IT Security Analyst/ Security Control Assessor IT Security Analyst/ Security Control Assessor IT Security Analyst/ Security Control Assessor - I-Way Networks, LLC Laurel, MD To continue my career as a successful Information Security Analyst in a major global organization within the Washington Dc, Maryland and Virginia (DMV) area. Work Experience IT Security Analyst/ Security Control Assessor I-Way Networks, LLC - Dumfries, VA July 2018 to Present Developed, reviewed and updated all security documentations required to obtain system ATO including providing support through the continuous monitoring phase Developed and submitted final Risk Assessments Report (RAR), Security Assessment Report (SAR), Plan of Action & Milestone (POA&M), System Security Plans (SSP), Security Test & Evaluation (ST&E), and reviewed copy of the System Security Plans (SSP) to the Office of the CIO for internal review and ATO approval Assessed system security controls using NIST SP 800-53A assessment procedures Reviewed FIP 199 to determine the rationale behind individual system information and information system categorizations Identified and evaluated the technical, management, and operational security controls in accordance with NIST SP 800-53 Rev 4 recommended controls and NIST SP 800-53A assessment procedures Reviewed System Security Plan (SSP) based NIST SP 800-18 guidelines Supported the agencies system owners with maintaining the security postures of their assigned information systems ensuring the protection of the confidentiality, integrity, and availability of information and information system Developed, reviewed, and completed the Assessment & Authorization packages such as: ? E-Authentication using NIST SP 800-63-1 ? Risk Assessment Report using SP 800-30 ? System Security Plan using SP 800-18 ? Conduct a Security Test & Evaluation ? Develop Security Assessment Report ? Develop Privacy Threshold Analysis Cybersecurity Specialist/RMF AVINEON LLC April 2017 to June 2018 Mc Clean, VA Conduct and execute certification & accreditation activities Complete and compile RMF phase II certification package Conduct security test and evaluation (ST&E) Provide analytical, technical, and policy expertise in the completion of the Assessment & Authorization (A&A) efforts in accordance with the National Institution of Standard Technologies (NIST) Risk Management Framework (RMF) Work with internal teams in observation remediation activities and remediation Participate in the categorization of the system using FIPS 199 and NIST SP 800-60 based on NIST impact requirements of Low, Moderate or High system Develop, review and update System Security Plans (SSP) based on NIST 800-53 rev4 requirements and organization standard Recommend security enhancements and purchases consistent with information security strategy and evolving threats Coordinate responses to information security control assessments and implement practices to optimize this process across organization Perform activities to help measure and monitor compliance with company policies and procedures Assist in the analysis and definition of security requirements Develop, deliver, maintain and monitor IT security policies, standards, and best practices Implement, integrate, maintain, report and monitor security and compliance risk management procedures Perform security, vulnerability and threat assessments and security incident management Assess system security controls to determine controls implementation and effectiveness and document findings in the assessment report Provide security life-cycle support (assessment, authorization, and continuous monitoring) for minor, major applications, and general support systems Develop security documentation (such as security plan, privacy analysis, E-authentication analysis, FIPS categorizations, and plans of action and milestones plan) required for authorization packages Create, track, and manage POA&Ms activities during remediation and continuous monitoring phases Participate in interagency meetings, workshops, conferences, and security awareness training IT Security Analyst JMAT System LLC - Greenbelt, MD January 2012 to April 2017 Developed, reviewed and updated all security documentations required to obtain system ATO including providing support through the continuous monitoring phase Reviewed FIP 199 to determine the rationale behind individual system information and information system categorizations Assessed system security controls using NIST SP 800-53A assessment procedures Identified and evaluated the technical, management, and operational security controls in accordance with NIST SP 800-53 Rev 4 recommended controls and NIST SP 800-53A assessment procedures Developed and submitted final Risk Assessments Report (RAR), Security Assessment Report (SAR), Plan of Action & Milestone (POA&M), System Security Plans (SSP), Security Test & Evaluation (ST&E), and reviewed copy of the System Security Plans (SSP) to the Office of the CIO for internal review and

ATO approval Reviewed System Security Plan (SSP) based NIST SP 800-18 guidelines Supported the agencies system owners with maintaining the security postures of their assigned information systems ensuring the protection of the confidentiality, integrity, and availability of information and information system Developed, reviewed, and completed the Assessment & Authorization packages. Network Security Specialist Synergy Tax and Financial - Cheverly, MD January 2009 to January 2012 First point of contact for all end-user connectivity issues Provided Weekly and Monthly performance and projects reports Monitored tools for better judgment and troubleshooting Involve in customer site survey Delivered comprehensive training sessions to over 120 clients on a monthly basis, on the use of various Microsoft applications Provided client support based on specific needs and business requirement Acted as a liaison between Network Team, Server Team and Desktop Support Team Remote into PCs and Servers using RDP to assist troubleshoot IPV4/Mac-Address conflicts Installed and configured companywide rollout of Cisco Catalyst 6509, 6504, 4500, 4900, 3750, 3560, 2960 switches including dual core implementation, VLAN configuration, 802.1q and ISL trunk configuration, use of link aggregation protocols (PAGP and LACP) and Spanning-Tree protocol Assisted in troubleshooting complex layer 1, 2, and 3 connectivity using Wireshark protocol analyzer and recommended solution for better performance Manage network IP access via Dynamic Host Configuration Protocol (DHCP) Layer 2 Switching such as: VLANs, PVLAN, VTP, STP (mst and pvst+), Trunking (802.1Q and ISL) Revised & maintained both port-level and Layer 3 network diagram using Visio Configured and managed redundant and high availability network design using HSRP, VRRP and GLBP Attend regular design and implementation meetings Resolved and troubleshoot end-users connectivity issue Education Bachelor's University of Maryland University College - Adelphi, MD May 2016 Skills SECURITY, NESSUS, NIST, MAPPING, RISK ASSESSMENT, Organizational Skills, Customer Service, Excel, Word Additional Information The ability to serve as an independent security analyst by ensuring technical security planning, testing, verification and risk analysis in accordance with applicable policies, laws, standards and regulations. Capable of defining, deploying and monitoring risk management, compliance, and information security programs while functioning as a primary point of contact. TECHNICAL SKILLS Security Test and Evaluation (ST&E) Plan of Action and Milestones (POA&Ms) Management System Security Plan (SSP) Security Assessment Report (SAR) Vulnerability Scan - WebInspect Vulnerability Scan - Nessus FIPS Publication 199 (Security Categorization) FIPS Publication 200 (Minimum Security Controls) NIST Special Publication 800-18 (Security Planning) NIST Special Publication 800-30 (Risk Assessment) NIST Special Publication 800-37 (System Risk Management Framework) NIST Special Publication 800-53 (Recommended Security Controls) NIST Special Publication 800-53A (Security Control Assessment) NIST Special Publication 800-59 (National Security Systems) NIST Special Publication 800-60 (Security Category Mapping)

Name: Michelle Rodriguez

Email: qpotter@example.com

Phone: 978-990-2108x4831