SECURITY CONTROL ASSESSOR, URGE SECURITY CONTROL ASSESSOR, URGE Work Experience SECURITY CONTROL ASSESSOR, URGE URGE - Washington, DC May 2018 to Present   Utilized NIST 800-53A to assess assigned Financial systems.   Conduct comprehensive technical evaluations of information system designs, focusing on information security according to NIST Risk Management Framework (RMF).   Assisted team in documenting and reporting vulnerabilities by utilizing Nessus.   Conducts periodic assessments of facilities to ensure compliance with security requirements.   Assessed technical security controls and provided implementation response to meet requirements. INFORMATION SECURITY SPECIALIST TECH IMPACT - Washington, DC March 2016 to May 2018 WASHINGTON D.C.)   INFORMATION SECURITY SPECIALIST, TECH IMPACT   Performed Assessment & Authorization (A&A) activities on assigned systems by reviewing system architecture, key artifacts, interviewing stakeholders and documenting results in alignment with NIST 800 53/53a.   Analyzed Nessus vulnerabilities to evaluate and document the security posture of technical controls.   Developed Security Authorization Packages (SAP) and present system findings to all stakeholders for Authorization to Operate (ATO) recommendations.   Provide subject matter expertise to establish policies, procedures, processes, and role-based training in support of the agencies RMF program. INFORMATION SECURITY ASSESSOR, INOVA FAIRFAX HOSPITAL FAIRFAX, V.A January 2015 to March 2016   Reviewed System Security Plans, Contingency Plans, and other artifacts to gauge the effectiveness of control implementation.   Created Security Authorization Packages, including Risk Assessment Reports, Security Assessment Reports, and other documents for stakeholders.   Engaged with Stakeholders to conduct systems walkthrough, kickoffs, and closing meetings during the assessment process.   Presented system findings to the Stakeholders and provided recommendations for each system.   Assisted the SOC team in documenting and reporting vulnerabilities by utilizing Splunk.   Experienced in reviewing and interpreting Nessus Vulnerability and Compliance Scans. JUNIOR SECURITY ANALYST SONA NETWORK SUBCONTRACTING TO BAH - Washington, DC October 2013 to December 2014   Experienced with conducting hands-on security control testing, analyzing results, documenting risk, and recommending

countermeasures. Developed risk assessment reports based on a review of the security plan and interviews with customers to assess systems against information policies. Continued working knowledge of NIST documents and applied them where applicable. Participated in weekly status meetings to ensure POA&M's were being addressed in a timely manner. IT SUPPORT VENABLE LLP - Washington, DC May 2013 to October 2013 Managed access to permissions and privileges for all databases. Responded to escalated request in a timely manner by utilizing BMC Remedy. Lead the deployment of Windows XP to Windows 7 for the entire firm. Delivered guidance and support to partners on all systems. IT INTERN SIDLEY AUSTIN LLP - Washington, DC September 2012 to May 2013 Troubleshoot LAN/WAN issues, worked with ISP when necessary. Managed Active Directory accounts and permissions for Utilized a range of diagnostic tools to accurately assess and correct technical issues. Managed installations of software and the modification and repair of hardware systems. 2 Education PARTNER OF NOTHER VIRGINIA COMMUNITY COLLEGE July 2013 Skills Nessus. (4 years), NIST (4 years), Risk Management (1 year), SECURITY (5 years), Splunk. (1 year) Additional Information PROFESSIONAL SKILLS Security+ Certification Risk Management Framework FIPS 199 FIPS 200 Patch/ Security Management Plan of Action and Milestones (POA&M) Authorization to Operate (ATO) NIST 800-53 NIST 800-53A Microsoft Office 2018 Splunk Nessus Scanning Tool Active Directory Windows Server 2008, 2012

Name: Charles Owens

Email: dawsonandrew@example.net

Phone: 974-730-6418