Senior Information Security Analyst Senior Information Security Analyst Senior Information Security Analyst - ASM Research INC Fairfax, VA Work Experience Senior Information Security Analyst ASM Research INC - Fairfax, VA February 2014 to Present Responsible for performing secure code reviews, software and vulnerability scans utilizing static and dynamic code analysis tools, and ensures the use of secure Software Development Life Cycle (SDLC) practices for the Department of Veteran Affairs (VA) project. Analyze code against industry best practices and federal security standards to ensure compliance. Integrate best practice into the development process to ensure that the secure code is being developed and architecture decisions are being reviewed from a security perspective. Integrate Fortify within the AWS environment and Continuous Integration pipeline process such that vulnerability scans can occur against the application source code. Work cooperatively with the Director and other applicable organization units in overseeing patient rights to inspect, amend, and restrict access to protected health information when appropriate. Present security findings to management and technical staff and assist the IA team in completing compliance tasks in accordance with the NIST Risk Management Framework (RMF) and submit Assessment and Authorization (A&A) documentation to support an Authority to Operate (ATO). Develop Plan of Actions and Milestones (POAMS) and Corrective Action Plans (CAPs) to remediate audit findings. Track and communicate team velocity and sprint/release progress. Conduct vulnerability assessments and support the mitigation of any defined risks. Create and maintain documentation in support of Assessment and Authorization (A&A) activities for the VA project. Experienced in Agile development environment. Senior IT Security Analyst REI Systems - Sterling, VA April 2012 to February 2014 As a Senior IT Security support and work closely with the senior security manager for performing the security requirements and preparation the documents. Deploy network-based IDS for internal systems for unusual attack mechanisms and to detect any malicious or suspicious traffic.

Reviewed all system-related information security plans throughout the organization's network to ensure alignment between security and privacy practices, and acts as a liaison to the information systems department. Participated in the development, implementation, and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns,

requirements, and responsibilities are addressed. Conduct systems scanning and configure Nessus scan tool of vulnerability management for the security compliances of the OS and Netsparker, WebInspect for the software applications. Identify security risks, threats and vulnerabilities of networks, systems, applications and new technology initiatives. Plan effective AGILE IT security using mind mapping techniques. Apply FISMA system security framework and NIST requirements to the architecture, design, development, evaluation and integration of systems and networks. Ensure compliance with FedRAMP and NIST technical control requirement for cloud computing as SaaS (software as a service). Coordinate with AWS (Amazon Web Services) Cloud Computing technical staff. Configure the Orion Network Monitoring tool and coordinate with the vendor's technical staff Perform security administration of firewalls, Intrusion Detection Systems, and Security Monitoring Systems. Interact with management and other teams in a collaborative, problem solving environment addressing technical and business issues. Conduct vulnerability assessments and mitigate risks. Develop documentation in support of Certification & Accreditation activities for various federal agencies such as NASA, DOE, DHS, HRSA and USDA. Design, deploy, and support end-to-end peer review and security posture application designed to process grants annually. Ensure that security controls are part of the System Development Lifecycle. Solid foundational knowledge in PKI, certificates, TLS/SSL, and Federal security configuration compliance requirements for FIPS 140 and FIPS199. Principal IT Security Engineer Advance Technology Services Corporation - McLean, VA June 2011 to April 2012 Brief Senior Executive Management regarding system documentation, identified vulnerabilities, and POA&M remediation. Support the DHS (Science and Technology) in identifying and meeting information assurance requirements and develop and implement information security policies and procedures. Review and recommend mitigations or countermeasures, and resolve integration issues related to the implementation of new systems within the existing infrastructure. Oversee development team and ensure application security standards are being followed and compliant with the DHS policies and security handbook. Conduct on-site visits to Data Centers and performed interviews with ISSO's, system Owners, network administrators, and system administrator. Assess security controls

in-place in accordance with NIST guidance. Configure the Orion Network Monitoring tool and oversee the vendor's technical staff for system to be able to analyze the metrics for the better and efficient performance. Review technical requirements. Work with DHS/S&T BorderNet Team in integrating IA controls into the final solutions. Identify security risks, threats and vulnerabilities of networks, systems, applications and new technology initiatives. Experienced working with FISMA, Computer Security Act and other federal regulations related to information security. Managed auditing functions that follow national, federal and organizational policy to ensure all unclassified DHS (Science and Technology) information systems (to include general support systems and major applications) are in compliance. Provide expertise on the coordination, development, improvement and implementation of the IT security risk management program and risk mitigation strategies. Senior IT Security Engineer ActioNet INC - Alexandria, VA May 2010 to June 2011 Coordinate with internal and external auditors to determine compliance with policies, directives and standards. Provide information on security policies, directives, standards and procedures to trading partners of the agency and interact for operational or commercial reasons. Reviewed OS baseline configuration and policies. Audit the Plan of Action and Milestones (POAM) for security weaknesses. Interpret data and create reports and dashboards for senior management. Assist the IT Department in developing a policy and procedures to provide cost effective, quality, system and network security assessment and certification based on unified federal guidelines and procedures. Assist SEC Operational Data Center in identifying and meeting information assurance requirements. Analyzed the development and implementation of information security policies and procedures for patch and vulnerability. Used Qualys and Bigfix tools to create regular reports for vulnerabilities and path management in the network systems. Senior Information Assurance Analyst General Dynamics Information Technology (GDIT) - Arlington, VA September 2008 to May 2010 Recommended mitigations or countermeasures and resolved integration issues related to the implementation of new systems. Perform Certification & Accreditation (C&A) activities in accordance with DHS 4300 Handbooks for the OIT managed systems. As team lead, supported the process framework project for the implementation and management of controls to ensure that

specific security objectives are met. Support United States Citizenship and Immigration Services (USCIS) in identifying and meeting Information Assurance requirements and analyzed the development and implementation of information security policies and procedures. Supported DHS (US CIS) Operations & Maintenance division and users throughout the agency in the development and implementation of systems and subsystems to meet the transactional processing needs of the US CIS. As IT Security team lead, interpreted civil and federal government guidance, including FISMA and NIST security requirements for US CIS. Ensured application security standards are followed and implemented correctly by the development teams. Provided vulnerability mitigation strategies. Evaluated new security technology & trends and recommended ways to strengthen client information security environment. Worked closely with the Project Management Office (PMO) to provide risks assessments, cost estimates and schedules for projects and Operations and Maintenance (O&M). Supported the Director of Information Assurance division in vulnerability release management, incident response, operational inefficiencies, intelligence analysis and research, and other areas. Provided operational and strategic support to the Department of Homeland Security (DHS) Control Systems Security Program (CSSP). Senior Information Assurance Analyst SRA International - Fairfax, VA September 2007 to September 2008 Integrate with a team of skilled information technology security professionals demonstrating competence in the application of the system certification guidelines and procedures. Conduct on-site visits to Data Centers and performed interviews with ISSO's, System Owners, Network Administrator, System Administrator, etc. to properly assess security controls in-place in accordance with NIST guidance, Perform Federal Information Security Management Act (FISMA) audit reviews; Develop and review system security plans, plan of actions and milestones (POA&M), security control implementation, configuration management plans, contingency plans, incident response plans, security policy, and vulnerability scans at the Veteran Affairs (VA) Department. Provide technical architecture support to the Department of Veteran Affairs (VA) Public Key Infrastructure (PKI) program utilizing Java and C++ based certificate authorities, directory services, transaction processing systems, and smart card applets. Support security architects in developing existing

and future systems architecture artifacts. Perform design and system analysis, requirements definitions, interface and data architectures, lifecycle cost estimation, and governance. Prepared informational documents to reduce cyber security risks and threats in critical infrastructure systems at VA OIT office. Information Security Specialist U.S. Department of Agriculture - Washington, DC February 2005 to September 2007 GS-13), Assess benefits, risks, and risk-adjusted life-cycle costs of alternative solutions and capital investments. Establish realistic cost, schedule, and performance goals for the selected alternative before proceeding to full acquisition of the capital project. Responsible for the strategic development and implementation of cost-effective training and support solutions that are designed to provide improved productivity, streamlined operations, and faster access to critical information. Lead the team and worked closely with the development and staging group in the application. Incorporate and integrate the new emerging information security concepts, principles, trends, technologies, and practices in the development and application of infrastructure control system security policies and practices. Provide technical expertise in advising and making recommendations for mitigating risks and conduct assessment activities to improve cyber security in critical infrastructures at the OIG office. Worked closely with the senior management at the OIG to carryout assessments to identify privacy-related risk for the IT Departments and monitored development of privacy training. Reviewed incident response planning and aided business with evaluating vendors. Analyzed adequacy of privacy programs. Implemented Cisco Security Agent software tool (CSA) as proactive intrusion detection and ensure all systems and servers had appropriate system patches installed. Performed audits of critical information systems such as mail servers, web servers and host applications and established mechanisms for risk review and mitigation. Coordinated with the client with technical understanding of systems and applications to ensure the C&A packages were completed on time. Use ISS (Internet Security System) tool and work closely with the OIG director to deploy network vulnerability and scanning to identify patching and vulnerability assessments across the servers, desktops, operating system, firewall, switches and routers Education Masters of Business Administration Strayer University - Manassas, VA Additional Information Experience in the Risk

Management, Risk Analysis and the NIST 800-30 Special Publication (SP). Coordinate the cyber security projects. These include supporting cyber security for IT infrastructure and IT- based organizations, resource protection, security planning, identity management, security information management systems, Assessment and Authorization (A & A, or C&A), policy and guidance, system test and evaluations (ST&Es). Excellent skills in clarifying business requirements, performing gap analysis between goals and existing procedures/skill sets, and in designing process and system improvements to increase productivity and reduce costs. Excellent project management skills - consistently delivered complex, large-scale projects on time and within budget. Consistently improved delivery times and service levels while reducing costs. Keen attention to detail and expert in providing interpretive knowledge of Federal agency IA requirements, policies, and procedures for information/infrastructure protection. Seasoned leadership and competence in planning, organizing, and executing agency projects with competing priorities in a fast-paced environment Results-driven team player; eager to take on new challenges with personal initiative and a keen sense of urgency, diligence, and enthusiasm. Excelled at strategic planning, building high-performance teams, project management, and implementing best practice methodologies and continuous improvement programs. Technical and Communications Skills People-oriented. Highly skilled in written and verbal communications with a diverse group of individuals to resolve complex issues with clarity and enthusiasm; able to handle difficult and sensitive issues with diplomacy and objectivity. NIST/IA Policies: FISMA, NIST, FIPS, OMB A-130, TSA1400.3, DHS 4300A &B Information Assurance Tools: ISS (Internet Security System), CSA agent, Nessus Scanner, Qualys and Bigfix,

Name: Andrew Wilson

Email: ojones@example.org

Phone: +1-391-216-5655