Cyber Security Engineer/ISSO Cyber Security Engineer/ISSO Cyber Security Engineer/ISSO - Novetta Woodbridge, VA Broad knowledge of hardware, software, and network security technologies that provide a powerful combination of analysis, implementation, and support. Experience in performing analysis of network traffic/DNS, utilizes project management skills for time sensitive assignments, and provides vulnerability analysis for a variety of security technologies that entail research/report to upper management. Strong command for FISMA and NIST guidelines in C&A efforts, and provides compliance knowledge and solutions in a diverse work environment. Recommended and developed secure solutions for all TSA Information Assurance and Cyber Security Division. Protected confidentiality, integrity, and availability of business processes for Federal information systems for TSA, CBP, FBI, the Air Force. INTENTION To support all designated areas of business in an Information Security role where my technical knowledge, initiative, and understanding of company assets will be of value. Work Experience Cyber Security Engineer/ISSO Novetta January 2019 to Present Validates the security of a cloud-based classified information system and ensure the ~~~~~~~~~ compliance with DoD policy. ? Ensures that the system is securely configured and properly documented to achieve and maintain Authorization to Operate (ATO) by working with the ISSM, cyber team, engineers, and developers. ? Writes and walidates body of evidence documentation for classified information systems using multiple overlays. ? Works part of a team which builds and maintains the Risk Management Framework (RMF) authorization body of evidence, to include: System Security Plan (SSP), Security Control Traceability Matrix (SCTM), Continuous Monitoring Plan, Incident Response Plan, Access Control Plan, Security Assessment Plan, etc. ? Architect, implement, and support monitoring of information security operations center.. ? Provide security engineering support to other tools, sensors, and assets with ongoing analysis, recommendations, and support for continuous improvement of cyber security. ? Perform troubleshooting and problem resolution to restore auditing and monitoring services. ? Provide technical and administrative support relative to the problem definition ? Analyze issues and recommend alternative solutions to end users and other stakeholders. Information Systems Security Officer Allied Associates International December 2017 to January 2019 Operate

as the Information Systems Security Officer (ISSO) for this specific government agency's division. ? Provides security engineering designs and implementation in all aspects of Information Assurance and Information Security (InfoSec) Engineering. ? Assesses and mitigates system security threats/risks throughout the program life cycle. ? Validates system security requirements definition and analysis; establishes system security designs. ? Implements security designs in hardware, software, data, and procedures. ? Verifies security requirements. ? Function as the systems security subject matter expert (SME) in configuration control board (CCB) meetings. ? Performs system certification and accreditation planning and testing and liaison activities, and supports secure systems operations and maintenance. Information Systems Security Officer Crystal Management October 2016 to December 2017 Ensure the implementation and maintenance of security controls are in compliance with security laws, regulations, guidance, and requirements as determined by their General Support Systems and/or Major Applications. ? Manage the security aspects of the assigned information system which include, but is not limited to, physical security, personnel security, incident handling, and security awareness and training. ? Develops system security policy, system security plans, and ensures compliance with the policy on a routine basis. ? Controls changes to the all assigned information systems as well as assesses the security impact of those changes from a security professional standpoint. ? Coordinates with external agencies and assists in the preparation of the Information Security Agreement to ensure all external connections meet protection requirements, and that those requirements are documented accurately in the Security Plan, Risk Assessment, and Security Operating Procedure documentation. Information Security Officer mLINQS April 2016 to October 2016 Manages company security program, hosted application site, and user accounts that access the site. ? Conducts and documents vulnerability scans, which are set to occur monthly and quarterly. ? Act as an Account Manager for government customers that use mLINQS hosted application. ? Created the following policy and procedures documentation that relate to FISMA compliance: Security Categorization, Privacy Impact Assessment, System Security Plan, Security Assessment Report, Plan of Action and Milestone, Contingency Plan, and Configuration Management Plan. ? Performed periodic training to employees and lead mandatory

annual security awareness training meetings. Assessor Team Lead (Federal Employee) Transportation Security Administration November 2014 to April 2016 Risk Mgmt Continuous Diagnostic & Mitigation SME June 2012 to November 2014 Part-Time Technical Analyst Reston, VA January 2013 to May 2013 Utilized IPS/IDS (intrusion prevention systems/intrusion detection systems) systems on a daily basis in order to determine if Cyveillance customer(s) are experiencing specific malware attacks. ? Examine, analyze, and mitigate targeting attacks that involve phishing, branding, copyright infringement, trademark violations, malware detection, and online impersonation activities. ? Perform incident response services to online threats for customers with various products offerings from a multitude of industries ranging from Banking, Pharmaceutical, Government, etc ? Assists in tracking of unresolved cases to ensure their successful completion or escalation to the appropriate individuals or organizations based on established guidelines and procedures. ? Communicate tactfully and effectively utilizing oral and written communication skills. Compliance Analyst (Contractor) FISMA May 2011 to June 2012 Serve as the agency Subject Matter Expert in the daily execution of the regulations contained with FISMA of 2002. Ensuring that all security performance metrics are thoroughly and accurately reported according to FISMA regulations, and that activities are tracked and are submitted to the designated higher authorities. ? Managing the application of the Security Authorization (SA) program to ensure TSA information systems are in compliance with applicable Federal, Departmental, Administration Directives, and Congressional Mandates. ? Develop guidance and procedures for using the SA document related templates to ensure consistent data input, assessments, and document quality. Conduct training and presentations as needed to enhance the SA process. ? Provide support to the Information System Security Office community in support of SA related activities for infrastructure systems. ? Ensure that the NIST Risk Mgmt Framework SP 800-37 is properly applied to the agency IT system enterprise. ? Ensure proper reporting of TSA activities that involves 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. ? Directly supporting the Section Chief and the Branch Manager in the

creation of proper execution of all TSA IT systems Plans of Actions and Milestones as a result of executing the assessment phase of the Risk Mgmt Framework. ? Collaborating with the IAD Security Infrastructure team in reviewing and analyzing raw automated scan results, with the Audit Team in the sharing of system information and testing results, and with the IAD Focused Operations team in working on cross-programmatic projects. ? Perform duties as the Continuous Diagnostic & Mitigation subject matter expert for all of TSA information technology systems, while abiding by processes and procedures mandated from DHS Information Security Performance Plan. ? Ensure proper reporting of TSA activities that involve confidentiality, integrity, and availability of systems, networks, and data through planning, analysis, development, implementation, maintenance, and enhancement of information systems security programs, policies, procedures, and tools. ? Perform and provide advice to Engineers and Information Systems Security Officers for Nessus scanning requirements for all of TSA in a variety Operating System environments. ? Maintain, administer, and troubleshoot issues dealing with SharePoint and TSA's intranet web architecture. ? Provide oversight and apply program management techniques to ensure that the TSA Information Systems Continuous Monitoring program is executed in accordance with published directives and policies, while providing support to upper management in the creation and proper execution of the TSA Ongoing Authorization process. ? Developed risk evaluation processes and methodologies to stay ahead of federal requirements and industry best practices. ? Participated in a $3 million software development project named Compliance and Risk Mgmt Application that was implemented to support TSA's Continuous Monitoring efforts. ? Ensure that division goals are met through the security and performance metrics of the FISMA scorecard while maintaining high quality deliverables being reported and tracked according to FISMA regulations. ? Responsible for managing and maintaining TSA's specific IT Security Architecture for the Risk Mgmt Program. ? Work closely with IT Security Engineers supporting functional and business requirements for monthly Continuous Monitoring efforts pertaining to vulnerability scans. ? Performed product evaluations and software testing against multiple applications. ? Coordinate with system administrators, engineers, and security architects in order to establish connections to various data

feeds and security monitoring applications. ? Developed guidance and procedures for fulfilling Security Authorization requirements, while ensuring consistent data input, assessments, and document quality aligned with DHS Risk Management Framework related templates. ? Responsible for managing/monitoring all applications due to continuous monitoring and ongoing authorization efforts to ensure TSA information systems comply with all applicable Federal, Departmental, Administration directives, and Congressional mandates. ? Contribute to initiating FISMA metrics such as Annual Testing, POA&M Management, and Program Management. ? Conducted ongoing training efforts for TAFT, RMS, FISMA and other DHS/TSA related IT security mandates which may include developing and presenting briefings given to an audience of other IT professionals. ? Participate in the development and maintenance of reports, which serve to monitor and track multiple FISMA related metrics. ? Analyze DHS-issued fiscal year policy documentation to determine the upcoming annual metrics TSA must follow and enforce. ? Use and maintain expertise in IACS/XACTA which include but are not limited to, data research, report creation, account maintenance, data entry, file upload/downloading, etc ? Attended training involving Contingency Planning, Disaster Recovery, and Continuity of Operations. ? Perform review of security documentation such as SSPs, RAs, CPs, CPTRs, ST&E Plans, ST&E results, weakness matrices, PTAs, and others. IT Security Engineer (Contractor) - DOD Secret Clearance STG/Department of State - Washington, DC November 2010 to May 2011 Serve as the office information assurance subject matter expert. ? Support and advise executive agencies on ways to be in compliance with federal and civilian agency requirements as practiced at the Department of State. ? Formulate and develop security plans that are compliant with the information assurance system development life cycle. ? Perform audit analysis on Dept of State's Information Technology Asset Baseline for application inventory justification. ? Develop weekly sites security score reports for reporting vulnerabilities and compliance issues within major Department of State databases. ? Utilize processes within the Certification and Accreditation environment such as system security categorization, development of security and contingency plans, certification testing, system accreditation and continuous monitoring. FISMA Analyst (Contractor) Alon/Department of Homeland

Security - Springfield, VA July 2010 to November 2010 Provide technical input for FISMA/ Certification & Accreditation activities. ? Coordinate with technical stakeholders to develop C&A documentation such as Security Risk Assessment, Security Test and Evaluation Plan, Systems Security Plan, and Plan of Action and Milestones based on NIST 800-53 A Revision 3. ? Develop and complete security plans based on the National Institute of Standards and Technology (NIST) Special Publications. ? Complete risk assessments based on NIST standards to ensure IA design sufficiently mitigates IA risk. ? Develop and conduct security tests and evaluations based on NIST 800-53A. ? Manage Plan of Action and Milestones for accuracy and currency. ? Assist with contract and vendor management issues directly related to security requirements and deliverable of projects. ? Gather and analyze information for defining requirements, specifications and issues to support the development of new policies, standards and procedures or update existing ones. ? Perform and oversee basic to complex security analysis, standards design, and security gap analysis. ? Utilize TAF (Trusted Agent FISMA) to input various Plan of Action and Milestones for the Department of Homeland Security. Associate Security Analyst Richmond, VA November 2008 to July 2010 Monitors, evaluates, and maintains security systems and procedures established to safeguard information assets from intentional or inadvertent access or destruction. ? Evaluates and resolves security related problems and advises users on security issues. ? Exercises independent judgment and decision-making in planning, organizing and conducting work assignments. ? Perform reviews and developed security policy plans and operating procedures in compliance with NIST and FISMA mandated policies. ? Provides technical assistance to users concerning network security, virtual private networks and computer network defenses. ? Conducted vulnerability assessments and audits of enterprise network Infrastructure using nCircle IP360 software. ? Effectively utilizes the proper resources to develop solutions and devise new approach encountered in work assignments. ? Provides technical and administrative support in the modification, design, and set-up of applications security and firewall management. PC Technician (Contractor) Richmond, VA March 2008 to November 2008 Provide second and third tier technical support and problem management to end users on the moderately complex issues regarding computer operations and

networks. ? Arrange remote installations of software, setup of new workstations, and technical troubleshooting for a variety of customers in the insurance industry. ? Supports a variety of users ranging from the Tidewater region up to the D.C. area. Associate LAN Administrator (Contractor) Richmond, VA January 2007 to January 2008 Install network software and train users on LAN operations via phone support. ? Communicate with clients and coworkers in Lotus Notes emailing system. ? Configured and tested client workstations to utilize VPN access using secure token identification. ? Arrange workload by using USPSD ticketing system with call volume ranging from 50 - 100 tickets a day. ? Manage workload by prioritizing tasks in a multitasking environment and adjusting to any situation at hand. ? Installed and configured SAP applications to meet client needs. ? Evaluate and recommend hardware\software solutions plus telecommunication equipment that meet the end user's business requirements. ? Support various company wide multi-platform environments daily. ? Support and work collaboratively towards solutions that generally benefit all parties and accomplishes company/group objectives. ? Demonstrate a sense of commitment by addressing issues or problems that affect customers plus their performance on a daily basis. ? Support a team effort environment and work collaboratively towards issues to benefit IT and the end user. Albemarle Corporation - Richmond, VA July 2006 to January 2007 Resolved IT issues and work orders for Executives. ? Troubleshoot and update end-users in mixed Windows NT4/Active Directory network environment. ? Upgrade user maintenance and network share security in mixed network environments. ? Work daily with Windows 2000 Professional and Windows XP operating systems, Windows 2003 Server/Window NT4 network servers, and Office 2000 products. ? Plan, coordinate and implement upgrades of multiple applications including Lotus Domino, Lotus Domino Server, Lotus Notes client software and support and Windows XP. ? Communicate daily with end-users in Lotus Sametime. ? Maintain, troubleshoot and support HP network printers, Blackberry handheld devices, videoconferencing, SAP software applications, LAN/WAN connections, IBM client-server environment. ? Provide end-user support and system maintenance for video conferencing systems in a LAN/WAN environment. Tech Team Specialist (Internship) MeadWestvaco - Richmond, VA July 2005 to December 2005 Under general direction,

perform analytical and technical work to aid in the on-going support of technology assets in the enterprise, including installing, maintaining, troubleshooting, supporting, and controlling critical infrastructure. ? Assist with end-user questions, problems, and training. Install common and standard software and hardware peripherals. Configured third-party, networked, and site-specific applications. ? Troubleshoot hardware and software problems using standard problem management tools and processes, document problem resolution at each step. ? Work primarily with technology assets including single-user and networked desktop and laptop clients, network switches and cabling with some exposure with fiber optics. ? Manage and maintain phone/video systems running over IP and ISDN networks using Polycom and Lucent technologies. Education Master of Science in Management in Information Sys Security Colorado Technical University - Colorado Springs, CO May 2010 Bachelor of Science in Business in Information Systems Virginia Commonwealth University - Richmond, VA May 2006 Skills Cyber Security, Siem, Network Security, Information Security, Nist

Name: James Gillespie

Email: williammclaughlin@example.org

Phone: 293.792.5772x55855