

Information Security Compliance Analyst Information Security Compliance Analyst Information Security Compliance Analyst - Bureau of Labor Statistics Burtonsville, MD Authorized to work in the US for any employer Work Experience Information Security Compliance Analyst Bureau of Labor Statistics - Washington, DC December 2014 to Present Advise customer on systems recertification and accreditation procedure and best practices. Advise customer on Scanning Windows systems in their preparation and development of actions associated with security Certification and Accreditation package (SA&A) to achieve: an Authority to Operate (ATO) ? Review and create POA&M based on customer provided scans and artifacts ? Develop, review and update Information Security System Policies, System Security Plans(SSP) and Risk Assessment Report in accordance with NIST RMF: OMB A-130 Appendix III ? Update IT security policies, procedures, standards, and guidelines according to SP 800-53 Rev 4 ? Establish schedules and deadlines for assessment activities ? Hold kick-off and weekly meetings with system owners prior to assessment engagements and weekly activities relating to CSAM (IAES) ? Collect, review and analyze audit logs for anomalies ? Prepare and submit Security Assessment Plan (SAP) to ISO for approval ? Monitor controls post-authorization to ensure continuous compliance with security requirements - On Going Authorization ? Manage vulnerabilities using Nessus vulnerability scanners to detect potential risks on a single and multiple assets across the Enterprise Network ? Create reports detailing identified vulnerabilities and the steps to remediate them ? Assist the System Owners in preparing Certification and Accreditation package for the Company's 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. ? Work with the Information System Security Officer and other Security analysts ensuring compliance with all security requirements and updates ? Provided support for implementing and following the Federal Information policies and guidelines throughout the whole Certification and Accreditation process for securing clients information system.(NIST SP 800 series) ? Ensure all users of the system are aware of their security responsibilities in case an incident or vulnerability is discovered. ? Develop Risk Assessment Reports that identify threats and vulnerabilities; and they also evaluate the likelihood that the

vulnerabilities can be exploited. I assessed the impact associated with these threats and vulnerabilities and identified the overall risk ? Conduct Walkthroughs, Test plans, Test results and develop remediation plans for each area of testing ? Work with the IT team to gather evidence, develop Test Plans, Testing Procedures and document test results ? Assist the system owner to create the business Impact Analysis (BIA) document which formed part of the contingency plan and I also assisted in reviewing and updating it Information Security Analyst Equal Employment Opportunity Commission - Washington, DC November 2012 to November 2014 Nov 2012 to Nov 2014 ? Supported client's information security governance, risk and compliance activities to align with the NIST Risk Management Framework (RMF) ? Assisted in communicating and facilitating the requirements for security risk assessments for both custom developed and third-party applications within the Freddie Mac Infrastructure. ? Developed security A&A artifacts, to include but not limited to, sensitivity assessments, SSPs, and ATO package according to SP 800 - 37 ? Assisted in identifying and communicating application control deficiencies and the associated risks ? Assisted with the development and maintenance of plan of action and milestones (POA&Ms) to document security vulnerabilities and mitigation strategies. ? Monitored controls post-authorization to ensure continuous compliance with security requirements ? Provided expertise and assistance in the development of continuous monitoring programs and plans ? Scheduled kick off meetings with stakeholder to help identify assessment scope, system boundary, information types (Information process, store or transmitted by the Information Systems), and eventual categorize Information System accordingly ? Analyzed, review and update System Security Plan (SSP), Risk Assessment Report, Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E), and the Plan of Actions and Milestones (POA&M) ? Designated System and categorize its CIA using FIPS 199 and NIST SP 800-60 ? Conducted Self-Annual Assessment and test Security Controls (NIST SP 800-53A) ? Assisted System Owners and ISSO in preparing certification and accreditation package for companies IT Systems, making sure that management, operational and technical security control adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4 ? Reviewed vulnerability assessment makes sure that the risks are assessed; evaluated

and proper actions have been taken to limit their impact on the Information and Information Systems

? Created standard template for required security assessment and authorization document, including risk assessments, documents, including Risk assessments, security plans, security assessment plans and report contingency plans, and security authorization packages ? Additional responsibilities included; assurance of vulnerability mitigation, training on C&A tools, supporting systems test and evaluation (ST&E), efforts and other support to the IS Security Office IT Technical Specialist Freddie Mac - Washington, DC June 2010 to October 2012 Performed technical hardware and software support and technical functions for desktop, notebook, printers (including thermal), hand held computers, and server systems ? Acted as a liaison between the Help Desk and Infrastructure teams ? Tested and performed hardware and software installations for end-user devices ? Troubleshoot and research problems for users ? Recorded and maintained inventory of hardware and software ? Identified, researched, and resolved technical problems ? Recommended systems modifications to reduce user problem ? Provided software updates and upgrades to workstations and other equipment, such as anti-virus, Microsoft Office, and other workstation software Education Business Administration Strayer University - Takoma Park, MD May 2010 Skills NIST (6 years), Security (6 years), System Security (6 years), audit (6 years) Additional Information Core Skills ? Security Life Cycle and Vulnerability Management, using FISMA and applicable NIST standards. ? Perform Certification and Accreditation documentation in compliance with company standards ? Develop, review and evaluate System Security Plan based on NIST Special Publications ? Develop and conduct ST&E ( Security Test and Evaluation) according to NIST SP 800-53A and NIST SP 800-53R4 ? Compile data to complete Residual Risk Report and to insert contents into the POA&M ? Collect, review and analyze audit logs for anomalies ? Ability to multi-task, work independently and as part of a team ? Strong analytical and quantitative skills ? Ability to communication clearly and effectively with technical and business stakeholders. ? Solid problem solving and analytical skills; able to quickly digest issue/problem encountered and recommend an appropriate solution ? Excellent verbal and written communication skills including the ability to author and present materials ranging from detailed technical specification to high level

presentations ? Demonstrate ability to envision and integrate various security technologies and controls into a cohesive architecture that sufficiently mitigates risk to the organization. ? Ability to identify deficiencies in accordance with OMB Circular A-123 Appendix A Technical skills Platform/Artifacts: FIPS 199, SORN, E-Authentication, PTA, PIA, RA, SSP, CP, ST&E, SAR, POA&M, ATO Software: MS Office (Word, Excel, PowerPoint, Access, Outlook), MS Project

Name: Jamie Mason

Email: kevinlee@example.com

Phone: 001-427-624-5833x32484