Job Seeker Laurel, MD Work Experience Information Systems Security Officers - Temple Hills, MD January 2016 to June 2019 Perform cybersecurity planning process and gather information in order to implement detailed NIST operational supporting requirements. Ensure compliance to security standards and policies, monitoring access privileges, conducting risk assessments, investigation of suspicious activities, and remediation of identified security threats or risks. Assisting in the development, updating, distribution, and presentation of security training and awareness materials. Ensure compliance to security standards and policies like HIIPAA, HITRUST, NIST, FISMA and FEDRAMP, PCI DSS. monitoring access privileges, conducting risk assessments, investigation of suspicious activities, and remediation of identified security threats or risks. Monitor and conduct Security Control Assessment to ensure all controls meet security requirements as stipulated in the NIST 800-53 Rev4. Ensure client configure an audit logging solution and determine how logs are collected, reviewed, and accessed to meet HIPAA requirements. Identifies sensitive Personal Identifiable Information-PII (per NIST 800-122) and ensure that System Security measures are taken to protect them. Perform FedRAMP Government-wide program that provides a standardized approach for security assessment, authorization, and continuous monitoring for cloud products Conduct scheduled security audit log reviews, and report any suspicious activities. facilitate security documentation for SSP packages and work with designated approvers to move C&A process forward. Design, create, Update and track security Plans of Action and Milestones (POA&Ms). XACTA or CSAM Perform vulnerability and risk assessment using tools such as Nessus, AppDetective/DbProtect for enterprise level vulnerability scanning. Prepare Security Authorization Packages and Artifacts sing FIPS 199, 200, 201; NIST SP 800-18, 37 Revision 1, 39, 53 Revisions 3 and 4, 53A Revision 1, 60 Volumes 1 and 2, 800-64 Revision 2, 137, 144, 147, FEDRAMP, ISO 27001/2, SOX1 and SOX 2 Utilizes Security Information and Event Management (SIEM) tool Splunk, Intrusion Detection & Prevention (IDS/IPS)snort, Data Loss Prevention (DLP) symantec tools to detect potential data breaches/data ex-filtration perform patch deployment or workaround into the change control systems and follow the change control Ensure technical controls are implemented for encrypting PHI, PIA, PCI DSS data in-transit and at-rest on AWS. Ensure all

POA&M actions are completed and tested manage the Use automated tools to perform static source code and dynamic security testing to identify vulnerabilities and attack vectors in web applications. Planned, System Security Checklists, Privacy Impact Assessments, POA&M, and Authority to Operate (ATO) letters. Develop and conduct ST&E (Security Test and Evaluation) according to NIST SP 800-53A and Continuous Monitoring of Authorized System, NIST 800-137 guidelines. Schedule and attend weekly meetings for audits, POA&M findings and after action review. Cyber Security Analyst Imitor Group - Columbia, MD January 2014 to January 2016 Completed C&A/A&A packages that have obtained and maintained full authorization to operate (ATO) Worked with Security Operation Center Analyst in making sure Intrusion detection and prevention systems(IDS/IPS) such as SNORT to analyze and detect Worms, Vulnerabilities exploits attempts and IDS monitoring and management using Security Information and event management (SIEM), to collect and Analyze large volumes of logs and network traffic and alerts to assess, prioritize and differentiate between potential intrusion attempts and false alarms. Prepare, update and maintain RMF documentation such as, but not limited to, Authorization to Operate (ATO) packages, System Security Plans (SSP), Risk Assessment Reports (RAR), Security Control Traceability Matrixes (SCTM) and Plan of Actions and Milestones (POA&Ms) for all networks and systems. Provide Configuration Management (CM) for IS security software, hardware, firmware and coordinating changes and modifications with the ISSM, SCA and Authorizing Official (AO). Work closely with Security Control Assessors (SCA) to determine effectiveness of current security controls and a path forward to implement future security controls, where potential weaknesses might exist. Ensure the following activities are required and completed on a periodic basis (e.g. ensuring data is backed up, account management (deactivate unused accounts and validate user access rights), participate in the Systems Development Life Cycle (SDLC). Identified trends and root causes of system failures or vulnerabilities using NESSUS Vulnerability Scanner, Nmap to scan ports, weak configuration and missing patches. Assured that the Information Systems Security department's policies, procedures, and practices as well as other systems user groups are in compliance with FISMA, NIST, identifying and analyzing security logs from various security tools

such as Intrusion Detection System (IDS) and Security Information and Event Management (SIEM). Conduct Contingency Plan tests at least annually and updating the plan; Conducted FISMA-based security risk assessments for various government contracting organizations and application systems - including interviews, tests and inspections; produced assessment reports and recommendations. Participate in development and review of System Security Documentation, including System SecurityPlans (SSP), IA policies, Personnel Security, Disaster Recovery, Incident Responses, Authentication Management plan,, configuration management and patch management Generate, review and update System Security Plans (SSP) against NIST 800-18 and NIST 800 53 requirements. Review Technical Security Controls and provided implementation responses as to if/how the Systems are currently meeting the requirements. Participated in continuous monitoring that includes but not limited to POA&M management, waiver &Exception support and periodic re-certification in accordance to NIST SP 800-137. Perform Security Categorization (FIPS 199), review and ensure Privacy Impact Assessment (PIA).Document and finalize Security Assessment Report (SAR) and communicate a consolidated risk management activities and deliverables calendar. Conducted gap analysis to make sure correct controls were in POA&MAssisted with review of policy, security alerts guidance, regulations and technical advances in IT Security Management Utilize NIST SP 800-18 and update System Security Plans from SP 800-53.Provided continuous monitoring support for all FISMA systems. Develop and test security risk assessments. IT Specialist DC Department Of Correction - Washington, DC June 2011 to November 2013 Supporting users by identifying, troubleshooting, and resolving any hardware, software or connection issues Manage computer accounts in Active Directory Monitor staff responses to user problems with hardware and software to ensure that customers service, technical, SLA (service level agreement and quality control standards are met using Tool like Landesk. Providing support for mobile Android and IPad devices. Providing in-person support to users for various systems, including e-mail, printers, LAN/WAN, VPN, user accounts, standard desktop images and applicationss, laptop peripherals, and mobile devices. Create/Track service requests through SharePoint portal Submit/follow up on tickets requiring 3rd party action through Supporting

customers with computer related issues through customer education, training and direct assistance. Re-imaging, updating/applying approved patches to Windows 7 Ensuring backup, and data restoration from workstations for customers during re-images or when a problem with the system is diagnosed. Experience identifying/resolving laptop/desktop software/hardware/network issues. Experience identifying/resolving issues and replacing supplies for Printers, Scanners and multi-functional devices. Excellent analytical, oral and written communication, presentation, and problem-solving skills. Ability to gain internal support and to operate independently without supervision. Ability to establish a solid working relationship with customers, technical staff, managers and peers. Serve as the primary provider of technical support to users for desktop and laptop computers, mobile devices (iPhone, Android), printing, scanning, faxing and software applications Education Bachelor of Computer Science in Computer And Information Sciences University of Benin

Name: Nancy Gray

Email: bmartin@example.org

Phone: (400)990-0129