Senior Risk Management Specialist/ Security Control Assessor Senior Risk Management Specialist/Security Control Assessor Senior Risk Management Specialist/ Security Control Assessor - SCA Clarksburg, MD To obtain employment in Cyber Security related position where training and skills will be used Work Experience Senior Risk Management Specialist/ Security Control Assessor SCA - Washington, DC July 2018 to Present Worked as senior risk examiner/validator/ for information technology supporting United States Secret Service part of the Chief Information officer (CISO) Worked closely with system owners, CISO's, and compliance management to validate security controls and provided system risks matrix. Provided security control assessment for a number of DHS component systems. Served as subject matter expert and resource in IT examination to compliance requirement. Exercised FISMA six steps of risk management process to examine system risks and weaknesses and provided recommendation AO risk severity level of the organization Used XACTA for system authorization and continues monitoring purposes. Validated security controls and provided recommendations to mitigate/accept a risk to system owners and CISO. Provided training for system security officers on managing Plan of action and milestone Used security policies including DHS 4300A att. B, H, K, G, Q and NIST SP-800 53, NIST 800 SP-34, SP 800 SP- 171, FIPS 199, DHS performance plan, and DR. check to evaluate system security compliance with the DHS. Provided security control change updates and managed high value/Major/classified add unclassified system assess. Worked closely stakeholders of organization to evaluate system risk status and provided briefs to senior management and board of directors. Validated system security status and prepared Packages for Authorization to operate recommendations to the agency authorized official (AO) Prepared security policy and procedures to the organization including Contingency plan, Configuration Management and Risk Assessment process. Monitor all system status and address security weakness and provided remediation strategies Represented USSS compliance working group to enhance the agency security posture coordination with DHS security team Lead/Acted as POC for the agency for inventory systems and provided system change status to DHS. Information Security System Officer ISSO - Washington, DC November 2017 to July 2018 Managed systems for

certification and accreditation process- ATO by testing, examining, and reviewing security control of each system. ? Worked closely with system owners, CISO's, and compliance management to effective manage system risks and developed mitigation strategies. ? Managed systems to comply with FISMA, FIPS, DHS 4300A, NIST 800, and ISO security regulation and standards based on the system requirements. ? Developed ISSO Security training materials including developing incident response and compliance references. ? Experienced with XACTA-360, Continuum, security center-Nessus, and AppDetector, ? Experienced with FISMA scorecards matrix, PIA, POA&M, CP, CPT, SSP, CM & others ? Created contingency plan and test based of the confidentiality, integrity, and availability of the system CIA trend. ? Developed POA&M for all system weakness identified during current and past findings ? Successfully implemented six risk management frameworks as part of ATO process. ? Developed IT customized security policy in compliance with NIST 800 and DHS 4300A for FEMA project. ? Exclusively utilized system and web application vulnerability tools including tenable Nessus, AppDetrctor and other for scanning and auditing all system activities. ? Worked on incidents reporting and provided procedures for handling security issues. ? Worked on system security configuration and provided security troubleshooting in QA (Quality of Assurance) security practices. ? Developed IT customized security policy in compliance with NIST 800 and DHS 4300A for FEMA project. ? Used NIST SP 800-53v.4 Security control frame work for Auditing, program managing, incident handling, risk management, configuration management, and Security assessments. ? Provided/updated network design architecture for all of the systems I was supporting Cyber Security Consultant III/Information system security officer ISSO March 2016 to October 2017 Worked as subject matter expert in managing system authorization process ? Examined security risks of private independent service providers (SPs) including financial institutions. ? Provided cyber security recommendations based on standards, and regulations set by NIST and DISA standards to support new and existing projects ? Used DoD/NIST frameworks including SP 800-53 Access Control, Audit and Accountability, for developing risk security assessments. ? Provided oral briefings and/or presentations to board members, deputies, and upper management personals. ? Examined and implemented Windows, and Linux OS to design a

network architectures ? Provided subject matter expertise in applying and maintaining FISMA security requirements to ensure that the developed IT security system in compliance with FIPS 199 modification and application requirements in protecting cardholder data - integrity. ? Applied and developed contingency plan based on NIST (RMF) Risk Management Framework in a complete work environment. ? Conducted security risks and compliance assessments by linking legal & regulatory status of Unisys client's environment. ? Analyzed evaluated and recommend technical security solutions ISO 27002 standers ? Enhanced & developed security configuration standards based on system requirement needs. ? Worked on auditing systems including audit logs using windows & Linux OS ? Developed IT customized security policy on customer's system environment. ? Implemented STEALTH Core network security solution integrating data centers from being visible to invisible network attacks. ? Installed and maintained Aunigma security system solution to Staples project -US and Canada locations by developing PCI- compliance risk recovering strategies. ? Conducted network and application-layer for testing vulnerability assessments. ? Worked on incidents response and provided procedures for handling security issues ? Used Red hat Enterprise Linux and Windows OS for testing security of third party organization business environment (using White and gray). ? Supported NYC operation center by integrating stealth and SPLUNK security tools. ? Worked on QA (Quality of Assurance) by testing Stealth security software ? Worked as security consultant and provided Stealth IT security recommendation based on client's system design. ? Worked on migrating customer's security licenses and updated stealth services ? Worked on Stealth security- verification and certification on V-lab environment ? Implemented PCI-DSS Audit requirements by examining Identity Access Management (IAM) ? Worked in Cloud security and management in cross -functional environment (RM) ? Reviewed Unisys's third-party service provider's system structure and determines COBIT compliance solution to maintain efficient and productive environment. ? Worked on VMware and Cloud security infrastructure supporting AWS and Azure platforms. GSA/Protiviti Gov - Alexandria, VA September 2016 to October 2016 Alexandria, VA. Sep- October/2016 Used NIST and FISMA security requirement compliance control to manage GSA systems and provided subject matter expertise on managing the corporate

security including ISA/MOU Worked on two factor authentications using PKI system auth. management. Developed and provided input on existing documentation in compliance with GSA Provided training to team memebers in regad to Payment Card Industry (PCI) security compliance project per PCI DSS guidelines Assessed verification and validation of security policy in compliance with NIST-800 and ISO 27000 standards. Developed enterprise system risk mitigating strategies of GSA using FIPS 199 and NIST specification regulatory framwaorks. Assessed security program compliance, support program briefs, and coordinate and compile application security-related documentation for various applications Created, maintained and updated C&A documentation and audited existing policy Maintained System Security Plan (SSP), Plan of Action & Milestones (POA&M), Security Procedures, Implementation Guides, and other security documentation when necessary Engaged and maintained in PCI-DSS of GSA auditing process in collaboration with team members to discuss workflow, issues and assignment. Security Analyst/ Information System Security officer ISSO - Reston, VA July 2015 to March 2016 Worked on C&A configuration to DSS standards of Windows/Linux OS best of DISA req. ? Reviewed risk/threat in compliance with the information assurance vulnerability (LAVM) to DOD. ? Worked in Certification & Accreditation (C&A) process for classified network (SIPRNet) connecting Unisys network. ? Worked in processing SSP (System Security Plan) into system applications. ? Certified and worked as Alternate COMSEC custodian to maintain government network and system security control solution. ? Used Windows event manage auditing tools to monitor system security activities. ? Deployed patches on servers to configure on Solaris OS and windows environment ? Worked on evaluating security tools based customers network system design ? Implemented the NIST Risk Management Framework in a complete work environment. ? Used ACAS and Nessus Vulnerability scanning tool to monitor potential security threats and do analysis upon security assessment requirements ? Used MAC OS to configure system structures & monitor network traffic ? Used Solaris, Red hat Linux, Windows in a virtualized environment ? Experienced in designing IDS/IPS, firewall, and cryptographic devices for secure network environment. ? Worked on reviewing and remediating items found during vulnerability scanning tools ? Worked on system compliance of DISA Security

Technical Implementation Guides (STIG) ? Integrated PCI-DSS security compliances with Unisys security policies to maintain corporate network design. ? Worked as Information Systems Security Officer (ISSO) as subject matter experts ? Used ASA firewalls applications and McAfee Web Gateway for filtering network traffic Worked in network architecture and deployed network architecture using Cisco ASA Firewalls integrated with IDS/IPS model, Red hat Linux, SVGS, and Windows OS. Used SYS, Error and Event logs for troubleshooting failed systematic endpoint protection. Designed Red hat Enterprise and Windows OS for developing proof of concept on customer's network environment. Conducted web application-layer vulnerability assessments using Tenable Nessus Designed and implicated Patch Management Security Policy of the project. IT Specialist (FEMA) (DHS) - Washington, DC May 2015 to July 2015 Second Job) Developed Incident Response Plan and Procedure Worked with BCP (Business Continuity Plan) with project management for FEMA disaster recovery Collaborated in processing and implementing NIST risk management framework(RMF) FIMA. Worked with primary team lead in hardware and computer security Implemented Winmagic encryption technology on computers and mobile devices. Designed enterprise LAN network connectivity and configured security policies Programmed telegram and voice over IP telephone and monitored users' connectivity issues. Used SSL VPN implementation on TCP/IP network architecture. Maintained system security by sanitizing computer's hard drive and set to the original manufacturer program. Diagnosed government electronics devices and mapped to designated network group Preformed data recovery including backup, offsite storage, and remote Journaling. Troubleshoot Windows and Mac OS hardware and system failure on client side. Enterprise System Administrator/Desk Support Specialist Mid II/ Department of Defense/Pentagon - Washington, DC September 2014 to May 2015 Assisted Headquarter DOD Computer Incident Response in the administration of mission critical infrastructure. ? Configured PKI certificate issues and managed access privileges authentication. ? Responded PKI service tickets and assisted in the resetting of PKI certificate. ? Provided maintenance VOIP call support for AD by integrating with PKI services. ? Managed users to access DOD applications by connecting to classified & unclassified network structure. ? Maintained

remotely troubleshoot network connectivity issues and track using Remedy ticketing system. ? Responsible for installing and uninstalling software applications using CIA trend. ? Managed user's profile and changed customers rank and personal info in the GAL. ? Assisted users using Outlook - Exchange Server and Internet Explorer technical issues. ? Updated software applications and deployed system backup. ? Worked IP phones and fixed network connectivity issue using security parameters. ? Escalated tickets to security level service and provided resolutions ? Used Active Directory and Microsoft Exchange services to enforce group and user's policy. ? Worked on account management by modifying DOD user's profile ? Collaborated with System Security Team on Implementing NIST -800-Rev-4 frameworks. Computer & IT Specialist ADT - Gaithersburg, MD April 2014 to December 2014 Performed security gap analysis by comparing existing security policy in compliance with PCI -DSS and ISO 27001/27002 standards. ? Preformed employees training to adhering PCI standards. ? Coordinated with risk management team and worked on auditing compliances. ? Migrated new application and documents from laptop to a host station. ? Configured iHubs, routers, and modems by configuring the devices to work with ADT ? Designed security solution for IT infrastructure. ? Installed physical IDS, Motion detectors, and Sensors. ? Setup emails encryption using PKI and PGP to maintain security of business standers. ? Implemented network security system parameters using active directory. ? Trained employee usage of electronic devices such as (laptops, iPods, and PDA's) ? Installed CCTVs and Alarm system (Motion Detectors, Fire, and Carbon monoxide) ? configured VPN using IPsec security standards to access to the ADT network ? Used Cisco VLAN trunking to set network security system. ? Reviewed the implemented third party access control systems ? Examined security computer systems, change management process using SDLC. System Analyst Support /CTR Quality Technology - Falls Church, VA January 2014 to April 2014 Coordinated CMS employees to access Government security through MMS security portal. Used Remedy to assist Agents to solve technical difficulties regarding Health care enrollment with level of Need to know and Clearance level. Supported Agent/ brokers by resetting security the password, unlocking account, and walking through the CMS (Center for Medicare and Medicaid) portal to complete the registration

process. Provided phone support in compliance with established policies and procedures by obtaining contractual Service Level Agreement (SLA) metrics. Provided risk management procedures to manage scope of the system support Used Five9 phone application system to monitor phone calls to a system. Assisted the administrators and remote user workstations and resolution of remote connectivity issues. Resolved escalated tickets and email by supporting for local and off-site users. Supported security incidents and escalated potential incidents to security incident handling team. System Specialist Great Indoors - Gaithersburg, MD May 2008 to July 2011 Managed security of all systems and enhanced the company policy. Installed antivirus and malware removing softwares on the client computer. Maintained and troubleshoot laptop & desktop computers and others Migrated document, files, and application of Windows OS. Upgraded software problems and settled up computer security measures Installed software and applications on customer's personal computer Assisted with complaints, orders, errors, account questions, billing, cancellation, & other queries. Worked on configuring and fixing printers of HP and Xerox models, and others and documented all system changes. Installed security patches to computers, smartphones, tablets, & electronic accessories and as necessary. IT Coordinator/Instructor Nile College & Sheba College 2005 to 2008 Coordinated and facilitated IT system across all sectors ? Trained instructors to familiarize with new IT technological for all educational system ? Created and implemented college IT teaching curriculum. ? Coordinate distance educating students and facilitated by integrating IT solution ? Provided classroom instruction to college students graphics design and information technology including software and hardware's ? Installed and repaired computer hardware and software in the university ? Provided networking connectivity maintenance- to facilitate educational system ? Developed, implemented, and maintained policies, procedures, and associated training plans for network administration and usage. ? Designed and maintained LAN/WAN/MAN network infrastructure for the institution ? Provided maintenance and incident/problem resolution for network-related issues Education B.S in Cyber- Security University of Maryland - Adelphi, MD May 2018 AAS in Cyber Security Montgomery College - Germantown, MD May 2014 M.S in Cyber- Security Policy and Management University of

Maryland - Adelphi, MD Skills Risk Management, Compliance, Governance, SOX, Hospital

Certifications/Licenses Security+ Present CEH June 2018 to June 2022 Class D Security License

Name: Joel Fisher

Email: jasonrichardson@example.net

Phone: (745)304-8595x811