Senior IT Security Analyst Senior IT Security Analyst Senior IT Security Analyst - DMI Clifton, VA Authorized to work in the US for any employer Work Experience Senior IT Security Analyst DMI - Arlington, VA August 2016 to Present Develop security documentation, including System Security Plan (SSP), Plan of Action & Milestones (POA&M) and Contingency Plan to ensure compliance Review and analyze third-party vendor Security Artifacts including but not limited to: IT Security Plans, Disaster Recovery Plan, Service Organization Control Reports, and Independent Penetration Tests Execute Information System security assessments within the guidelines of the National Institute of Standards and Technology (NIST) 800 Series publications, Federal Information Processing Standards (FIPS) Implement the system-level controls and maintain system documentation; performed control scoping Serve as IT security specialist on security projects involving a wide range of IT issues. Investigate, document and report any undisclosed software and hardware vulnerabilities. Make recommendations to resolve shortfalls in system security features and practices Evaluate and manage POA&M for Information Systems and develop remediation plans with stakeholders Assemble all findings, results, evidence, and documentation, annual security testing, audits, vulnerability tests Update the appropriate security authorization security documents accordingly with the vulnerability results Review and identify finding from vendor provided Penetration Tests and Vulnerability Scans done by independent third parties as well as tools used such as HP Webinspect and Nessus. Analyzed the raw scan output, verify the results, filter out false positives, identify false negatives, and developed final analysis reports with recommended mitigation actions Assist in all phases of the security authorization process for assigned information subsystems Perform continuous monitoring of security controls Assist in the development and maintenance of security documentation and PIA/PTA for all systems under their responsibility; Develop and maintain network diagram for all assigned systems. Ensure knowledge and skills to incorporate IT security throughout the system s SDLC process to protect the business operations and information the system supports; Coordinate with other designated personnel in preparing the SAP, participate in post-authorization activities, and ensure the appropriate operation security practices are maintained for assigned information subsystems;

Assist with design, implementation, and evaluation of awareness and training activities for the users, operators and maintainers of their systems IT Security Specialist Highlight Technologies - Arlington, VA September 2014 to August 2016 Supported in the area of compliance including: o Vulnerability Management o Continuity Management o Security Assessments o Audit & Reporting Develop security documentation, including System Security Plan (SSP), Plan of Action & Milestones (POA&M) and Contingency Plan to ensure compliance Execute Information System security assessments within the guidelines of the National Institute of Standards and Technology (NIST) 800 Series publications, Federal Information Processing Standards (FIPS) Implement the system-level controls and maintain system documentation; performed control scoping Serve as IT security specialist on security projects involving a wide range of IT issues. Investigate, document and report any undisclosed software and hardware vulnerabilities. Make recommendations to resolve shortfalls in system security features and practices Evaluate and manage POA&M for Information Systems and develop remediation plans with stakeholders Assemble all findings, results, evidence, and documentation, annual security testing, audits, vulnerability tests Develop security documentation, including System Security Plan (SSP), Plan of Action & Milestones (POA&M) and Contingency Plan to ensure compliance Execute Information System security assessments within the guidelines of the National Institute of Standards and Technology (NIST) 800 Series publications, Federal Information Processing Standards (FIPS) Implement the system-level controls and maintain system documentation; performed control scoping Serve as IT security specialist on security projects involving a wide range of IT issues. Investigate, document and report any undisclosed software and hardware vulnerabilities. Make recommendations to resolve shortfalls in system security features and practices Evaluate and manage POA&M for Information Systems and develop remediation plans with stakeholders Assemble all findings, results, evidence, and documentation, annual security testing, audits, vulnerability tests Served in a Technical Assessment role in conducting ISS Authorizations for Systems, which includes annual security self-assessments, independent security control assessments, contingency plan testing, and continuous monitoring activities. Responsible for developing corrective action plans in conjunction

with system owners for Plan of Action & Milestones (POA&M) remediation activities and tracked POA&M status within the Cyber Security Assessment and Management (CSAM) tool. Tracking vulnerability scan results and timely remediation activities for systems. Assisted with the development of a security model and security risk analysis for a system under development. This includes reviewing Memorandums of Agreement between the system and its interconnections with external Departmental and Federal Government systems. Updated the appropriate security authorization security documents accordingly with the vulnerability results Reviewed and identify finding from vendor provided Penetration Tests and Vulnerability Scans done by independent third parties as well as tools used such as HP Webinspect and Nessus. Analyzed the raw scan output, verify the results, filter out false positives, identify false negatives, and developed final analysis reports with recommended mitigation actions Assisted in all phases of the security authorization process for assigned information subsystems Performed continuous monitoring of security controls Assisted in the development and maintenance of security documentation and PIA/PTA for all systems under their responsibility; Developed and maintain network diagram for all assigned systems. Ensured knowledge and skills to incorporate IT security throughout the system s SDLC process to protect the business operations and information the system supports; Coordinated with other designated personnel in preparing the SAP, participate in post-authorization activities, and ensure the appropriate operation security practices are maintained for assigned information subsystems; Assisted with design, implementation, and evaluation of awareness and training activities for the users, operators and maintainers of their systems Information Security Analyst Lender Service Providers - Fairfax, VA June 2013 to September 2014 Participated in the analysis, implementation, and evaluation of current and proposed security initiatives and needs including performing various activities to support Access Control activities including maintaining and monitoring user access, performing monthly reviews, monitoring access to the Network, reviewing audit activities, performing monthly reviews and annual user reviews on applications, IT Resources and Outsourced Contractor Services. Performed assigned tasks that have a high level of technical complexity or organizational visibility or requires specialized technical or analytical expertise.

Planned and implemented data analyses and reporting projects of varying degrees of complexity using a variety of databases and software. Gather facts, analyze data, and prepare synopsis comparing alternatives in terms of cost, time, availability of tools and personnel, and recommend a course of action. Provided advice on information assurance best practices processes and procedures. Assisted in the development of an enterprise risk management framework for managing risk from the senior executive level to the operations level. Participated as a subject matter expert in the areas of privacy, risk management and the protection of sensitive information. Support included the following activities: o Development of a Privacy Handbook and Privacy related Policies; o Development and implementation of a Privacy Implementation Plan and Strategy; o Development of Privacy Awareness Training program for all IT managers; o Development of a PII reduction strategy; o Ensuring compliance with privacy provisions based on Federal mandates, law Senior Analyst Apple Federal Credit Union - Manassas, VA September 2012 to March 2013 Analyzed the administrative security programs and access control mechanisms for information systems. Assisted in the design, implementation and maintenance of comprehensive security program information systems. Developed and implemented procedures for ensuring network survivability and recovery following security awareness and training materials. Monitored their organization s networks for security breaches and investigate a violation when one occurs Installed and use software, such as firewalls and data encryption programs, to protect sensitive information Prepared reports that document security breaches and the extent of the damage caused by the breaches Researched the latest information technology (IT) security trends Helped plan and carry out an organization s way of handling security Developed security standards and best practices for their organization Recommended security enhancements to management or senior IT staff Assisted computer users when they need to install or learn about new security products and procedures Performed technical tasks efficiently and effectively providing a high quality product while meeting project objectives and deadlines under minimal technical supervision. Analyzed technical and functional information security application specifications for accuracy and completeness. Performed information security problem

determination and analysis. Performed research on new and improved ways to protect the information assets. Technical Analyst United Bank - Fairfax, VA May 2008 to August 2010 Gathered supporting documentation, forms and business requirements needed for specific projects. Reviewed business requirements and forms for missing and incorrect information. Created of forms to support development of quoting and enrollment tools. Loaded of forms in the document administration tool. Built out enrollment questions, business rules, disclaimers and other information in enrollment administration tool. Worked closely with manager and effectively communicate updates and edits to documentation with Web Developers, Software Manager and Business Analyst. Worked with stakeholders to prioritize test activities. Provided communications on testing status to the team Kept management informed of special needs or problems. Provided technical support for problems and issues identified for online quoting and enrollment tools. Researched issues and reported the resolution to management. Education Bachelor of Business Administrative in Business James Madison University - Harrisonburg, VA Skills A&A, RMF, CASP, FIPS 199, CSAM, C&A, Microsoft Office Suite (10+ years) Certifications/Licenses ITIL v3 Foundation Security+ CASP CEH Additional Information SECURITY CLEARANCE Secret TECHNICAL SKILLS Networking: TCP/IP, Router Configuration Databases: MySQL, MS SQL, Microsoft Access, Oracle Applications: Visio, Microsoft Office Suite (Excel, Word, PowerPoint), Dreamweaver, SharePoint, Outlook, MS Project Assessment & Authorization: Ongoing Authorization, Security Authorization, FISMA, NIST 800 Series Special Publications, FIPS Standards199 & 200, Risk Management, Security Control Assessment, Plans of Action and Milestones Penetration/Forensic: Windows/Unix Server Analysis - HP Webinspect, Web Target Analysis - Nessus Operating Systems: Windows 8, Windows 7, Windows Vista, Windows XP, Linux Languages: Java, XML and HTML

Name: Nancy Wall

Email: aoliver@example.org

Phone: 6788001960