Senior IT Security Analyst Senior IT Security Analyst Senior IT Security Analyst - Intercon Security Services Glen Burnie, MD Authorized to work in the US for any employer Work Experience Senior IT Security Analyst Intercon Security Services - Washington, DC April 2018 to Present 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 Plan of Action and Milestones (POA&M), Security Control Assessments. (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). Monitored controls post authorization to ensure constant compliance with the security requirements. Conduct Annual Assessment based on NIST SP 800-53A Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs) Review and analyze Nessus Vulnerability and Compliance scans for possible remediation. Assess systems of varying scope and complexity and comprised of various technologies. 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. IT Security Analyst Allied Universal - Washington, DC July 2014 to April 2018 Supports the Security Assessments and Authorization process of the clients' systems as a technical Security Analyst 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. Helped with updating IT security policies, procedures, standards and guidelines per the respective department and federal requirements. Performed risk assessments to identify the risk level associated with the findings. (SA&A) Security Assessment and

Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). Monitored controls post authorization to ensure constant compliance with the security requirements. Reviewed artifacts regarding Plans of Action and Milestones (POA&M) created by ISSO before closing. Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). Review and analyze Nessus vulnerability and Compliance scans for possible remediation. Assess systems of varying scope and complexity and comprised of various technologies. Provide weekly status reports on ongoing tasks and deliverables. Junior IT Security Analyst XO communications L.L.C - Rockville, MD September 2009 to July 2014 Assisted in conducting cloud system assessments. 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 SSP (System Security Plans) using NIST 800-18 (Guide for Developing Security Plans for federal information systems), POA&M (Plans of Action and Milestones), 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. Education B.S in Computer Science University Of Maryland University College 2021 Skills Active Directory, HTML, access, Security, testing, Sharepoint, Cisco, Microsoft Office, training, SQL Certifications/Licenses Certified Ethical Hacker (CEH) First Aid CPR AED April 2020 Top Secret Clearance Additional Information FIPS 199, FIPS 200, NIST 800-53 Rev4, NIST 800-37, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), Risk Assessment (RA), SSP, ISCP, ST&E, SAR, Plans of Action and Milestones (POA&M), Authorization to Operate (ATO) Letter, MS Office, SharePoint, Access, PeopleSoft, Nessus Vulnerability Scanning Tool, Splunk

Name: Zachary Moreno

Email: claudiahoward@example.com

Phone: 7505816175