Information Security Analyst Information Security Analyst Information Security Analyst - Inova Loudoun Hospital Leesburg, VA Exceptional leader talented at data management, security analysis and consultant. Technically-savvy with outstanding relationship building, training and presentation skills. Seeking an Infomation System Auditor or Information Assurance position in a growth oriented organization with focus on FISMA, Sarbanes-Oxley 404, System Security Monitoring, Risk Assessments, Audit Engagements, Testing Information Technology Controls and Developing Security Policies, Procedures and Guidelines. Work Experience Information Security Analyst Inova Loudoun Hospital - Leesburg, VA November 2015 to Present Develop, review and update Information Security System Policies, System Security Plans (SSP), and Security baselines in accordance with NIST, FISMA, OMB, NIST SP 800-18 and industry best security practices. Develop and update System Security Plan (SSP), Privacy Impact Analysis (PIA), System Security Test and Evaluation (ST&E) and the Plan Of Actions and Milestones (POA&M). Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60. Developed policy and procedural controls relating to Management, Operational and Technical Controls for the Organization. Conduct Security Control Assessment on General Support Systems (GSS), Major Applications and Systems to ensure that such Information Systems are operating within strong security posture. Update IT security policies, procedures, standards, and guidelines according to department and federal requirements. Reviewed and updated some of the system categorization using FIPS 199. Carried continuous monitoring after authorization (ATO) to ensure continuous compliance with the security requirements. Put together Authorization Packages (SSP, POA&M and SAR) for Information systems to the Authorization Officer. Develop Security Assessment Plan (SAP) to initiate Security Assessment for low, moderate and high control information systems. Managed firewall, network monitoring and server monitoring both on- and off-site. Proposed technical feasibility solutions for new functional designs and suggested options for performance improvement of technical objects. Provided methodologies for object-oriented software development and efficient database design. Designed and implemented new server standards for core business services. I.T AUDITOR/COMPLIANCE OFFICER Ericson Retirement Community Ashby Ponds - Ashburn, VA

March 2014 to Present Provided technical auditing duties as liaison between IT and Internal Auditing Department. Planned, executed and lead security audits across the organization related to Sox, PCI, HIPAA and other compliance initiatives. Inspected and evaluated financial and information systems, management procedures and security controls. Evaluated the efficiency, effectiveness and compliance of operation processes with corporate security policies and related government regulations. Develop and administer risk-focused exams for IT systems. Reviewed and interviewed personnel to establish security risks and complications. Executed and properly documented the audit process on a variety of computing environments and computer applications. Assessed the exposures resulting from ineffective or missing control practices. Accurately interpreted audit results against defined criteria. Weighed the relevancy, accuracy and perspective of conclusions against audit evidence. Provided a written and verbal report of audit findings. IT SECURITY ANALYST BANK OF AMERICA - Reston, VA September 2013 to March 2014 Performed analysis on security incidents that is required to learn valuable lesson about attack and implement changes proactively based on knowledge learned. Monitored a worldwide network of for cyber security events and anomalies using tools such as Site protector, Splunk and Net witness. Developed, coordinated, implemented and maintained standards and procedures to protect the security and integrity of information systems and data. Experienced in computer security technologies such as: IDS/IPS, port and vulnerability scanners, and network detection used in performance of daily activities and to perform assessments and audits. Generated security documentations including: security assessment reports; system security plans; contingency plans; and disaster recovery plans. Research and maintain knowledge regarding information security issues, solutions and potential implications. Responsible for implementing and maintaining a continuous process improvement work environment while executing security risk assessments in accordance with industry standards and best practices. IT COMPLIANCE ANALYST Verizon Wireless - Ashburn, VA January 2011 to September 2013 Analyzed and updated System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Analysis (PIA), System Security Test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M). Assisted System Owners

and ISSO in preparing Certification and Accreditation package for IT systems, making sure that management, operational and technical security controls adhere to a formal and well established security requirement authorized by NIST SP 800-53 R4. Designated systems and categorized its C.I.A using FIPS 199 and NIST SP 800-60. Performed vulnerability Assessment and make sure that risks are assessed; evaluated and proper actions are taken to limit their impact on the information and information systems. Created standard templates for required security assessment and authorization documents including risk assessments, security plans, security assessment plans and reports, contingency plans and security authorization packages. Conducted IT controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard. Education B.S in Health Promotion Liberty University - Lynchburg, VA May 2012 Skills SECURITY (7 years), NIST (4 years), LIAISON (3 years), RISK ASSESSMENT (2 years), FEDERAL INFORMATION SECURITY MANAGEMENT ACT (2 years) Additional Information Skills Certification and Accreditation Compliance Testing Risk Assessment Security Assessment and Authorization (SA&A) Contingency Planning Planning and Procedures NIST SP 800-53 NIST SP 800-53A NIST SP 800-37 FIPS FISMA FISCAM and GRC.SOFTWARE/PLATFORM Excel /ARTIFACTS:Microsoft Word Access Power Point SharePoint Visio Linux Windows SDLC SQL SORN FIPS 199 PTA E-Authentication RA PIA CP SSP ST&E CIPT POAM SAR Retina Scan ATO Nessus Vulnerability Scanner.Project Risk Vision management Team liaison Self-motivated Strong verbal communication Conflict resolution Powerful negotiator Extremely organized Team leadership Data management Process implementation Staff development

Name: Jonathan Le

Email: hickmanjohn@example.org

Phone: 522-611-9485