Information System Security Analyst Information System Security Analyst Information System Security Analyst - Caelum Research Corporation Washington, DC Authorized to work in the US for any employer Work Experience Information System Security Analyst Caelum Research Corporation - College Park, MD June 2016 to Present Develop, review, and update Information System Security Policies, System Security Plans, and Security baselines in accordance with NIST, FISMA, OMB App. III A-130 and industry best security practices. Applied appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53, FIPS 199, FIPS 200 and OMB A-130 Appendix III. Document, review and update System Security Plan (SSP), Security Assessment Report (SAR), Security Plan of Action and Milestones (POA&M), to obtain system Authorization letter/memorandum (ATO). Developed and conducted ST&E (Security Test and Evaluation) according to NIST SP 800-53A and perform on-site security testing using vulnerability scanning tools such as NESSUS Reviewed scan report and advice system owners on remediation efforts. Performed Federal Information Security Management Act (FISMA) audit reviews, using NIST 800-37 rev 1. Updated IT security policies, procedures, standards, and guidelines according to department and federal requirements. Performed risk assessments, developed and review System Security Plans (SSP), Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Management Plan (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation in accordance with NIST SP 800-37 rev 1, 800-18, 800-53 rev 4 and 800-34. Performed, post authorization monitoring of security controls to ensure continuous compliance in accordance with FISMA guidelines. Analyzed Nessus vulnerability result in accordance with the organization Continuous Monitoring Plan and NIST 800-137. Information System Security Analyst Rockville, MD January 2014 to June 2016 Reviewed monthly vulnerability scan reports and track and address weaknesses in POA&Ms as needed. Develop, implement and maintain an information security plan for newly formed enterprise systems and legacy systems. Identify, implement and maintain information security processes, through automated and continuous monitoring to detect, contain and mitigate incidents that can impair and compromise a system. Develop and maintain documentation such as SSP,

SAR & POAM for C&A in accordance with NIST Publication and OMB Circular policies. Identify vulnerabilities within the information technology infrastructure and work with the responsible team(s) to resolve these issues. Provide Continuous Monitoring for security-relevant information system components. Develop and manage security plans, procedures, and documentation for accreditation of all Government owned Information Systems. Create and compile Authorization packages to include: Designation Letters, Security Plans, Contingency Plans, SOPs, SAR, POAM Communicate and enforce security policies, procedures and safeguards for all systems and staff, based upon NIST and agency policy. Provide advice and guidance on matters relating to information security. Provide support for implementing, and enforcing information systems security policies, standards, and methodologies. Assist with the management of security aspects of the information system and perform day-today security operations of the system. Develop system security documentation and ensures RMF compliance. Knowledge of current security tools, hardware/software security implementation; communication protocols; and encryption techniques/tools. Initiate, coordinate and track the remediation of security weaknesses as they are discovered, via a "Plan of Actions and Milestones" (POAM) Carried out the preparation of Assessment and Authorization (A&A) packages for submission to the Authorizing Official (AO) for an Authorization to Operate (ATO). Performed Federal Information Security Management Act (FISMA) audit reviews using NIST 800-37 rev 1. Information Security Compliance Analyst REI Systems Inc - Sterling, VA August 2012 to January 2014 Identified information types collected, processed, maintained, used, shared, disseminated, transmitted, and/or stored by or through the information system. Using SP 800-60 and FIPS 199, evaluated the information types related to the data and document this information in the Security Categorization Worksheet. Determined which information types, if any, contain privacy data and/or financial data. For each information type identified, determined the security impact that might result from the unauthorized disclosure, modification, and/or loss of the information (Confidentiality, Integrity, and Availability [CIA]) and adjust the default CIA impact levels as necessary. Using the impact results of the information types, applied the high watermark concept to derive the appropriate categorization level of the

system. Using FIPS 200, selected the applicable security controls to the information system. Documented the selected security controls in the SSP. Implemented the security controls outlined in the SSP. Participated in information-system authorization briefings and associated meetings to review the assessment results. Supported the development of Plans of Action and Milestones (POAM), documenting corrective action plans for remediation of identified security control deficiencies. Reviewed and validated the Security Authorization Package (SAP), which includes, the SSP, Risk Assessment Report (RAR), Security Assessment Report (SAR), POAM Status Report, Privacy Threshold Assessment (PTA), Privacy Impact Analysis (PIA), E-Authentication Threshold Analysis (ETA), E-Authentication Risk Assessment (ERA), Request for Authorization to Operate, and Authorization Decision Letter. Develop/update the SSP and other relevant security documentation Maintain and update all security-related documentation during the Continuous Monitoring period. Supported the management of POAMs by remediating weaknesses and findings, working with support personnel and vendors to develop fixes, and provide POAMs status updates to management. Supported the documentation and implementation of all technical, operational, and management controls in accordance with NIST guidance and FISMA requirements for all designated systems within his/her portfolio. Linux Systems Administrator STAVANGA ATS - Baltimore, MD June 2010 to August 2012 Hands on experience providing Enterprise support to Linux servers hosting Red Hat and CentOS Linux 6 and 7 in Production and Development environment. Perform installation and support of Red Hat Enterprise Linux 6 on Dell Servers in a Data center Environment. Hands-on experience Supporting Server Clusters. Installed, configure, update and manage Red Hat Enterprise Linux Versions 6 CentOS version 6 and 7 on Dell PowerEdge R720xd and Dell PowerEdge 2650 Servers. Experience in performing Server Auditing and Hardening to meet Standard Security Policy and Guidelines. Experience using VMware EXSi 5 for Server Virtualization. Scheduling and automating task using corn jobs to run backup scripts Performed backup of system data for on-site and off-site storage. Experience in compiling and Installing Apache HTTP, MySQL and PHP Validating remediation efforts of findings related to vulnerability and system configurations. Implementing, testing, and maintaining defined security

solutions. Resolve POAMs by assisting other systems administrators in describing the weaknesses, creating the mitigation plan and vetting potential solutions from the security assessment report-SAR Update SSP and POAM Documentation and Tracking of issues, logs and audit files. Experience in Administering users account and passwords on Red Hat 5, 6 and CentOS 5, 6. Experience Creating users and groups; assign users to group for group collaboration and granting access to resources, application and services. Skillful in troubleshooting Network connectivity issues as well as implementing TCP/IP protocol on the host computers and Severs. Working knowledge of networking and security best practices on Servers Experience Monitoring Network services and System performance using Nagios Monitoring tools. Experience in performing network authentication of users using IPA and configuring network access to shared directories. Experience using Linux Bash shell in performing System Administration task Configure Local firewalls and managing Iptables on host systems and Servers. Strong experience in creating and managing file systems using Logical Volume Management - Red Hat LVM. IT Help Desk Technician CompuTech - Baltimore, MD February 2008 to June 2010 Assisted with Software and Hardware installation. Configure Motherboards, Sound cards, Network cards, Printers, Video Cards, Memory and hard disk drive. Answer customer request for assistance by phone and email Escalate technical support issues that could not be addressed by Help Desk to the appropriate technician. Troubleshoot and resolve Network connectivity issues. Troubleshoot, resolve and maintenance of network printers Troubleshoot and resolved basic network and server access problems for end-users, when possible from the Help Desk Resolve computer problems for clients in person, via telephone and via remote assistance Perform Software and hardware distribution, maintenance, update and testing SCANNING /ASSESSMENT TOOLS CSAM Retina WebInspect Burp Suite Nessus ORGANIZATION / MEMBERSHIP: Phi Theta Kappa. Honor Society Information Systems Security Association (ISSA). National Technical Honor Society. Education Master's Skills Security, Networking, Server virtualization, Virtualization, Information security, Vm, Vmware, System development, Life cycle, Sdlc, Risk assessment, Risk management, Goal oriented, testing

Name: William Villanueva

Email: jonesamanda@example.org

Phone: 001-559-841-2093x07814