Cyber Security Analyst - Rx- IT Cyber Security Analyst - Rx-IT Cyber Security Analyst - Rx- IT Washington, DC To develop a career in the information security sector as an Public Policy Analyst in a growing company where my skills and experience will be utilized in achieving the goals and objectives of the organization. Work Experience Cyber Security Analyst - Rx- IT Security Assessment June 2015 to September 2016 Duties included: Coordinate in-depth interviews and examine documentation/artifacts in accordance with NIST SP 800-53A rev 4. Perform Federal Information Security Management Act (FISMA) audit reviews using NIST 800-37. Conduct risk assessments and collaborate with clients to provide recommendations regarding critical Performing daily ongoing (A&A) Assessment and Authorization projects in support of client infrastructure, network security operations and Continuous Monitoring processes. Working knowledge of Categorizing Information Systems (using FIPS 199 as a guide), NIST Risk Management Framework, FIPS and FISMA Act. Review and update some of the system categorization using FIPS 199, Initial Risk Assessment, E-authentication, PTA, PIA, SAR, SSP, SAP& POA&M. Participate in ST&E Kick-off Meeting and populate the Requirements Traceability Matrix (RTM) per NIST SP 800-53A. Conduct a Privacy Threshold Analysis (PTA), and Privacy Impact Analysis (PIA) by working closely with the ISSOs and the System Owner. Develop and maintain Plan of Action and Milestones (POA&MS) of all accepted risks upon completion of system (C&A). Coordinate, participate and attend weekly ISSO forums for security advice and updates. Provide continuous monitoring support for control systems in accordance to FISMA guidelines and conduct FISMA-based security risk assessments. Develop and conduct ST&E (Security Test and Evaluation), Security Assessment plan (SAP) according to NIST SP 800-53A. Worked with business process owners to ensure timely identification and remediation of jointly owned risk related issues and action plans (POA&M). Communicate effectively through written and verbal means to co-workers, subordinates and senior leadership. Perform Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), E-Authentication with business owners and selected stakeholders. Assist with review of policy, security alerts, guidance, regulations and technical advances in IT Security Management. Contribute to initiating FISMA metrics such as Annual

Testing, POA&M Management, and Program Management. Review audit logs and provide documentation guidelines to business process owners and management. Determine security controls effectiveness (i.e., controls implemented correctly, operating as intended, and meeting security requirements). IT Security Analyst Swift Systems Inc March 2012 to May 2014 Duties included: Provided input to management on appropriate FIPS 199 impact level designations and selecting appropriate security controls. Oversee the preparation of Assessment and Authorization (A&A) packages for submission to the Authorizing Official (AO) for an Authorization to Operate (ATO). Performed evaluation of policies, procedures, and analyzed security scan results, in order to address controls that were deemed insufficient during Assessment and Authorization (A&A). Provided audit briefings to agency and Information Systems Security Officer's (ISSO), to assist in the preparation of independent audit assessments with the agency's goal of improving their operational effectiveness and ensuring that all findings are documented as Plan of Action & Milestones within their Trusted Agent FISMA (TAF) tool. Authentication with business owners and Performed Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), E-d selected stakeholders. Monitored controls post authorization to ensure continuous compliance in accordance with FISMA guidelines. Generated, reviewed and updated System Security Plans (SSP) against NIST 800-18 and NIST 800 53 requirements. Performed Information Systems Security Audits and Certification and Accreditation (C&A) Test in compliance with the NIST 800 Series Standard. Documented and reviewed System Security Plan (SSP), Security Assessment Report (SAR), Security Plan of Action and Milestones (POA&M), 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. Documented and finalized Security Assessment Report (SAR) and communicate a consolidated risk management activities and deliverables calendar. Performed Enterprise Architecture for network discovery and provided a gap analysis. Reviewed and ensured Privacy Impact Assessment (PIA) document after a positive PTA is created. Performed specific quality control for packages validation on the SP, RA, RTM, PIA, SORN, E-authentication assessment and FIPS-199

categorization. Education Bachelors of Science in Business in Business/ Information Systems University of Phoenix May 2011 Associates in Visual Communications in Visual Communications Gibbs College - Vienna, VA May 2003 Skills Federal Information Security Management Act (3 years), FISMA (3 years), Nessus. (2 years), NIST (3 years), Security (3 years), Information Security, It Security Additional Information ? More than 5 years of professional experience in Risk Management Framework (RMF) Processes and FISMA. ? Experience in the development of System Security Plans (SSP), Security Assessment Report, Contingency Plans, and Incident Response Plans. ? Experience in Federal Information Processing Standards, Security Assessment Plan (SAP), Plan of Action & Milestone (POA&M), Risk Assessment ? Sound understanding and experience with NIST Risk Management Framework (RMF) process. ? Experience working with NIST SP 800-53 rev 4. ? Experience in assessment of security controls using NIST SP ? Good communication and writing skills. Technical Skills: - IT SECURITY, FISMA, NIST SP 800-18, [ ] [ ] FIPS 199 & 200. -Vulnerability Scanning Tools: NESSUS, SPLUNK and APP Detective.

Name: Christopher Anderson

Email: garciarichard@example.org

Phone: +1-260-547-8106