Information Security Analyst Information Security Analyst Information Security Analyst - Acentia LLC Philadelphia, PA Work Experience Information Security Analyst Acentia LLC June 2014 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) Assist System Owners and ISSO in preparing certification and Accreditation package for companies IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 R4 Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60 Conduct Self-Annual Assessment (NIST SP 800-53A) Perform Vulnerability Assessment. Make sure that risks are assessed, evaluated and a proper actions have been taken to limit their impact on the Information and Information Systems Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages Conducted I.T controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard. IT Auditor Royal Bank of Scotland - Stamford, CT June 2013 to May 2014 Perform IT risk assessment and document the system security key controls Meet with IT team to gather evidence, develop test plans, testing procedures and document test results and exceptions Design and Conduct walkthroughs, formulate test plans, test results and develop remediation plans for each area of the testing Wrote audit reports for distribution to management and senior management documenting the results of the audit Participate in the SOX testing of the General Computer Controls Develop a Business Continuity Plan and relationship with outsourced vendors Evaluate clients key IT processes such as change management, systems development Computer / data center operations and managing security at database, network and application layers IT Security Analyst Verizon Wireless August 2012 to May 2013 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) Assist System

Owners and ISSO in preparing certification and Accreditation package for companies IT systems, making sure that management, operational and technical security controls adhere to a formal and well-established security requirement authorized by NIST SP 800-53 Designate systems and categorize its C.I.A using FIPS 199 and NIST SP 800-60 Conduct Self-Annual Assessment (NIST SP 800-53A) Perform Vulnerability Assessment. Make sure that risks are assessed, evaluated and a proper actions have been taken to limit their impact on the Information and Information Systems Created standard templates for required security assessment and authorization documents, including risk assessments, security plans, security assessment plans and reports, contingency plans, and security authorization packages Conducted I.T controls risk assessments that included reviewing organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard C&A Analyst Foreground Security March 2009 to July 2012 Analyzing and defining security requirements for a variety of IT issues. Designing, developing and implementing solutions to IT security requirements at various levels of the agency's System Development Life Cycle (SDLC) through the Program Manager. Gathering, analyzing and organizing technical information about systems, existing security products and ongoing programs. Running intrusion detection and protection (IDS/IPS) using specialized tools Performing forensics analysis. Performing risk analysis that also include risk assessments. Developing, analyzing and implementing security specifications in line with NIST, FISMA etc. Performing vulnerability checks on desktop computers. Running security checks on laptops and PDAs before and after overseas travels by personnel. IT support to students and faculty DESKTOP SUPPORT January 2008 to February 2009 01/2008-2/2009 Handle technical troubleshooting with an enterprise environment including systems crashes, slow-downs and data recoveries Engage and track priority issues with responsibility for the timely documentation, and escalation Provide information and/or technical assistance to users concerning the development and maintenance of the computer network or for resolution of special problems Earn recommendation for teamwork, flexibility and work excellence in providing IT support to students and faculty Technology Summary Security Technologies: Retina Network

Security Scanner, Nessus Nmap, Nsat, Csam, Anti-Virus Tools Systems: Unix-Based Systems, Windows 9X/NT/2000/XP Networking: LANs, WANs, VPNs, Cisco Routers/Switches, Firewalls, TCP/IP Software: MS Office (Word, Excel, PowerPoint, Access, Outlook) Education University of Ghana Additional Information Perform Certification and Accreditation documentation in compliance with company standards Develop, review and evaluated System Security Plan based NIST Special Publications Perform comprehensive assessments and write reviews of management, operational and technical security controls for audited applications and information systems Develop and conduct ST&E (Security Test and Evaluation) according to NIST SP 800-53A and NIST SP 800-53R4 In depth knowledge of COOP, COSO and COBIT Frameworks Compile data to complete Residual Risk Report and to insert contents into the POA&M Ability to multi-task, work independently and as part of a team Strong analytical and quantitative skills * Effective interpersonal and verbal/written communication skills Key Skills Network & System Security Risk Management Authentication and Access Control Vulnerability Assessment System Monitoring & Regulatory Compliance

Name: Frederick Scott

Email: kellyjones@example.org

Phone: +1-301-709-1176x705