Senior IT Security Analyst Senior IT Security Analyst Senior IT Security Analyst - Diversified Protection Corporation Bladensburg, MD Has over 8 years of Information Technology (IT) Security Analyst experience supporting Federal Agencies. - Has a Bachelor of Science degree in Computer Science, an active CompTIA Security+ certification, and an active Secret clearance. - Is experienced in the cyber security disciplines of Continuous Monitoring, Incident Response, and Security Engineering. - Has a strong working knowledge of a full range of IT security principles, concepts, practices, products, services, and methods for evaluating information system risk and vulnerabilities. - To prevent, detect, analyze, and respond to security incidents, has operated and analyzed continuous monitoring tools (e.g., vulnerability and configuration scanners) SECURITY CLEARANCE Possesses an active Secret clearance Authorized to work in the US for any employer Work Experience Senior IT Security Analyst Diversified Protection Corporation - Arlington, VA January 2017 to Present Operate and analyze continuous monitoring tools (e.g., vulnerability and configuration scanners. Identify incident/breach trends and incorporate them into training activities to reduce the likelihood of future incidents/breaches. Conduct interviews with select personnel, document and evaluate business processes, and execute audit test programs to determine the adequacy and effectiveness of internal controls and compliance with regulations Analyze and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security Test and Evaluation (ST&E), and the Plan of Actions and Milestones (POA&M) Perform vulnerability scanning with the support of Nessus scanning tool to detect potential risks on single or multiple assets across the enterprise network. Conduct cloud system assessments, primarily with Amazon Web Services (AWS) by utilizing FedRAMP and NIST guidelines. Review and analyze results of Nessus Vulnerability and Compliance scans, WebInspect scans, and DbProtect scans for possible remediation. Develop, review, and update information system security policies and establish security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices. Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). Create standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages. Provide weekly status reports on ongoing tasks and deliverables. Prepare Security Assessment and Authorizations (SA&A) using NIST SP 800-53 rev4/FIPS 200 (Security Controls) and NIST SP 800-53A rev4 (Assessing Security Controls). Monitor controls post authorization to ensure constant compliance with established security requirements. Provide weekly Technical Security situational awareness briefs for management and appropriate stakeholders. Provide weekly risk assessments updates and Activity Status Reports. Review the FISMA related existing technical controls (i.e., security tools and sensors) to best protect organizational resources and data through improved response readiness, identification of threats and vulnerabilities, and regular reporting on all FISMA systems. Provide risk analysis for vulnerabilities and incidents indicating any special issues the vulnerability or incident may present to organizational systems and resources. Document incident response activities in event (timeline) and action logs to ensure efforts are well documented to support after action reporting requirement. Provide logs to become part of the formal event activity records. IT Security Analyst Trinity Corporation - Upper Marlboro, MD April 2014 to December 2016 Conducted Certification and Accreditation (C&A) on major applications following the Risk Management Framework (RMF) from Categorization through Continuous Monitoring using the various NIST Special Publications in order to meet Federal Information Security Management Act (FISMA) requirements. Developed SSPs, SARs, and POA&Ms which were presented to the Designated Approving Authorities (DAAs) to obtain the Authority to Operate (ATO). Conducted security assessments on major applications, updated POA&Ms with findings, and monitored for remediation deadlines. Provided weekly status reports on ongoing tasks and deliverables. Performed risk assessments to identify the risk level associated with findings. Reviewed artifacts regarding POA&Ms created by ISSO before closing. Assisted in updates of IT security policies, procedures, standards, and guidelines according to department and federal requirements. Helped with updating IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. Performed cloud and non-cloud system assessments. Supported cyber security analysis by conducting

Vulnerability Management, Security Engineering, Certification and Accreditation, and Computer Network Defense.   Monitored controls post authorization to ensure constant compliance with the security requirements.   Conducted annual assessments based on NIST SP 800-53A.   Documented findings within RTMs and SARs.   Reviewed and analyzed Nessus Vulnerability and Compliance scan results for remediation.   Monitored security tools and correlated reporting and other appropriate information sources to identify incidents, issues, threats, and vulnerabilities.   Provided daily anomaly and alert reporting from all reviewed tools and sensors.   Provided risk analysis for vulnerabilities and incidents indicating any special issues the vulnerability or incident may present to organizational systems and resources.   Provided Security and Privacy expertise to assist with research and response to security and privacy incidents. Junior IT Security Analyst Neway IT Solutions - Hyattsville, MD February 2011 to April 2014   Developed, reviewed, and updated Information System security policies and established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices.   Assisted in the update of IT security policies, procedures, standards, and guidelines per federal guidance and direction.   Conducted scans and identified vulnerabilities for remediation.   Installed, configured, and maintained client computing devices and ancillary hardware.   Assisted in the conduct of Assessments and reports on systems.   Performed risk assessments and reviewed and updated POA&Ms and Security Control Assessments.   Monitored controls to ensure ~~~~~~~~~ compliance with security requirements.   Performed risk assessments to identify the risk level associated with findings.   Contributed to the certification and accreditation (CA) process by performing network, system, and software vulnerability assessments via security tools and walk-downs.   Analyzed results to determine the level of risk posed, both internally and externally, and contacted system owners to propose recommendations to resolve or lower the security risk level or to mitigate or accept the risks associated with the vulnerabilities.   Assisted in the operation and ~~~~~~~~~ development of an Information Security Continuous Monitoring (ISCM) strategy that provides awareness of threats and vulnerabilities, visibility into organizational assets security readiness, and ensures the effective utilization of deployed security tools, sensors and controls.   Provided daily anomaly and alert reporting from all reviewed tools and sensors. Updated IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. Troubleshot hardware and software ? Worked with network security (network administrator policies and procedures, firewalls, etc.) ? Worked in a SOC environment in order to conduct scans and identify vulnerabilities. Education Bachelor's degree in Computer Science in Computer Science Strayer University 2003 Skills Cisco (Less than 1 year), Ethernet (Less than 1 year), Lan (Less than 1 year), Lan/wan (Less than 1 year), Linux (Less than 1 year), Microsoft sharepoint (Less than 1 year), Ms office (Less than 1 year), Networking (Less than 1 year), Nist (8 years), Novell (Less than 1 year), Peoplesoft (Less than 1 year), R2 (Less than 1 year), Red hat (Less than 1 year), Risk management (2 years), Sap (Less than 1 year), Sar (Less than 1 year), scanning (2 years), Sharepoint (Less than 1 year), Sms (Less than 1 year), Trading (2 years) Certifications/Licenses Comptia Security+ Additional Information TECHNICAL SKILLS OVERVIEW Platforms: ? Windows 7/8/8.1/10, Windows Server 2012 R2, Linux /Red Hat/, FIPS 199, FIPS 200, NIST 800-53 Rev4, NIST 800-30, NIST 800-37, NIST 800-39, SSP, ST&E, SAR, Plans of Action and Milestones (POA&M), Authorization to Operate (ATO) Letter, MS Office, SharePoint, Access, PeopleSoft, NessusVulnerability Scanning Tool, Splunk, Scan Analysis, Risk Management Framework (RMF), CSAM, XACTA Networking: ? LAN/WAN Administration, VPN, TCP/IP, Novell, SMS/SQL, 100BaseT Ethernet, SecureID, Cisco Routers & Switches.

Name: Cynthia Rodriguez

Email: jadelynn@example.org

Phone: (482)605-8050x52825