IT Security Specialist IT Security Specialist IT Security Specialist - DSA, McLane, VA Analytical IT security professional with 6+ years of extensive experience in conducting IT security assessment and compliance, system controls, system verification and validation testing techniques. Extensive background in leading compliance projects. Comprehensive knowledge on regulatory compliance for implementing and communicating Federal Information Security Modernization Act (FISMA) compliance for the Federal government as well as several internationally recognized commercial frameworks. Work Experience IT Security Specialist DSA, McLane, VA August 2018 to Present Conduct Pre-Assessment phase for ATO packages to prepare clients for third party assessment. ? Develop Security Impact Analysis for client systems. ? Create & track POA&Ms for clients using findings to develop milestones/corrective actions for successful remediation. ? Input & manage data within Xacta system. ? Conduct meetings with the client to discuss client's material weaknesses identified in an audit to gain an understanding and develop mitigation strategies for the findings. ? Conduct GAP analysis. ? Responsible for developing continuing education trainings for colleagues. ? Update artifacts (i.e. System Security Plans, Contingency Plans, etc.) with appropriate information. ? Review and update implementation statements for clients. ? Review audit logs to track trends and/or vulnerabilities IT Security Analyst ICF - Fairfax, VA February 2016 to August 2018 Assess systems using NIST 800 Risk Management Framework. ? Categorize information systems into low, moderate, or high- security impact using FIPS 199 as a guide. ? Create Security Assessment Plan's (SAP) to document assessment schedules. 301.273.8509 | deja.matthews27@gmail.com ? Review and update the Contingency Plan (CP) annually as part of the system security documents, following NIST 800-34 Federal CP Guide. ? Review configuration management (CM) controls as part of security assessments. ? Responsible for POA&M Management/Continuous Monitoring and milestone follow through by coordinating with system stakeholders'/control owners (e.g., Systems Admins). ? Open POA&M items, track, and facilitate POA&M closer. ? Examine remedy tickets, activity logs, user access lists and email correspondence for new users to verify that usernames and passwords were not being provided at the same time. ? Responsible for Internal Assessments of NIST SP 800 Series controls such as Remote Access Control (AC) for various Information

Systems. ? Co-developed Assessment/Audit plans using control baselines documented in system security plans as a starting point, meeting with system stakeholders, documenting control implementation statements, and assessment. Information Assurance Compliance Analyst SIE Consulting Group - Arlington, VA January 2013 to January 2016 Provided expertise in vulnerability management processes and network vulnerability scanning using Tenable Security Center and/or Nessus. ? Responsible for the development of system security control test plan and in-depth security assessments of information systems. ? Developed security baseline controls and test plans used to assess implemented security controls. ? Conducted interviews, test and examine organizational processes and policies for FISMA compliance. ? Assessed system design and security posture as well as advise information security compliance with FISMA and NIST SP 800-53 rev 4 controls. ? Created Security Assessment Reports (SAR) identifying the results of the assessment along with Plan of Action and Milestone (POA&M). ? Recommended and performed maintenance and system configurations in order to protect systems from emerging cyber threats. ? Participated in CDM meetings to discuss vulnerabilities and potential remediation actions with system and application owners. ? Developed System Security Plans (SSP) to provide an overview of system security requirements and describe the controls in place or planned by information system owners to meet those requirements ? Conducted follow up meetings to assist ISSOs, System Owners, and Authorizing Officials to close remediated POA&M items. ? Conducted trending and analysis of monthly results to identify high-risk vulnerabilities impacting the network and ensure proper security posture from a vulnerability management standpoint. ? Documented findings and severity levels of non-compliance in formalized reporting, written and oral briefs, etc. ? Assisted with the development of processes and procedures to improve incident response times, analysis of incident, and overall SOC functions. Education Masters of Science in Project Management Morgan State University - Baltimore, MD Skills Nist, Cyber Security, Information Security, Siem

Name: Kenneth Cunningham

Email: tranjennifer@example.com

Phone: 4225947807