integrity and availability. Adept at Governance, Risk Management, and Compliance (GRC). Experienced in Information Security frameworks including NIST COBIT, ISO 27001, and TAC 202 etc. Promotes IT as a key enabler for organizational and enterprise success, aligning effort levels with outcomes. Department of Defense Top Secret Security Clearance and currently holds the rank of Major in the US Army Reserves and is assigned as a Cyber Fusion Watch Officer to the Cyber Security Operations Center at United States Pacific Command Headquarters at Camp H.M. Smith in Hawaii. Work Experience Deputy Chief Information Security Officer STATE OF TEXAS DEPARTMENT OF PUBLIC SAFETY February 2019 to Present Performs highly advanced (senior-level) managerial work overseeing the daily security operations and activities of DPS's networks and programs. Work involves establishing goals and objectives; developing guidelines, procedures, policies, rules, and regulations; developing schedules, priorities, and standards for achieving established goals. Coordinating and evaluating program activities to include a Security Operations Center (SOC); and developing and evaluating budget requests. Provides leadership, management and supervision for activities related to DPS security initiatives. Assists in establishing direction for the statewide security function in state government. Assists in the development of statewide plans, standards and guidelines to address new security technology issues and trends with a concentration in Internet and E-Business applications. Plans, assigns, and supervises the work of others to include 28 FTEs. Works under minimal supervision with extensive latitude for the use of initiative and independent judgment. Network Security Operations Center Security Manager STATE OF TEXAS DEPARTMENT OF INFORMATION RESOURCES March 2014 to January 2019 Provides leadership and strategic direction for the function, ranging from planning and budgeting to motivational and promotional activities expounding the value on information security. Responsible for a "center of excellence" for information security management, for example offering internal management consultancy advice

and practical assistance on information security risks and controls. Leads the design and operation of related compliance monitoring and improvement activities to ensure compliance both with internal security policies etc. and applicable laws and regulations. Leads or commissions the preparation and authorizes the implementation of necessary information security policies, standards, procedures and guidelines, in conjunction with the Security Committee. Leads or commissions activities relating to contingency planning, business continuity management and IT disaster recovery in conjunction with relevant functions and third parties. Applies a comprehensive knowledge of information technology security principles, practices and procedures to develop, implement, and manage the overall information system security program. Ensures assigned information systems are properly managed, according to the JSIG, ICS 503, and other security directives as required. Liaisons with and offers strategic direction to related governance functions (i.e. Physical Security/Facilities, Risk Management, IT, HR, Legal and Compliance). Recruitment, leadership and direction for a loose network of information security ambassadors distributed throughout the organization. Direct design, implementation, operation and maintenance of the Information Security Management System. Directs or commissions suitable information security awareness, training and educational activities; information security risk assessments and controls selection activities. Performs other duties as assigned Works under minimal supervision with extensive latitude for the use of initiative and independent judgment. Key Results: ? Improved statewide IPS program by adding in new threat intelligence feeds which resulted in an increase from 3 million to 30 billion blocks against State of Texas Networks monthly ? Successfully monitored and protected over 2.8 million public IPs from the States Network Security Operations Center ? Produced 4th NSOC Annual Threat Report that was distributed statewide ? Performed multiple proof of concepts for new security technologies that related in successful procurement and deployment of new security devices ? Led security operations for DIRs' Shared services programs which includes TX.Gov, Data Center Services and Managed Security Services ? Assumed command as lead incident manager and designed all incident response plans for all shared services customers which include over 150 State agencies and institution of Higher Education and multiple vendors and monitoring and response technologies

Senior Security Planning Analyst CAPGEMINI CONSULTING, STATE OF TEXAS DATA CENTER PROGRAM March 2013 to May 2014 The Security Planning Analyst is responsible for collecting IT security reports across multiple IT technologies and combining the information into comprehensive reports for delivery to the customer. The position will assist in audit and compliance reporting. The position will require coordinating security related reporting across multiple IT technologies, developing reports, and delivery of reports to multiple levels of customers according to defined timelines Key Results: ? Reporting and tracking of security incidents and remediation activities. ? Assist in development of security training and provide reporting on security training compliancy. ? Reporting and tracking of Security Incidents and remediation activities of Security Incidents. ? Communicate with client, corporate executive management, and subject matter experts across various Infrastructure and Application Management towers Created Systems Security Plans for multiple applications utilizing Federal and NIST guidelines ? Work closely with Compliancy and Audit organizations. Respond to Compliance and Audit requests and activities, coordinate responses with technical towers, and coordinate remediation activities. ? Managed State of Texas Master System Security Plan and all associated documents. Senior IT Security Analyst VETERANS AFFAIRS, AUSTIN INFORMATION TECHNOLOGY CENTER October 2012 to March 2013 IT Specialist performing a variety of duties to support a wide range of Internet, intranet, and extranet accessible systems. Ensures the confidentiality, integrity, and availability of systems, networks, and data through the planning, analysis, development, implementation, maintenance and enhancement of information systems security programs, policies, procedures, and tools. Maintains the stability and currency of security software artifacts as applications and software change during the normal course of business. Key Results: ? Became trained and certified in all VA internal applications and processes. ? Published key security artifacts for General Support System Level Local Area Network (LAN) ? Provided complex technical consulting and support services for defining, developing, and improving functional or business processes to meet user and organizational needs. ? Conducted process redesign and compiles documentation for VA applications ? Created Systems Security Plans for multiple applications utilizing Federal and NIST guidelines ? Published privacy impact

assessments for Federal applications ? Managed Disaster Recovery plans for sensitive applications Manufacturing Supervisor SAMSUNG AUSTIN SEMICONDUCTOR September 2011 to October 2012 Responsible for supervising and coordinating the activities of manufacturing specialists who are involved in the wafer fabrication process. Schedules resources, develops staff, tracks metrics, and prepares reports and presentations regarding progress towards production goals. Ensures safety, quality, and productivity of staff. Key Results: ? Provided direction and training to employees regarding policies and management guidance. Recommended several beneficial changes to new management processes. ? Identified complex problems and reviewed related information and evaluated and implemented successful options and solutions for the manufacturing team. ? Works closely with departmental management and staff to define problems and management requirements Information Assurance Manager/Company Commander TEXAS ARMY NATIONAL GUARD October 1997 to September 2011 Responsible for Information Assurance Vulnerability Assessment strategies and procedures for all Texas Military Forces systems and reporting results to the National Guard Bureau in Virginia. Responsible for training, soldier readiness, logistics, personnel administration, equipment maintenance, strength management and the professional development of 300 Soldiers. Key Results: ? Developed all C&A Artifacts for state level enterprise secure network ? Managed TXARNG State level Security Operations Center (SOC) ? Created multiple security plans utilizing Federal guidelines including, Wireless Security Plan, Incident Handling Plan, Intrusion Prevention Plan ? Led efforts to manage all staff processes to ensure that processes meet changing departmental and organizational conditions ? Identified security issues and risks, and designed and deployed mitigation plans. ? Tested and implemented enterprise IT security solutions and monitored IPS/IDS, Wed Filter, and related commercial network security solutions. ? Ensured the process and procedures followed by State level Network Operations Center are compliant with industry and government legislation ? Responsible for analysis of network and system security events and briefed Senior IT and Leadership staff to accurately respond to information security incidents. ? Assisted with application testing and monitoring. ? Developed all network security plans and incident response procedures for a State

level military network ? Responsible for creating and submitting all Plan of Action and Milestones (POA&M's) to the National Guard Bureau on behalf of the State level DAA ? Managed all DIACAP procedures and personnel for the Texas Army National Guard ? Developed a State level Defense in Depth security plan which encompassed all layers of the Texas Army National Guard network including securing user accounts, hardware and numerous applications. ? Managed the training, duties and reporting responsibilities for over 300 Information Assurance Security Officers. ? Resolved day-to-day technology needs of the Texas Army National Guard with a focus on the analysis of processes, dissecting problems and suggesting solutions and developing plans. ? Ensured the patching of enterprise systems with current security updates, maintained an enterprise standard anti-virus program requirement, and planned and implemented enterprise Web Filters, Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS). ? Successfully managed the budget and personnel decisions for an enterprise that supported 23,000 users; over 6,000 computers and more than 300 servers. ? Responsible for analysis of network and system threats and works with IT and business staff to enable appropriate vulnerability remediation. ? Serves as a liaison between department users and the Information Technology organization in order to provide technical solutions to meet user needs Education US ARMY SIGNAL SCHOOL - Fort Gordon, GA 2009 NATIONAL GUARD PROFESSIONAL EDUCATION CENTER - Little Rock, AR 2008 TEXAS STATE UNIVERSITY - San Marcos, TX 2007

Name: Jaime Stevens

Email: bryantvirginia@example.net

Phone: (939)652-7849x89105