Principal Cyber Security Analyst/Validator Principal Cyber Security Analyst/Validator Sr. Information System Security Officer Suffolk, VA Work Experience Principal Cyber Security Analyst/Validator SAIC - Remote December 2018 to Present Responsible for conducting a comprehensive assessment of the management, operational, and technical security controls employed within or inherited by an information system to determine the overall effectiveness of the controls. The validator leads a team of cybersecurity analysts who complete the cybersecurity tasks to be validated. Reviews cybersecurity RMF packages for 21 systems - Tracks 21 systems progress and coordinates with inside and outside groups to accomplish RMF Step 1-3 tasks - Tracks vulnerability testing and scans, as well as configuration updates. - Tracks all Category I and II vulnerabilities within the systems - Works with the System Administrators to ensure STIGs are applied within the environment - Operates software tools needed to effectively observe and analyze network vulnerabilities - Configures and carries out necessary testing on dedicated application vulnerability. - Plans scans to effectively detect malicious software and hardware that might be present on the network. - Carries out audits of existing and newly acquired systems - Making recommendations on improvements to internal controls and security - Carrying out information security risk assessment annually in accordance with the RMF framework. - Ensure anomalies are effectively handled by developing prompt response procedures. - Completing statistical and status reports, as well as providing fast and timely responses. - Identifying ways to improve security by suggesting configuration changes to server, network, client, and/or security devices. - Coordinating with the Systems Administration team for network updates, patches and version changes. - Preparing weekly reports - Presenting results and progress to the team in Weekly Reviews Work with other cybersecurity team members to ensure Steps 1-3 of the RMF process are completed satisfactorily. Deputy Cyber Lead/Vulnerability Manager Raytheon - Hampton, VA December 2017 to Present Maintaining AOC WS security posture by performing the following: Perform technical security assessment to identify points of vulnerability, non-compliance with Information Assurance (IA) standards and recommend mitigation strategies. Validate and verify system security requirements definitions and analysis and establish system security designs. Design, develop, implement and/or

integrate IA and security systems and system components including those for networking, computing, and enclave environments to include those with multiple enclaves and with differing data protection/classification requirements. Assess and mitigate system security threats/risks throughout the program life cycle. Contribute to the security planning, assessment, risk analysis, risk management, certification and awareness activities for system and networking operations. Develop and review Certification and Accreditation (C&A) documentation, providing feedback on completeness and compliance of its content. Apply system security engineering expertise to one or more of the following: system security design process, engineering life cycle, information domain, cross domain solutions, commercial off-the-shelf and government off-the-shelf cryptography, identification; authentication; and authorization, system integration, risk management, intrusion detection, contingency planning, incident handling, configuration control, change management, auditing, certification and accreditation process, principles of IA (confidentiality, integrity, non-repudiation, availability, and access control), and security testing. Recommend hardware, software, and develop policies and procedures to investigate malware incidents for multiple networks. Develop, implement and maintain the information system security posture across multiple networks Provide security services for Certification and Accreditation (C&A) requirements, including developing and maintaining information assurance documentation for all network components. Conduct bi monthly vulnerability scans and reconcile results, and report all findings. Establish common processes across tasks, including Configuration Management (CM), risk management, Quality Assurance (QA), etc. Oversee identification and draft mitigation guidance for vulnerabilities with no-vendor provided remediation. Analyze and Prioritize publicly disclosed vulnerabilities of vendor software/hardware products and develop mitigation/remediation orders. Manage daily, weekly, monthly and annual vulnerability metrics associated with affected and non-compliant DoD Assets. Develop, document, and convey Operational Requirements to enhance the identification, tracking, and remediation of system and network vulnerabilities. Manage Tenable Security Center vulnerability detection, assessment, and analysis (ACAS). Ensure ACAS servers are properly maintained and in compliance Sr. Information System Security Officer Trusted QA - Hampton, VA

May 2017 to October 2017 Ability to review system configurations to ensure they are in accordance with agency hardening guidelines. Experience in reviewing proposed change requests related to system design / configuration and perform security impact analysis. Experience in reviewing monthly vulnerability scan reports and track and address weaknesses in POA&Ms as needed. Assist with the management and administration of applicable IT systems' operations and ensuring compliance with federal security regulations, policies, guidelines, and applicable National Institute of Standards and Technology (NIST) standards. Manage and coordinate audits and reports system security matters with the PM, System Owner, and DoD Officials. plan, configure, deploy, maintain, and upgrade COTS/GOTS and custom toolsets to address vulnerabilities and/or implement security controls. Apply a combination of expert engineering knowledge of enterprise IT and security solutions to design, develop and/or implement solutions to ensure they are consistent with enterprise architecture security policies and support full spectrum military cyberspace operations. Designs, tests, and implements secure operating systems, networks, security monitoring, tuning and management of IT security systems and applications, incident response. Aiding the customer in planning, managing and achieving Certification and Accreditation of GCCS-J/AF software and facilities. Lead Security team in the performance of ACAS scans, DISA Security Checklists (STIGS), SCAP scans and the performance of manual security vulnerability assessments. Participate in peer reviews of Assessments conducted by other technicians. Assist the Authorization Official in the oversight, inspection, review, and assessment and authorization of GCCS-J Sr Information Assurance Engineer Insight Global/Northrop Grumman - Hampton, VA April 2015 to April 2017 My main objective is to address security matters for the end client. Assist in investigating and analyzing response activities related to security incidents/events. Conduct highly technical examinations, analysis and relay these issues to the appropriate teams for resolution. Also be expected to document all incidents and help to prevent from these happening again in the future. Provide hands-on consulting services to clients that will offer enhanced levels of information security by utilizing the DIACAP, RMF and NIST controls. Conducts Risk Assessments and Information Security Program Assessments. Interprets information security policies, standards, and other

requirements as they relate to a specific internal information system, and assists with the implementation of these and other information security requirements. Complete assigned functions as stated in engagement proposals, or other statements of work. Understands and communicates engagement objectives internally and to the client. This includes both overall engagement goals and specific consultant objectives. Leverage subject matter expertise and consulting experience to help the client create information security solutions. Develops and communicates security strategies, solutions and plans to client executive team, staff, and stakeholders. Works closely with the client to fully secure information, computer, network, and processing systems. Creatively and independently provide resolution to security problems in a cost effective manner. Assess and communicate any and all security risks associated with any and all purchases or practices performed by the company. Collaborate with CIO leadership, privacy officer, human resources to establish and maintain a system for ensuring that security and privacy policies are met. Use ACAS to verify proper vulnerabilities in place on our network and deliver patches to fill the DISA IAVM requirement for each plugin. Sr. Information Assurance Analyst General Dynamics Information Technology - Suffolk, VA October 2014 to March 2015 Responsibilities Duties: Conduct Security Test and Evaluations of Joint Staff Programs. Enforce certification and accreditation policies during system security plan, POA&M, security package process using the RMF SP 800-37 format. Prepares incident reports of analysis methodology and results. Performs periodic and on-demand system audits and vulnerability assessments, including user accounts, application access, file system and external Web integrity scans to determine compliance. Ensures the integrity and protection of networks, systems, and applications by technical enforcement of organizational security policies, through monitoring of vulnerability scanning devices. Evaluate firewall change requests and assess organizational risk. Communicates alerts to agencies regarding intrusions and compromises to their network infrastructure, applications and operating systems. Performs Computer Security Incident Response activities for a large organization, coordinates with other government agencies to record and report incidents. Ensure Consistent integrity with DoD Cybersecurity policies, standards, architectures, security controls, validation procedures and tasks that Defense Information Systems Agency (DISA)

requires for finalization with C&A request. Sr.System Administrator General Dynamics Information Technology October 2012 to October 2014 Kabul, Afghanistan Duties: Maintain and implement Windows Server 2008, Bes Servers (Blackberry), SANS, SCCM, Microsoft Exchange, V-Sphere/VM Ware, Active Directory, DHCP, Printer Servers, File Servers, Use Retina to scan Servers to Enforce Information Assurance Vulnerability Alert (IAVA) Compliancy, Manage WSUS, and Use What's Up Gold for Accountability for System Equipment. Detect, analyze, and resolve problems associated with hardware, operating systems. Create Security Groups, Modify Permissions, Group Mailboxes, Distribution lists. Ensure adequate security measures are applied to servers/clients to ensure network protection. Use Symantec NetBackup to backup data/systems and recover. Maintain the integrity and security of servers and systems, system documentation. System Analyst ITT Systems February 2011 to October 2012 Camp Buehring, Kuwait Duties: To provide and adhere to IT support and tactics 60hours weekly for 581st Signal Company "Netcom". Equivalent to GS11 Responsibility for monitoring, operating, managing, troubleshooting and restoring to service any personal computers (PC) or notebooks that are authorized access to the network. Receive and log work request using applications such as Remedy. Ensure that supported customer accurately completes the approved work request with the date and time of submission. Provide phone and help-desk support for local and off-site users. Ensure the maintenance technicians close out their work orders properly and then log the work order in the automated system. Utilize Active Directory to create user accounts, groups, and new computer objects as well as to reset passwords. Monitor network connection and stability using WhatsupGold network utility. Utilize Retina to scan computers on the Network for compliancy. Provide user with required patches needed for network compliancy.Screen, refer and diagnose internal inquiries and work requests as they relate to maintenance of personal computers and related systems. Install, configure, and upgrade computer hardware and software. Provide end-users with software troubleshooting and support. Apply diagnostic techniques to identify problems, investigate causes, and recommend solutions. Assist in the administration of email systems. Assign end-users with permissions and file access on the network. Utilize DHCP to reserve printer IP addresses. Desktop Engineer Altek/Lockheed Martin -

Suffolk, VA March 2010 to February 2011 Joint Force Command) Duties: Provide technical assistance to computer system users, with their hardware and software needs, including printing, installation, word-processing, electronic mail, and operating systems. Maintain a service perspective including an understanding of relationships, dependencies and requirements of hardware and software components and the organizations that support them. Enforced policies to client workstations within the EPO Client.Ensure total maintenance on user workstations to meet and detain security requirements. Answer questions and resolve computer problems for clients in person, via telephone or from remote location. Provides technical, operations, and training support to users of client's personal computers either by telephone or on-site relative to desktop hardware and software packages. Perform hardware diagnostics and coordinate repairs. Assist in planning and designing personal computer support systems. Manages the installation and integration of systems fixes, updates, and enhancements. Act as liaison for data transfer systems design and implementation. Install and test personal computers, printers, and other peripherals; configure operating system, shrink-wrap programs, and applications software programs. Develop reports and databases. Provide technical support for personal computers. Manage account transfers, password resets, Exchange tasks, SharePoint management, printer mapping, and DNS issues. Hardware support includes the maintenance and repair of the JFCOM workstations, associated monitors, ghosting and setup of workstations, printer repair and maintenance, VTC maintenance and repair. DOD Experience with NIPRNET, SIPRNET Systems. Ensuring that the equipment meets DISA Security Technical Implementation Guideline when troubleshooting and modifying PC equipment. IT Specialist Lockheed Martin - Norfolk, VA July 2009 to February 2010 Joint Force Command) Provide Desktop support for the military. Tier 1 troubleshooting with active directory, Microsoft 2003 and 2007, Printers, Laptops. Also Reconnect and deploy helpdesk workstations to secure areas. Fixing User Profiles and provide overall PC/laptop hardware/software. Configure network and basic printer and copier troubleshooting. Strong customer service skills, strong organization skills and ability to manage multiple tasks. Knowledge of Microsoft Windows platform and office suites, working knowledge of trouble ticketing systems. Proficiency with email, directories, and standard

Windows desktop applications. Basic understanding of networking. Demonstrated ability to communicate orally and in writing and a positive customer attitude. Experience with Microsoft Exchange Server 2003. Maintaining User accounts in AD, OU, and creating Mailboxes, Distribution List, Configure Permissions Laid off from 6/11/2009 to 7/9/2009 for Personnel Reduction Tier 1 Technical Support Milvets System Technology - Norfolk, VA June 2008 to June 2009 Tier 1 Provide multi-user computer systems with technical support and analyze difficult situations with VPN and Active Directory to different users on different domain controller throughout the US. Maintain a proficient call rating with troubleshooting and providing superior customer service. Implemented structural database within Information reference to creating trouble tickets and documentation of the solution to the situations. High quality of maintain for setting up administrator and service accounts. Installing system software and delegate potential mass storage space to multi-users workstation. Experience with File Servers, Network Drives Configuration, Microsoft Exchange Server, Microsoft Office, Active Directory, Legacy Application, Internet Explorer configuration, Windows 2000 and XP, Adobe, Some Citrix exp on the NMCI Network supporting Navy/Marines throughout the US and Japan. Highly perform customer and IT troubleshooting services to meet SLA Agreement Prepare activity and progress reports relating to the information systems audit function. Responsible for effectively auditing, inspecting and maintaining changes made against the accepted Army baseline(s) standards. Develop, distribute, and track all change packages resulting from approved Configuration Control Board action. Train personnel by conducting workshops and seminars on the proper methodology to maintain a proactive CM program, and provide daily support and direction to staff as to change status requirements, deadlines, and problems. Receives technical and operational guidance from the Engineering (Systems) - Senior Lead and executes project or task requirements accordingly with minimal to no supervision. Conducts Site Surveys, analyzes the collected data, and performs necessary calculations to make technical recommendations, then prepares or provides input for C4 EIPs. Provides security engineering services and support for all networks and secure environments, as required within the CJOA-A. Coordinates with Certification and Accreditation personnel to develop and/or update certification and

accreditation documents to ensure all engineering solutions provided by this contract meet DoD 8500.2 and DoD 8500.01E regulations. Maintains a secure, archived, accessible library of all documents related to security, certifications and accreditation changes for modifications made to the network by personnel providing service for this contract. Possesses the ability to quickly identify, diagnose and provide solutions to complex problems, requirements and integration of various technologies, which may require out of the box thinking and innovation. Education Masters in Assurance and Security Management Capella University January 2011 to March 2014 Skills Cyber Security, Information Security, Nist Certifications/Licenses MCSE Windows Server 2012 August 2013 to August 2016 MCSA Windows Server 2012 August 2013 to August 2016 EC Council Certified Ethical Hacker (CEH) October 2015 to October 2018 EC Council Certified Security Analyst (ECSA) October 2015 to October 2018 EC Council Certified Network Defense Architect (CNDA) October 2015 to October 2018 HBSS McAfee EPO Server Certified September 2013 to September 2016 Retina Vulnerability Certified Present Comptia Security+ CE July 2017 to July 2020 Comptia CASP July 2017 to July 2020 CompTIA Advanced Security Practitioner (DoD 8570.1 IAT III/IAM II Compliant) Additional Information Competencies Strategic Planning System Analysis IT Security Customer Support Process Improvement Risk Management Network Vulnerability Monitor Auditing Hardware/Software Technician

Name: Anthony Porter

Email: jilljohnson@example.net

Phone: 695.884.0888