IT Security Analyst IT Security Analyst Silver Spring, MD DEDICATION | LEADERSHIP | ETHICS Vast background and experience in Federal Information Security Management, IT infrastructures, and maintenance of large information systems. Extensive experience using the appropriate tools to assess and analyze existing applications for system weaknesses and vulnerabilities and implementing techniques for mitigating security threats and risks. Hands-on experience in implementation of the Plans of Actions and Milestones / Corrective Action Plans, as well as remediation of the documented threats and vulnerabilities. An expert in the field of risk-based certification and accreditation using various flavors of the State, Federal, as well as International Cybersecurity frameworks (e.g. NIST RMF, FedRAMP, HIPAA, PCI DSS, ISO 27001, SOX, COSO/COBIT etc.) Immensely knowledgeable of industry standards and proven track record of implementing the necessary controls to ensure compliance. Authorized to work in the US for any employer Work Experience IT Security Analyst Smartlink - Annapolis, MD June 2017 to Present Support ISSO with investigation and closure of incidents in cooperation with the SOC. Use SIEM technologies and other tools to perform the monitoring of security events on a 24x7 basis. Manage/monitor request via the Remedy ticketing system. Conduct security control assessments to assess the adequacy of management, operation privacy, and technical security controls implemented. Assess security and privacy controls using the NIST SP 800-53A Rev4 publication guideline. Responsible for POA&M Management/Continuous Monitoring and milestone follow through by coordinating with system stakeholders/control owners (e.g., Systems Admins). Physically identify/open POA&M items, track, and facilitated POA&M closer. IT Security Specialist United States Secret Service - Washington, DC February 2017 to May 2017 Managed the information security function in accordance with the established policies and guidelines. Help conduct FedRAMP Readiness Assessments and reviewing ATO packages for FedRAMP Cloud environments. Responsible for IT Security Awareness Training, Contingency Plan Training and Incident Response Training. Assess security and privacy controls using the NIST SP 800-53A Rev4 publication guideline. Review security policy documents and make recommendations on documentation compliant. Conducted and performed continuous monitoring pursuant to NIST

Guidelines requirements. Provided impact analysis for updates and version changes required by the NIST Security Publications and FISMA Notices Support control testing and development of Plans of Action and Milestones (POA&M) Responsible for tasks related to the system and follow the Government IT security policies and standards. Senior IT Auditor/ Engineer Mitsubishi Heavy Industries Inc - Chantilly, VA April 2015 to January 2017 Performed information system and integrated audits to assess the adequacy of internal controls, validate compliance with regulatory standards and identify opportunities to streamline operational processes. Coordinated data collection, analysis and reporting for IT Security Data Calls, FOIA Requests, and Incident reports. Assessed the controls, reliability and integrity of the company's systems and data to assist with maintaining and improving the efficiency and effectiveness of risk management, internal controls and corporate governance. Worked with CISO to plan engagement strategy, define objectives, and address technology-related controls risks and issues. Ensure documentation reflects current control environment for Key Controls, Non-Key Controls, and Issues (with related Management Action Plans) Worked with management and compliance leaders to assure security programs were in compliance with security rules and other relevant laws, regulations and policies to minimize or eliminate risk and audit findings. Assisted management with incident response (CSIR) as well as determining the nature of incidents such as computer intrusion, distributed denial of service (DDOS) and working with senior management on mitigation risk strategies and remediation. IT Security Analyst URAC Helpdesk - Washington, DC August 2012 to July 2014 Provided expertise on technical services including all aspects of information security Conduct IT risk assessments to identify system threats Assessed system design and security posture as well as advising information security compliance with FISMA and NIST SP 800-53 controls. Conducted security control assessments to assess the adequacy of management, operation privacy, and technical security controls implemented Performed maintenance and advanced configuration of systems in order to protect systems from emerging cyber threats. Conducted forensic traffic logs analysis to isolate issues and respond to analyst alerts Business Impact Analysis (BIA) to analyze mission-critical business functions and identify and quantify the impact if these are lost (e.g.,

operational, financial). BIA helped to define the company's business continuity plan and IT internal control audit objective. References will be provided upon request Education B.S in Business Administration University of Maryland University College - Adelphi, MD May 2015 Skills FISMA Compliance Certification, FISMA Center, Washington, DC September 2013

Name: Megan Anderson

Email: jamesmunoz@example.com

Phone: +1-698-364-5292x640