Information System Security Officer (ISSO) Information System Security Officer (ISSO) Mid Level Information Security Professional Alexandria, VA I have 6 years of work experience in information security. I would like to take this opportunity to share certain skills sets which will justify my claim for the selection. As part of my work requirements, I have worked on various platforms and managed successfully, several IT security assignments. I have considerable experience of working at various stages of IT security, such as software development, implementation and monitoring etc. I am sure with my skill sets and knowledge, I will be able to perform effectively, and help the organization meet its goals satisfactorily. I do hold a Bachelor of Science in computer science and I am currently doing an online Master s of Science in Cyber Security at Maryville University ST Louis Missouri. In Addition, I am preparing to write the Certified Information Systems Security Professional (CISSP) board exam. I have held various responsibilities such as IT Security Analyst as well an Information System Security Officer (ISSO). I am sure with my comprehensive exposure I can be a vital part of your organization and contribute significantly in addressing your IT security concerns. All these qualities make me an ideal candidate for the job position. My experience has imbibed in me the leadership skills required to lead my team with motivation and enthusiasm. My communication skills have helped me in effective coordination with all liaison departments. This ensures smooth functioning with maximum productivity. I am interested in the job opening as it would give me an opportunity to explore my skills further and develop as a professional which will be beneficial for mutual growth. Authorized to work in the US for any employer Work Experience Information System Security Officer (ISSO) Arc Aspicio Consulting - Washington, DC January 2015 to Present Ensure security policies, procedures; recommendations comply with FISMA, NIST, Organizational guidelines and technical best practices. Implement Risk Management Framework (RMF) in accordance with NIST SP 800-37. Participates in the development and maintenance of system security plans and contingency plans for all systems under their responsibility. Planned, System Security Checklists, Privacy Impact Assessments, POA&M, and Authority to Operate (ATO) letters.

Develop Plan of Action and Milestones (POA&M) for identified vulnerabilities and ensure compliance through monthly updates. Maintain inventory of all information Security System

assigned. Develop a variety of Assessment & Authorization deliverables including; System Security Plan (SSP), Security Assessment Report (SAR), Contingency Plan (CP) and POA&M for review and approval for Authorization Official. Monitor and conduct Security Control Assessment to ensure all controls meet security requirements as stipulated in the SSP and NIST SP 800-53 Rev4. Verify file intergrity and encryption of communication. Effectively communicate Technical Information to non technical personels. Identify active network devices, ports and communication paths. Cordinate with ISSO across the organization to ensure timely compliance. Develop Waivers and exceptions for information system vulnerabilities. Performed Risk Assessment in accordance to NIST SP 800-30 Rev 1. Reviewed and ensured Privacy Impact Assessment document after positive is created. IT Security Analyst Pragmatics Inc - Reston, VA 2011 to December 2014 Perform System security categorization using FIPS 199 & NIST 800-60. Advise Information System Owner (ISO) of security impact levels for Confidentiality, Integrity and Availability (CIA) using NIST SP 800-60 V2. Utilize NIST SP 800-18 and update System Security Plans from SP 800-53. Perform vulnerability scanning on web applications and databases to identify security threats and vulnerabilities using Nessus Scanner. Collaborate with ISSO's in remediating audit findings, security planning and reporting, and mitigation of security vulnerabilities are completed in a timely manner. Monitors, evaluates and report on the status of information security system and directs corrective actions to eliminate or reduce risk. Initiate compliance and vulnerability scan request to identify and report weaknesses and potential security breaches. Conducted meetings with IT team to gather documentation and evidence about their control environment. Provided ongoing gap analysis of current policies, practices, and procedures as they relate to established guidelines outlined by NIST, OMB, and FISMA. Communicated clearly and concisely, both orally and in writing with team members and top management. Education Masters of Science in Cyber Security Maryville University - St. Louis, MO Bachelor of Science in Computer Science Catholic University of Central Africa Risk Management Framework TrainAce Cyber-Security Academy - Ashburn, VA Skills SECURITY (6 years), MITIGATION (4 years), NESSUS (4 years), SCANNING (4 years), ACCESS (Less than 1 year) Additional Information TECHNICAL SKILLS

Networking: LANs, WANs, VPNs, Routers, Firewalls, TCP/IP Software: MS Office (Word, Excel, Outlook, Access, PowerPoint) Vulnerability Scanning Tool - Nessus Tools of POA&M- CSAM and XACTA Security Monitoring- Splunk Penetration Testing Tool - Kali Linux KEY COMPETENCIES 1) Monitoring Monitor the security of critical systems (email, server, database and webservers) and changes to highly sensitive computer security controls to ensure appriopriate system administrative actions, investigate and report on noted irregularities. Conduct network vulnerability assessment using tools to evaluate vectors, identify system vulnerability and develop remediation plans and security procedures. Conduct routine social engineering tests and clean desk audits. Investigate potential or actual security violations or incidents in an effort to identify issues and areas that require new security measures or policy changes. 2) Strategic Development

Cordinate with third parties to perform vulnerability test and create security authorization agreements and standards. The ability to balance risk mitigation with business needs. Define, establish and manage security risk metrics and track effectiveness. Research new development in IT security in order to recommend, develop and implement new security policy standards, procedures and operating doctrines across a major global enterprise. 3) Disaster Recovery Collaborate with business units to determine continuity requirements. Conduct business impacts analysis for the vital functions, document recovery priorities of the key processes, applications and data. Established disaster recovery testing methodology. Plan and coordinate the testing of recovery support and business resumption procedures while ensuring the recovery and restoration of key IT resources and the data and resumption of critical systems within the desired timeframe.

Name: Diane Hays

Email: ethan51@example.com

Phone: 510-476-8836x1274