IT SECURITY ANALYST IT SECURITY ANALYST IT SECURITY ANALYST - Census Bureau Silver Spring, MD Work Experience IT SECURITY ANALYST Census Bureau - Suitland, MD September 2015 to Present Analyze and update System Security Plan (SSP), Risk Assessment (RA), Privacy Impact Assessment (PIA), System Security test and Evaluation (ST&E) and the Plan of Actions and Milestones (POA&M), in line with FISMA and FedRAMP regulations. ? Review vulnerability scan reports and track and address weaknesses in POA&Ms. Drive accreditation and assure the system is compliant with all required security controls as defined by agency policies. Develop and maintain C&A documentation (risk assessments; system security plans; contingency planning (CP); disaster recovery plans (DRP); plans of actions; milestones). ? Prepare regular status and audit findings reports for internal management, system owner, and ISSO. Ensure controls support Compliance with Regulations; enforcing adherence and advising management on needed actions. ? Conduct security control assessments based on NIST SP 800-53A to identify system threats, vulnerabilities, and risks. ? Conduct meetings to discuss vulnerabilities and potential remediation actions with system owners. ? Ensure identified weaknesses from vulnerabilities scans were remediated in accordance with the company's defined time frame. ? Involved in the company's security awareness program to educate employees and managers on current threats and vulnerabilities. ? Security Assessment Reports (SAR) are developed detailing the results of the assessment along with the Plan of Action and Milestones (POA&M). ? Lead the efforts across several security initiatives, including development and implementation of the customers' Continuous Diagnostics and Mitigation (CDM) program as well as the development of the formal process for maintaining clients' minor applications on an Ongoing Authorization (OA) ATO. ? Run security scans (Nessus, AppScan) and generate reports as part of clients' CDM program to identify system-level vulnerabilities. ? Lead kick-off meetings initiating security control assessments. ? Involved with customers' security awareness program to educate employees and managers on current threats and vulnerabilities. IT SECURITY ANALYST Iworks - Tyson, VA October 2013 to August 2015 Performed IT risk assessments and documented the system security keys controls in line with commercial frameworks (SOX 404 compliance, COSO, COBIT, ISO, IEC, HIPAA). ? Liaised with IT

team to gather evidence, develop test plans, testing procedures and document test results and exceptions. Designed and Conducted walkthroughs, formulated test plans, and test results, and developed remediation plans for each area of the testing. Wrote audit reports for distribution to management and senior management documenting the results of the audit. ? Participated in the SOX testing of the General Computer Controls. ? Developed a Business Continuity Plan and relationship with outsourced vendors. ? Provided support on security control testing, or another form of system testing as requested by Business/System Owners to identify vulnerabilities in security features of an application, system, network or operational weaknesses in process or technical countermeasures. ? Evaluated, maintained, and communicated the risk posture of each system to executive leadership and make risk-based recommendations to the Chief Information Security Officer (CISO). ? Provided guidance to stakeholders on required actions (systems planning and development projects), potential strategies, and best practices for the closure of identified weaknesses. ? Conducted periodic IT risk assessments and reviewed internal controls against the ISO standard for any deficiencies. Deficient controls were then reported to the CISO for appropriate mitigation actions. ? Initiated and led information security awareness and training program to inform the employees of their roles in maintaining a matured security posture. ? Created and maintained security metrics key risk indicators.to help senior management to make critical security risk decisions. ? Supported both internal and external audit activities including records collection, coordinating with other departments to collate all relevant information. ? Managed and coordinated audit-related activities with internal stakeholders and external auditors, and validating contractual obligations to ensure compliance. ? Categorized internal and external audit results and communicating findings, including recommendations to key stakeholders. ? Monitored the Information Security Compliance mailbox for inquiries from state and federal regulatory agencies. ? Prepared written responses to routine security and compliance inquiries by preparing, modifying documents including correspondence, reports, drafts, memos, and emails. ? Provided development guidance and assists in the identification, implementation, and maintenance of compliance policies, procedures, and work instructions. ? Maintained and reviewed regulatory documentation necessary

to maintain corporate standards. ? Design and perform IT and infrastructure HIPAA audits related to information security policy, regulations, governance, and other security-related provisions and best practices. ? Conducted related ongoing compliance monitoring activities to ensure the effectiveness of implemented controls. ? Tracked and communicated constraints, conflicts, or gaps to existing processes, as well as tracking cross-functional team remediation. ? Monitored and tracked best practices and emerging compliance changes/impacts for continuous improvement opportunities. IT SECURITY ANALYST CWorld Security LTD - Chevy Chase, MD April 2009 to September 2013 Creased the number of security reviews performed utilizing the same resources. ? Assisted with the planning and execution of domain integration, user account, and e-mail migration during M&A. ? Developed, designed, and implemented automated transaction processing, increasing production realized at 500%. ? Reviewed user accounts and access on a monthly basis to ensure regulatory and corporate compliance. ? Contributed to and participated in business continuity planning and verification. ? Adhered to and enforced corporate policies regarding network security, data, and software usage. ? Process re-engineered business protocols to meet the high demand of a changing business environment. ? Created, modified, and disabled user accounts base on authorized forms. ? Reduced security deficiencies by 98% over the previous calendar year. Education MASTER OF SCIENCE (MS) IN ACCOUNTING in ACCOUNTING Strayer University - Washington, DC BACHELOR OF SCIENCE in ACCOUNTING Prince George Community College Skills Security, Cobit, Data protection, Information security, Nessus, Nist, Nmap, Sox, Cisco, Firewalls, Fisma, Federal information security management act, Network security, Tcp/ip, Cyber security, Tcp, Unix, Sarbanes-oxley, System security, Risk assessments

Name: Adam Fox

Email: jenningspatrick@example.org

Phone: +1-282-633-5552x374