Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Department of Commerce Burtonsville, MD Diligent, result-driven and analytical IT security professional with 5+ years of broad experience in conducting risk assessment, Cyber/ IT auditing and compliance, system controls, system verification and validation testing techniques. Areas of expertise include NIST RMF, ISO, and, FedRamp, Cognizant of various industry standards pertaining to Federal and Commercial industries, resourceful, detail-oriented, and client focused, with a continuing passion for growth Years of Experience: 5 years of IT Security experience DHS Suitability Work Experience Cyber Security Analyst Department of Commerce - Suitland, MD March 2013 to Present Duties included: ? Working knowledge of NIST 800-53, NIST RMF, FIPS and FISMA ? FISMA Reports, Standard Operating Procedures (SOP) in accordance with ? Conduct the ST&E Kick-off Meeting and populate the Requirements Traceability Matrix (RTM) according to NIST SP 800-53A. ? Experience with NIST standard on cyber security and incident handling (800-63, 800-61) ? Analyze and update System Security Plan (SSP), Risk Assessment Report (RAR), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E), Security Assessment Report (SAR) and the Plan of Actions and Milestones (POA&M). ? Assist System Owners and ISSOs in preparing Assessment and Authorization packages for client IT systems, making sure that management, operational and technical security controls adhere to formal and well-established security requirements authorized by NIST SP 800-53 Rev 4. ? Initiate kick-off meetings to collect system information to assist in the categorization phase using FIPS 199 and NIST SP 800-60. ? Review and update Contingency Plan (CP) using NIST SP 80-34 guidelines. IT Security Analyst Smart Think LTD - Rockville, MD April 2010 to February 2013 Duties included: ? Worked with Certification and Accreditation team; performed risk assessment; updated System Security Plan (SSP), contingency plan (CP), Privacy Impact Assessment (PIA), and Plan of Actions and Milestones (POA&M). ? Performed data gathering techniques (e.g. questionnaires, interviews and document reviews) in preparation for assembling C&A/A&A packages ? Updated Plan of Action & Milestones (POA&M) and Risk Assessment based on findings assessed through monthly updates. IT Security Analyst Bank of America - Silver Spring, MD December 2008 to March 2010 Duties included: ? Managed internal IT

audit engagements including: system platform audits, PCI Compliance for the bank ? Readiness reviews, IT Risk Assessments, change management, and business process control assurance ? Managed security control assessments of Payment Systems for merchant boarding and settlement of funds. ? Collaborated with Information Technology and Operations areas to proactively assess security policy compliance and monitor risk ? Coordinated external 3rd party auditors, including PCI DSS, SAS 70, Record Retention, and Business Process Improvement reviews ? Performed investigations of internal fraud or presumptive fraud with a view to gathering evidence that could be presented in a court of law ? Coordinated and perform compliance audits in accordance to the information protection, data asset and threat provisions under the Gramm-Leach-Bliley and Sarbanes-Oxley Acts. ? Coordinate with Incident Response teams for post-event diagnosis, investigation and documentation. ? Evaluated and assess implementation of the disaster recovery/business continuity plan ? Provided effective project (audit) guidance and leadership to team members and management as it relates to data security and industry compliance Education Bachelor in Science University of Maryland - Salisbury, MD Associate in Science Montgomery College - Rockville, MD Skills NESSUS (Less than 1 year), SCANNING (Less than 1 year), SPLUNK (Less than 1 year) Additional Information ? Experienced in the development of System Security Plans (SSP), Contingency Plans, Disaster Recovery Plans, Incident Response Plans/Training, and Configuration Management Plans, System Security Checklists, Privacy Impact Assessments, POA&M, ? Familiar with VMware and other Virtual Machine Applications ? Experienced working with NIST SP 800-53 rev 3 and rev 4 ? Assisted in review of policy, security alerts, guidance, regulations and technical advances in IT Security Management ? Conducted continuous monitoring program using automated tools to maintain compliance. ? Conduct risk assessments regularly; ensured measures raised in assessments were implemented in accordance with risk profile, and root-causes of risks were fully addressed following NIST 800-30 and NIST 800-37. ? Perform Security Categorization (FIPS 199), review and ensure Privacy Impact Assessment (PIA) document after a positive PTA is created. ? Document and finalize Security Assessment Report (SAR) and communicate a consolidated risk management activities and

deliverables calendar. ? Coordinated external 3rd party auditors, including PCI DSS, SAS 70, Record Retention, and Business Process Improvement reviews Technical Skills: ? Vulnerability Scanning Tools: NESSUS, SPLUNK, and APP Detective.

Name: Cassidy Porter

Email: glewis@example.net

Phone: +1-389-271-0872x212