IT Security Control Assessor IT Security Control Assessor IT Security Control Assessor - IC Security Systems Washington, DC IT security professional with 5+ years of extensive experience in conducting IT security assessment and compliance, system controls, system verification and validation testing techniques. 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. Areas of expertise include NIST RMF, and Fed-RAMP, etc. Cognizant of various industry standards pertaining to Federal and Commercial industries, resourceful, detail-oriented, and client focused, with a continuing passion for growth. Work Experience IT Security Control Assessor IC Security Systems - Washington, DC July 2017 to Present Conducted assessments of Federal client systems using RMF NIST SP 800-53 r3/r4 and NIST SP 800-53A r3/r4Special Publication guidelines. ? Assisted in develop Security Assessment Report (SAR) detailing the results of the assessment and created (POA&Ms) for each of the findings within the SAR. ? Conducted IT risk assessments to identify system risk, vulnerability and threats. ? Assessed system design and security posture as well as advising stakeholders on information security compliance consistent with FISMA and NIST SP 800-53 control requirements. ? Conducted 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. ? Provided mitigation strategies and recommendations to key stakeholders to enhance their security posture. ? Understanding of Federal Authorization process, in accordance with NIST SP 800-37 r1 and Fed-RAMP for cloud. ? Supported activities for Assessment and Authorization (A&A) of new systems, and Information Security Continuous Monitoring (ISCM), in compliance with NIST SP 800-53 controls within the Risk Management Framework (NIST SP 800-37). Cyber Security Analyst PingWind Inc - Washington, DC April 2014 to July 2017 Conduct security control assessments for new client systems based on NIST SP 800-53A Rev4 and in accordance with client policies and procedures. ? Assess an average of 5 projects a year using NIST 800 Risk Management Framework. ? Review systems categorization information utilizing FIPS 199, FIPS 200 and NIST SP 800- 60 as a guide. ? Create Security Assessment Plan's (SAP) to document

assessment schedules. ? Create and updated the following Security Assessment and Authorization (SA&A) artifacts: FIPS 199, SSP, RA, E-Authentication, ST&E, and Contingency Plan. ? Review and updated the Contingency Plan (CP) annually as part of the system security documents, following NIST-800-34 Federal CP Guide. ? Review configuration management (CM) plans and procedures as part of security assessments. ? Responsible for tasks related to the system security Assessment and Authorization (A&A) and follow the Government IT security policies and standards. ? Utilize Risk Management Framework process to enable successful approval to operate (ATO). ? Prepare recommendation reports that are made available to system owners to remediate identified vulnerabilities during the risk assessment process. IT Security Specialist Accenture LLC - Washington, DC February 2013 to April 2014 Provided expertise in vulnerability management processes and network vulnerability scanning using Tenable Security Center. ? 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, tested and examined 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. ? Performed and recommended maintenance and system configuration settings 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. ? Assisted Developling 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 and System Owners to close POA&M items. ? Assisted subscribers with vulnerability remediation, as necessary ? 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. IT Help Desk/Computer Specialist Flextronics - Somerset, NJ May 2012 to February 2014 Troubleshoot Microsoft products eg: MS Word, Excel and PowerPoint ? Removal of Malware, Adware and installed Anti-virus ? Provided support in hardware, software and

network problem identification and resolution ? Swapped out defective hardware and installed new CPU Monitors and printers. ? Developed and Maintained configurations for Network stations VGA, HDMI, DVI cables. Education Master's Degree in Cyber Security Management and Policy in Cyber Security Management and Policy University of Maryland University College - Upper Marlboro, MD November 2019 Bachelor of Science in Aviation Management and Air Traffic Control Systems Vaughn College of Aeronautics and Technology - Flushing, NY September 2013 Skills Siem, Nist (4 years), Information Security (3 years), Cyber Security (3 years) Certifications/Licenses Security+ December 2018 to Present Top Secret Clearance August 2018 to Present

Name: Joy Flynn

Email: christopherwolf@example.org

Phone: 505-372-2258x71869