Senior Information Security Officer within the Wholesale Business Security Office Senior Information Security Officer within the Wholesale Business Security Office Senior Information Security Officer within the Wholesale Business Security Office - SunTrust Bank Atlanta, GA Work Experience Senior Information Security Officer within the Wholesale Business Security Office SunTrust Bank - Atlanta, GA May 2019 to Present Responsible for information security control enforcement, cyber security awareness, and enablement across all lines of business, enterprise functions, technology, and operations teams. The BISO team also leads and works with third-party cyber security on external engagements. The Business Information Security Office works closely with the line of business Chief Information Officers (CIOs)/Chief Technology Officers (CTOs). Support a group/team to develop a deep understanding of the business in order to have specialized information security risk-based discussions. Provide guidance on information security topics, policies and controls. Contribute to the ongoing information security initiatives and improvements development, implementation and maintenance of information security for the line of business (LOB) Possess strong / experienced application development and/or application security background; with solid knowledge of SDLC from design, testing, deployment to post production and the different risk elements associated with each step. Serves as an Information Security subject matter expert and participate in the development, implementation and maintenance of information security for the line of business (LOB). Provide guidance and advocacy regarding the prioritization of LOB investments that impact information security. Advises LOB management on risk issues related to information security and recommends actions in support of the bank's wider risk management and compliance programs. Monitor information security trends internal and external to the bank and keep LOB leadership informed about information security-related issues. Manages quality control and reporting and ensures compliance with policies and laws Risk Management and risk assessment analysis and documentation. Drives LOB risk deliverables. Collaborates with risk partners on info security critical priorities. Participate in senior LOB specific Risk Management & Business Continuity Routines Identify and measure global information security controls on most critical business processes or channels. Leadership/Strategy. Has a deep understanding of security

for computing platforms (PaaS, SaaS, etc.) Ability to build strong Partner relationships with peer technology groups and supported LOB. Supports the triage process with the client and helps them understand the BISO support structure. Drives required risk culture and partnership with peer technology teams and supported LOB Participates in key CIO operating routines to drive information security risk strategy. Information Security Officer for Consumer, Fraud Operations SunTrust Bank - Atlanta, GA August 2017 to April 2019 Ensuring that information security risks are being identified, documented appropriately, and to then work with the business to give direction with regard to appropriate mitigating controls and or remediation efforts. Work with the business and understand their business processes and advise them with regard to broad-based issues regarding information security and giving guidance and direction with regard to business need and information security risk. Work with both business and technical contacts to help ensure that applications and systems comply with SunTrust's information security program (or have a documented exception in place) in support of applicable laws, regulations/guidance, and industry standards. Effectively document and communicate assessment findings, and subsequently present them to peer and upper management. Completes business risk impact assessments, third party (vendor) contract reviews, and online fraud authentication risk (OFARA) reviews using RSA Archer GRC. Serves as lead liaison between all SunTrust segment functions, various lines of businesses and IT in the mitigation of cyber risks identified during audits and security risk assessments. Coach, train, and mentor junior Cyber security consultants and security assessment analysts totaling 20 or more teammates. Manages relationships within various business areas to ensure that Cyber security risks are identified and provides direction with regard to appropriate mitigating controls and/or remediation efforts. Build relationships with various business segments in order to provide guidance on business processes and issues regarding Cybersecurity. Collaborate with both business and technical contacts to ensure third party applications comply with applicable laws, regulations/guidance, and industry standards. Manages offshore engagements regarding IT Security controls. Serves as Business Risk Program Owner and provides maintenance of program documentation, procedures and processes to ensure compliance with changes in business or

regulatory drivers. Manages Third Party Risk Management (TPRM) assessments. Cyber Security Analyst Centers for Disease Control and Prevention October 2016 to July 2017 Strengthen the security posture within the agency, while being an integral part of a strong team. Evaluate and ensure quality assurance to CDC's management, technical, and operational controls for over 800 information systems CDC wide, and directly support 14 Information System Security Officers (ISSOs) and their Stewards with system packages and controls. Advise the Chief Information Security Officer CISO on all matters relating to security vulnerabilities and threats to CDC information systems. Analyze security reports (Appscan, Nessus) to identify vulnerabilities and create mitigation strategies. Create new documents to streamline and organize the functionality of daily routines among fellow teammates, including Standard Operating Procedures, a process change proposal form, a new BSI, a process change guide, quick reference guides for new processes, policy guidance, etc. Provide recommendations for mitigating system vulnerabilities through system security control remediation and redress; collaborate with ISSOs and security stewards. Work with C/I/O staff and ISSO's to assist in the documentation of technical controls and how they are applied to each system. Review the SA&A packages for compliance with Federal standards, i.e. National Institutes of Standard and Technology (NIST), Federal Information Processing Standard (FIPS), Office of Management and Budget (OMB), The Federal Information Security Management Act (FISMA) etc. ? Review network diagrams to ensure they accurately depict the topology, components and connection to the CDC network. ? Analyze Risk Assessment Reports to determine the impact of any vulnerabilities reported and create a Plan of Action and Milestone (POA&M) to mitigate any accepted weaknesses. ? Utilize knowledge of FISMA and NIST to provide guidance on specific technical and security requirements for new proposed security policies, methods, and standards. (NIST 800-53, 800-39, etc.) ? Innovate and develop new best practices for procedures, security policies, database usage standards and management, and services to the client. Maintain up to date knowledge of security and privacy mandates from NIST, OMB, DHS, and FISMA. Helped draft the 2017 CSP foreword Technical writing - Serve as tech writer and worked with Team lead and SMEs to create new user forms for CDC C/I/O staff, ISSOs

and Security Stewards ? Change Management Request form ? POA&M Reschedule and Closure Request forms ? Policy Exception form ? ACCS Inheritance forms, EMSSP Inheritance forms, Decision Papers, SBC Recommendation form, etc. CDC Federal Work Study Student, Security Assistant National Center - Atlanta, GA April 2015 to May 2016 30331 Completed Security Assessment and Authorization (SA&A) documentation to comply with National Institute of Standards and Technology Special Publication 800-37, 800-53, Federal Information Processing Standards (FIPS) 199-200 and FIPS 140-2 ? Ten Low EMSSP SA&A ? Eight Moderate EMSSP SA&A ? Four Low FULL SA&A ? Implemented updates from NIST 800-53 Rev 3 to Rev 4 security controls on 20 NCHHSTP Low, Full and Moderate systems. Completed 176 security controls on Low and Full systems and 313 security controls on Medium systems Completed twelve Annual Assessments ? Six Low Information Systems ? Four Moderate Information Systems ? Two Full contracted Information Systems Completed Business Contingency Plan (BCP) Assessments ? Ten Low Information Systems ? Five Moderate Information Systems ? Functional Exercise BCP Completed Recertification Assessments ? Five Low Information Systems ? Four Moderate Information Systems Member of NCHHSTP Computer System Incident Response Team (CSIRT) ? Completed 35 Incident Responses ? Completed 30 computer re-image requests ? Completed 10 International (Global) Incident Responses Completed 22 Commercial Off The Shelf (COTS) Level III requests to include creating forms, requesting digital signatures for supervisor, TSE, ISSO and sending completed forms to CDC OCISO Product Evaluation for review Completed 30 Change Requests and sent out forms to Change Owner, Security Steward, Business Steward and ISSO for digital signatures. Emailed completed documents to CDC OCISO Change Management Mailbox Completed eighteen IBM Watchfire AppScans Completed 5 Social Media and Third Party Web Sites to include writing approval justification, requesting digital signatures for supervisor and ISSO approval and sending the request to Program Official and ISSO Issued 42 Biometric Encrypted USB drives. Initialized USB drive, showed User how to access USB and use the Biometric scan and unique password. Sent Users NCHHSTP USB User guide Revised four Standard Operating Procedure (SOPs) for the NCHHSTP IT Security Team: ?

Commercial-Off-The-Shelf (COTS) LEVEL III SOP ? Security Content Automation Protocol (SCAP) Compliance Checker Version 1.0 SOP ? Security Assessment and Authorization (SA&A), Annual Assessment and Business Plan SOP Version 1.1 ? Security Incident Response SOP Version 1.0

Follow information security policies, methods, standards, Federal Information Security Management Act (FISMA/National Institutes of Standard and Technology (NIST) standards and practices to organizational information systems, IT reference materials and interpret regulations. Implement security controls, perform ongoing maintenance and prevent, detect, analyze and respond to security incidents. Conduct risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, rules, and protection needs. Communicate with Information Security Systems Officer (ISSO), CDC organizations and organizational staff. Communicates with senior executives through oral and written reports and presentations, as required. Works with business owners, IT managers, staff, and vendors in order to provide timely and efficient IT coordination of security services to meet agency needs. Work with the Enterprise Performance Life Cycle project manager to collaborate on the Information System Security tools required in the implementation cycle. Worked on a new NCHHSTP IT Security Website content as co-author Co-created the IT Security Team's Microsoft Access database Attend weekly ISSO/ IT Security Team meetings IT Internship Cypress Skilled Nursing June 2014 to January 2015 Performed hardware support for (PCs, laptops, kiosks, printers, cellphones) Set up printers, computers on the company network Software, Operating Systems (Windows), support and implementation of tailor made company software (mostly account setup/permissions) Server; helped set up and update Domain Name Systems, Internet Protocol (Administration/Group Policy) Complied with HIPPA standards of privacy, while dealing with individual personal data, addresses, SSN, medical records Updated new employee data, i.e. set up user names, passwords and access IDs to comply with the company's service sites Education Master of Science in Computer Science in Computer Science Kennesaw State University December 2020 Bachelor of Science in Mathematics in Mathematics Kennesaw State University Skills Security, Business continuity, Cisa, Cissp, Disaster recovery, Ffiec, Glba, Hipaa, Nist, Payment card industry, Pci, Bcp, Business continuity planning, Rsa, It

project management, Risk assessment, Remediation, Contracts, Bsa, Bank secrecy act

Name: Keith Shepard

Email: michaelstevens@example.org

Phone: 001-474-390-7559x8065