IT Security Analyst IT Security Analyst IT Security Analyst - Service Source Work Experience IT Security Analyst Service Source June 2015 to Present Applying and implementing the NIST Risk Management Framework and Special Publications 800-53, 800-37, NIST Cybersecurity Framework, and other FISMA requirements Reviews and continuously monitors implemented security controls. Creates and maintains security checklists, templates and other tools to aid in the A&A process. Performs security control assessment using NIST 800-53A guidance and as per continuous monitoring requirements. Document the results of Certification and Accreditation activities and technical or coordination activity and prepare the system Security Plans and update the Plan of Actions and Milestones POA&M. Help guide System Owners and ISSOs through Certification and Accreditation (C&A) Process, ensuring that Operational, management and technical control securing sensitive Security Systems are in place and being followed according to the Federal Guideline (NIST SP800-53). Review System Security Plan (SSP) Develop and implements information assurance/ security standards and procedures. Coordinated, developed, and evaluated security programs for an organization. Supports customers at the highest levels in the development and implementation of doctrine and policies. Responsible for Developing the appropriate documentation and reports necessary to validate systems that need security and privacy requirements in accordance to the Risk Management Framework (RMF) authorization process. Information Assurance Analyst RedSpeed June 2012 to April 2015 Advise system owners on all matters, technical and otherwise, involving the security of assigned IT systems. Develop standard operating procedures in accordance with security control requirements. Conduct self-assessments of security controls, identify weaknesses and track remediation activities in Plan of Action and Milestones (POA&M).. Perform continuous monitoring of security controls to ensure that they continue to be implemented correctly, operating as intended and producing the desired outcome with respect for meeting the cybersecurity requirements for assigned IT systems. Validate IT security architecture for compliance. Complete required A&A (Assessment and Authorization) activities on assigned IT systems. Monitor security scans and analyze data to assess threats. Conduct vulnerability assessments on networks, servers, websites, databases, and assist with other assessment activities. Provide the required system access, information, and documentation to security assessment and audit teams Perform security controls assessments in accordance with NIST SP 800-53A, to include interviews, examinations, and vulnerability testing. Help Desk Support Manav Consulting Group Inc September 2010 to June 2012 Tier 1) Assigned ticket severity, prioritized work accordingly, and collaborated with other staff and vendor support resources to resolve issues. Coordinated with contractors and vendors to repair office equipment's such as printers, fax, copier and workstations. Provided customer service support and end-user training via phone and email. Maintained an inventory and database of IT related assets, including hardware, software, peripherals. Provided office equipment to office staff as requested through Remedy ticketing systems. Able to offer versatile office management skills. Education Business Management and Administration College of DuPage

Name: Frank Hernandez

Email: rachelgreene@example.net

Phone: +1-210-929-7042x351