Information System Security Analyst Information System Security Analyst Information System Security Analyst - CYBERSOFT TECHNOLOGY INC Saddle Brook, NJ Years of experience in compliance, & system security management with focus in: Business development, internal controls compliance, customer data confidentiality, risk management. Managed operations in the following areas; information technology compliance, customer data confidentiality, integrity and availability. Currently work directly with the SISO to ensure that implemented controls are operating effectively and as intended. Authorized to work in the US for any employer Work Experience Information System Security Analyst CYBERSOFT TECHNOLOGY INC - Lanham, MD December 2015 to Present Monitoring existing security controls against the risks of potential vulnerabilities being exploited by threats. Responsible for selecting and installing firewall and anti-virus software to protect our organization's network against malicious threats Responsible for installing software to monitor security across organization's computer system Responsible for effective backup & recovery strategy to ensure availability of data in case of major security attacks or natural disaster Responsible for monitoring employee access levels, review & update employee privileges & permissions on a regular basis Using NIST SP 800-60 & FIPS 199, determine the system categorization for organizations by evaluating information types and then relate them to the security objectives (Confidentiality, Integrity, & Availability) Responsible for determining the classification of information systems, impact levels, assess existing security controls and recommend alternative controls to include technical, management & operational to enhance the security posture of organization if necessary When working on projects, responsible for developing a security authorization package, consisting of; (i) System Security Plan (SSP), (ii) System Assessment Report (SAR), and (iii) Plan of Action & Milestones (POAM) Conversant with risk assessment plan, business impact assessment, continuous monitoring strategy, data loss prevention, disaster recovery plan / contingency plan, configuration management plan, information & information security management, security assessment plan, system architecture diagrams, & incidence response plan Perform vulnerability scanning using Nessus & Retina. Run intrusion detection system (IDS) with low or no false positives IT Support/ Analyst NETWORK DYNAMIC INC - Owings Mills, MD October

2012 to November 2015 Provided training & support to on the use of electronic information system. Implemented strong security controls and password complexity and ensured staff complied to them Developed an effective plan to improve workflow via electronic system. Troubleshoot systems errors, malfunction or glitches Ensured that all electronic information systems are running smoothly Installed and configured software and related products Established effective Backup & Recovery policies & procedures, also created and maintained users and roles Assigned and revoked user privileges using least privilege and role-based policies (maintained database security) Worked in conjunction with developers to design and implement databases Education Certification ISC Bachelor's Degree in Public Administration University of Maryland - Upper Marlboro, MD Skills disaster recovery (2 years), Nessus (2 years), NIST (2 years), SAR (2 years), Security (5 years) Additional Information SKILLS & EXPERTISE: Extensive experience in mitigating against vulnerabilities by dispatching up-to-date patches on a regular basis and hotfixes when needed. Familiar with FIPS 199, FIPS 200 & NIST Special Publications 800-30 & 37, 800-39, 800-53A & Rev4, 800-60, 800-70, 800-115, 800-137 etc. Understand the importance of backup & recovery, and system disaster recovery plan. Ability to run vulnerability scanning, using Nessus and Retina vulnerability scanners. Knowledgeable in penetration testing and port scanning. Experience in evaluating and analyzing the Risk Management Framework (RMF). Ability to develop and analyze a System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), and also a Plan of Action & Milestones (POAM). Possess knowledge in Security Control Assessment (SCA); testing controls to ensure they are implemented correctly, operating as intended, and producing desired results. Extensive experience in implementing a robust continuous monitoring strategy. Interpersonal Skills: An effective communicator (written and oral), great team player with an equally great ability to work as an individual. Organizational and problem solving skills. TECHNICAL SKILLS: Operating Systems: Windows. Microsoft Office Applications, Access Control, Identification & Authentication.

Name: Eric Frazier

Email: ehughes@example.org

Phone: 846.485.6464