Cybersecurity analyst Cybersecurity analyst Cybersecurity analyst - CSC Alexandria, VA Work Experience Cybersecurity analyst CSC - Baltimore, MD July 2015 to Present Perform Security Assessments on assigned systems using the Risk Management Framework (RMF) guidelines. Reviewed technical security controls and provide implementation responses to meet requirements Document findings in the SAR 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 April 2013 to July 2015 Assisted in conducting cloud system assessments Worked in a SOC environment, where I assisted in documenting and reporting vulnerabilities (Tier 1). 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 Responsible for conducting analysis of security incidents. Perform investigations of unauthorized disclosure of PII. Responsible for reporting findings and provide status to senior leadership. Perform escalations to Regional Computer Emergency Response Team (RCERT) when required. Perform vulnerabilities scan and monitor continuously using NIST 800-137 as a guide with the aid of Nessus IT Security Analyst Argus Technology Associates Inc - Baltimore, MD March 2012 to April 2013 Assisted in conducting cloud system assessments Worked in a SOC environment, where I assisted in documenting and reporting vulnerabilities (Tier 1). Helped in updating IT security policies, procedures, standards and guidelines according to department and federal requirements Worked with client in safeguarding CUIs by performing the necessary assessments which primarily deals with 14 control families. 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 Information Assurance Vulnerability Management (IAVM): Responsible for acknowledging and tracking IAVM notices and creating Plan of Actions and Milestones (POAMs) for review and approval by the Authorizing Official (AO) formerly known as Designated Approving Authority (DAA). Management Plans (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation. COOP/Disaster Recovery (DR) Security Engineering Responsible for conducting analysis of security incidents. Perform investigations of unauthorized disclosure of PII. Responsible for reporting findings and provide status to senior leadership. Perform escalations to Regional Computer Emergency Response Team (RCERT) when required. 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 January 2009 to March 2012 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. Performed risk assessments, help review and update, Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Management Plans (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation. (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). Education Ph.D. in Information Assurance and Cyber Security

Capella University Present Master of Science in Information Assurance in Information Assurance Strayer University Bachelor of Science in Criminal Justice Administration in Criminal Justice Administration Westwood College Skills Excel Certifications/Licenses CompTIA Security+ May 2018 to May 2021 Additional Information FIPS 199, FIPS 200, NIST 800-53 Rev4, NIST 800-30, NIST 800-37, NIST 800-39, E-Authentication, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), Risk Assessment (RA), SSP, Contingency plans, ST&E, SAR, Plans of Action and Milestones (POA&M), Authorization to Operate (ATO) Letter, MS Office, Visio, SharePoint, Access, PeopleSoft, Nessus Vulnerability Scanning Tool, WebInspect, Splunk, DbProtect IT CERTIFICATION: CompTIA Security +

Name: Charles Chapman

Email: hahndana@example.net

Phone: 354-486-4933