Information Security Team Lead Information Security Team Lead Information Security Team Lead - Cybersecurity Division Falls Church, VA Work Experience Information Security Team Lead Cybersecurity Division July 2019 to Present Responsible for managing team of 15 analyst on day to day activities and projects. Responsible for tracking 35 systems in the RMF process. Responsible for submitting weekly and monthly status reports to Government management. Responsible for creating and updating Policy and Procedures, System Security Plan, Contingency Plan, Contingency Plan Test, Risk Assessment Report, System Categorization, Privacy Threshold Assessment, Privacy Impact Analysis, Security Assessment Report, Security Impact Analysis, and the Security Risk Traceability Matrix. Create detailed remediation reports and recommendations for compliance and security improvements across systems based on constant changing threats. Creating, updating, and maintaining the associated Plan of Action and Milestones (POAM) via CSAM. Provide verbal status reports and written reports, conduct weekly meetings, and attain to the needs of all clients and vendors. Up to date with the latest FISMA, NIST standards, and RMF. Familiar with AWS Cloud Security Responsible for managing POAM entry into CA Agile Central for tracking purposes. Cyber Security Analyst Team Lead SAIC March 2019 to July 2019 Responsible for managing team of 5 analysts on day to day activities and projects. Responsible for managing 25 systems. Provided weekly updates to Government managers regarding statuses of all 25 systems. Worked directly with System PMs, and technical leads to remediate all outstanding POA&Ms. Worked with team to provide milestones for all outstanding POA&Ms. Created SharePoint pages to help track RMF ATO process & POA&M Remediation. Analyzed scans via Vulnerator and provided vulnerability reports to all systems via VRAM. Verified all STIGs and scans were tested according to latest Navy Testing Guidance. Updated all system documentation and POA&Ms via eMASS. Worked with all systems to help transition ATO process from DIACAP to RMF. Responsible for initiating RMF workflows within eMASS for tracking purposes during ATO process. Scheduled and lead bi-weekly meetings with internal team and Navy AO representatives. Seidcon - Contracted to U.S. Patent and Trade Office Information Security Analyst Cybersecurity Division July 2017 to March 2019 Responsible for creating and

updating Policy and Procedures, System Security Plan, Contingency Plan, Contingency Plan Test, Risk Assessment Report, System Categorization, Privacy Threshold Assessment, Privacy Impact Analysis, Security Assessment Report, Security Impact Analysis, and the Security Risk Traceability Matrix. Recommend changes to the current strategy on external threat factors and known good cyber protection initiatives. Create detailed remediation reports and recommendations for compliance and security improvements across systems based on constant changing threats. Perform Vulnerability and Compliance scans via Nessus and WebInspect whilst mapping each finding to the NIST SP 800-53 Revision 4. Creating, updating, and maintaining the associated Plan of Action and Milestones (POAM) via CSAM. Provide verbal status reports and written reports, conduct weekly meetings, and attain to the needs of all clients and vendors. Up to date with the latest FISMA, NIST standards, and RMF. Familiar with AWS Cloud Security Responsible for inputting POAMs into CA Agile Central for tracking purposes. Security Engineer Phacil Inc January 2014 to June 2017 Develop and implement documentation outlining system operating environment to include hardware configuration, software, and type of information processed. Manage Plan of Action & Milestones (POA&Ms) Assisted in vulnerability and compliance remediation by analyzing quarterly scan results. Provide IT security consulting to System Owners in regards to the security documents that are included in the Security Authorization package. Utilize Trusted Agent FISMA (TAF) to input POA&Ms and worked with ISSOs to ensure all POA&Ms were mitigated by the deadline assigned. Implement the latest revisions of NIST SP 800-53 Rev. 4, and NIST SP 800-37 Rev. 1. Responsible for completing a reauthorization on a Major Application and successfully received the Authorization to Operate (ATO). Create and complete all the documents that are applied in the Security Authorization package. Perform and complete the Contingency Plan Testing (CPT), and ensured all points-of-contact were aware of their duties and responsibilities. Serve as a team lead in a liaison with government clients, guaranteeing a great client/contractor rapport. Set up meetings and conference calls with all appropriate Points-of-Contact. Serve as lead analyst on multiple projects and packages, worked as a team with other security analysts and initiated peer review sessions on SA&A documents. Complete

System Security Plan (SSP), Information Technology Contingency Plan (CP), Disaster Recovery Plan (DRP), Risk Assessment (RA), Rules of Behavior, Privacy Impact Assessment (PIA), Privacy Threshold Assessment (PTA), and Plan of Action and Milestones (POA&M) Report. Conduct kick-off meetings with all stakeholders when required. Keep a professional relationship with the ISO and provided regular updates. Compass Real Estate Washington, DC IT Security Associate February 2013 to November 2014 Managed all aspects of cyber security documentation for all internal systems. Briefed senior management on all aspects of security. Developed required security assessment documentations using the Risk Management Framework (RMF). Identified security findings from the vulnerability reports, mapped each finding to a NIST control and tracked findings as needed. Reviewed and continuously monitored implemented security controls. Created and maintained security checklists, templates and other tools. Briefed new employees on security policies and procedures Responsible for conducting and maintaining up to date security trainings for all employees and vendors. Education Bachelors of Arts in Business Administration George Mason University - Fairfax, VA December 2012 to Present Skills Cisco, Database, Voip, Drivers, Public relations Additional Information SKILLS/PROFICIENCIES: Expert knowledge of Windows 7/8/10 Installation of printer and peripheral drivers Intermediate knowledge of Cisco VoIP, and ability to configure VoIP systems Excellent interpersonal communication and social skills Strong public relations skills, with an excellent customer service/client focus Excellent conflict resolution skills between merchant and customer Microsoft Office Suite, Mac, Adobe Suite, Legal and non-legal research database skills Ability to adapt quickly to procedural and technological changes Familiar with network setup and troubleshooting

Name: Amber Walsh

Email: john02@example.com

Phone: 822-586-1334x495