Cybersecurity analyst. Cybersecurity analyst. Cybersecurity analyst - Aspect Security, Inc Baltimore, MD FIPS 199, FIPS 200, NIST 800-53 Rev4, NIST 800-30, NIST 800-37, NIST 800-39 Risk Management Framework NIST 800-53 Nessus scan analysis. Splunk Authorized to work in the US for any employer Work Experience Cybersecurity analyst. Aspect Security, Inc - Columbia, MD March 2017 to Present Perform Security Assessments on assigned systems using the Risk Management Framework (RMF) guidelines. Reviewed technical and operational security controls and provide implementation responses to meet requirements Meet with client to discuss findings and process of remediation Review provided or requested Artifacts and Plan of Action & Milestones (POAMs) to determine if controls are implemented correctly. Use Nessus to run scans on operating systems. Utilizes NIST 800-53A and NIST 800- 53 rev-4 to review implemented controls and enter information into the Requirements Traceability Matrix (RTM) and findings into the Security Assessment Report (SAR). Collaborate with other team members and system owners/ technical managers to schedule and conduct Kick-off meetings and interviews to discuss findings. Provide weekly status reports. Uses High-Watermark from scans as a reference to categorize the risk level of the system. Cybersecurity analyst ZeroFOX - Baltimore, MD June 2015 to March 2017 Assisted in conducting cloud system assessments Helped in updating IT security policies, procedures, standards and guidelines according to department and federal requirements Support Cyber Security analyst in conducting Vulnerability Management, Security Engineering, Certification and Accreditation, and Computer Network Defense. Perform risk assessments, update and review System Security Plans (SSP) using NIST 800-18 (Guide for Developing Security Plans for federal information systems) Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Perform vulnerabilities scan and monitor continuously using NIST 800-137 as a guide with the aid of Nessus Entry level/Junior IT Security Analyst Crest consulting group - Rockville, MD November 2013 to June 2015 Developed, reviewed and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices. Performed vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple asset across the enterprise network.

Updated IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). Account management/ IT security analyst intern Internal Revenue Service - Baltimore, MD November 2011 to November 2013 Worked with network security (network administrator policies and procedures, firewalls, etc. Policy writing and understanding of NIST publication Interned as an IT security analyst as well as worked with different SIEM tools Managed customer accounts Managed incoming customer registration Worked primarily with taxpayers and their representatives through telephone and face-to-face contact. Provided Authoritative tax law assistance, and took action where needed to resolve tax issues, often involving delinquent situations. Actions may have included analyzing the taxpayer's ability to pay, initiating liens, and negotiating installment agreement payments. Maintained and operated the electronic taxpayer records and billing systems Education Bachelor's Skills Excel Additional Information FIPS 199, FIPS 200, NIST 800-53 Rev4, NIST 800-30, NIST 800-37, NIST 800-39 Risk Management Framework NIST 800-53 Nessus scan analysis Splunk

Name: Sherry Morales

Email: pbeasley@example.com

Phone: +1-724-628-0909