IT Security Analyst IT Security Analyst IT Security Analyst - Reality - Technology Greenbelt, MD Over 10 years of experience in Information Technology services supporting security initiatives for government and commercial customers. Work experience encompasses threat analysis, incident response, Risk Management Framework (RMF), National Institute of Technology (NIST), System Development Life Cycle (SDLC), Information security documents, developing and promulgating Security Assessment Plans (SAP) and Security Assessment Reports (SARs). Work Experience IT Security Analyst Reality - Technology February 2017 to Present Conduct IT risk assessment to identify system threats, vulnerabilities and risk, and generate reports. Maintain, review and update information security system documentations, including System Security Plan (SSP), Plan of Action & Milestone (POA&M), Risk Assessment (RA), policies and procedures, security control baselines in accordance with NIST guideline and security practices. ? Apply appropriate information security control for Federal Information System based on NIST 800-37 rev1, SP 800-53, FIPS 199, FIPS 200, and NIST SP 800-53A R4, PIA's, PTA's Assess security controls and develop security assessment report (SAR) Support A&A activities (Categorize, Selection, Implement, Assessment, Authorize, Monitor) according to the A&A project plan. ? Review authorization documentation for completeness and accuracy for compliance. ? Facilitate Security Control Assessment (SCA) and monitor activities. ? Executed examine, interview, and test procedures in accordance with NIST SP 800-53A Revision 4. ? Ensure cyber security policies are adhered to and that required controls are implemented. ? Validated information system security plans to ensure NIST control requirements are met. ? Assist team members with proper artifact collection and detail to client's examples of artifacts that will satisfy assessment requirements. ? Review security logs to ensure compliance with policies and procedures and identifies potential anomalies. ? Update and review A&A Packages to include Core Docs, Policy & Procedures, Operations & Maintenance, Artifacts, SSP, SAR, FIPS 200, FIPS 199, and POA&M. ? Collect Operation & Maintenance artifacts on an ongoing basis so that Security Control Assessment (SCA) is seamless. ? Upload supporting documentations into the SharePoint, Google Docs, and CSAM. ? Manage vulnerabilities with the aid of Nessus Vulnerability Scanners to detect potential risks on a single or multiple asset across the enterprise network. Information Security Analyst KFORCE February 2014 to July 2017 Ensure proper system categorization using NIST 800-60 and FIPS 199; implement appropriate security controls for information system based on NIST 800-53 rev 4 and FIPS 200. ? Conduct security assessment interviews to determine the Security posture of the System and to Perform kick Off Meetings. ? Apply appropriate information security control for Federal Information system based on NIST 800-37 Rev 1 ? Facilitate Security Control Assessment (SCA) and monitor activities. Develop a Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain Company Authorization to Operate (ATO), the Risk Assessment, System Security Plans, and System Categorization. ? Reviewing, maintaining, and ensuring all assessment and authorization (A&A) documentation is included in the system security package. ? Perform information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements. ? Work with system owners to develop and test on contingency plans and incident response plans. ? Tests, assess, and document security control effectiveness. Collect evidence, interview personnel, and examine records to evaluate effectiveness of controls. ? Review and update remediation on plan of action and milestones (POA&Ms), in organization's CSAM Work with system administrators to resolve POA&Ms, gathering artifacts and creating mitigation memos, residual risk memos and corrective action plans to assist in the closure of the POA&M. Cyber Security Documentation Specialist Nu-Pulse Technologies October 2011 to February 2014 Created folders in Active Directory groups and assigned read/write permissions, disabled/enabled accounts/devices and managed policies. ? Utilized Excel to create static templates of deliverable schedule; schedule included task, owner, comments, start/end date for actions required for Risk Assessment Report, Security Assessment Report, Plan of action & Milestone, penetration test report results, categorization guide, topology, hardware/software list, Information flow, and deliverables pertaining to Authority to Operate. Once deliverables are submitted, verify completion and submit package to Chief Information Officer for review. ? Reviewed Interconnection Service Agreement (ISA) to ensure affiliates are inside of our accreditation boundaries. ? Reviewed Web Hosing Plan for the fiscal year ensuring the customer proposal summary information support workbook has a proper renewal. ? Produced Business Impact Analysis documentation ? Corresponded with Information System Security Officer on a weekly basis to ensure task/action items are being completed while taking notes on any new task that are distributed. ? Knowledge of understanding in-depth security procedures for new Information Systems ? Created and disseminated Knowledge base (KB) Articles to facilitate Service desk functionality including screenshots with step by step instructions for redundant issues ? Provided Weekly Activity Reports Computer Operator V-Tech March 2007 to October 2011   Adhered to administrative and service desk standards   Provide Audiovisual Support to end user for teleconferences; supporting set up delegations, troubleshooting connectivity issues as well as performing routine preventative maintenance support on all Audio-Visual devices specified by the manufacturer and or local operating instructions   Utilizing SharePoint for setting permissions to folders; recovered deleted files utilizing audit logs & MS365 Protection Center; uploaded and modified documents & permission levels, stored organized and access client's information   Utilized MS Outlook calendar; created shared files with-in outlook for scheduled task delegated by management   Manage VoIP phones   Utilized MS Excel to create template   Ensured all request for services were followed-up in a timely manner via email, VOIP telephone, and in person   Provided excellent communication, documentation, and customer service   Provided people skills, attention to detail, multi-tasking and professionalism   Created folders in AD groups and assigned read/write permission, disabled/enabled accounts/devices and managed policies   Interacted weekly with customers via VoIP & remotely to ensure resolution of any product issues   Programed NRAS tokens via LDAP & SEC DOC Server's and push certificates via HDE Server for end users working remotely   Responsible for installing various software applications including antivirus, pushed patches & ensured maintenance of end user workstations and peripheral devices   Remotely wiped devices that were lost or stolen and created report documenting the acts that lead up to the lost or stolen device   Removed/Added Datasets to mainframe and reset mainframe passwords   Computer & Software Proficiencies   ? Microsoft Office Suite ? PowerPoint ? CSAM

? Adobe ? Qualified Typist (70wpm) ? Nessus Vulnerability Scanner (SC-5) ? IBM Security App Scan ? MS Project Education Bachelor's in Cyber Security ITT Technical Institute - Hanover, MD August 2012 to May 2016 Certifications/Licenses Sec+ June 2018 to June 2021 A+ Certified September 2015 to September 2021 MTA Security Fundamentals December 2014 to Present

Name: Jane Hernandez

Email: eoconnell@example.net

Phone: (554)457-0088x77858