Senior IT Security Analyst Senior IT Security Analyst Senior IT Security Analyst - Invincea Philadelphia, PA Work Experience Senior IT Security Analyst Invincea - Fairfax, VA May 2016 to Present * Developed, reviewed and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices. * Performed vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple asset across the enterprise network. * Updated IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. * Performed risk assessments, help review and update, Plans of Action and Milestones (POA&M), Security Control Assessments. * (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). * Monitored controls post authorization to ensure constant compliance with the security requirements * Conduct Self-Annual Assessment based on NIST SP 800-53A * Document findings within Requirements Traceability Matrix (RTMs) and Security Assessment Reports (SARs). * Review and analyze Nessus Vulnerability and Compliance scans, WebInspect scans, IBM Guardian, Burp Suite and DbProtect scans for possible remediation. * Assess systems of varying scope and complexity and comprised of various technologies. * Create 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 * Provide weekly status reports on ongoing tasks and deliverables IT Security Analyst Aspect Security, Inc Group - Columbia, MD June 2013 to May 2016 * Assisted in conducting cloud system assessments * Worked in a SOC environment, where I assisted in documenting and reporting vulnerabilities (Tier 1). * Helped in updating IT security policies, procedures, standards and guidelines according to department and federal requirements * Worked with client in safeguarding CUIs by performing the necessary assessments which primarily deals with 14 control families. * Support Cyber Security analyst in conducting Vulnerability Management, Security Engineering, Certification and Accreditation, and Computer Network Defense. * Perform risk assessments, update and review System Security Plans (SSP) using NIST 800-18 (Guide for Developing Security Plans for federal

information systems) Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration * Creating Plan of Actions and Milestones (POAMs) for review and approval by the Authorizing Official (AO) formerly known as Designated Approving Authority (DAA). * Responsible for conducting analysis of security incidents. Perform investigations of unauthorized disclosure of PII. Responsible for reporting findings and provide status to senior leadership. * Perform vulnerabilities scan and monitor continuously using NIST 800-137 as a guide with the aid of Nessus Junior IT Security Analyst XO communications - Rockville, MD February 2012 to June 2013 * Developed, reviewed and updated Information Security System Policies, established security baselines in accordance with NIST, FISMA, FIPS, and industry best security practices. * Performed vulnerability scanning with the support of Nessus scanning tool to detect potential risks on a single or multiple asset across the enterprise network. * Updated IT security policies, procedures, standards, and guidelines per the respective department and federal requirements. * Performed risk assessments, help review and update, Plans of Action and Milestones (POA&M), Security Control Assessments, Configuration Management Plans (CMP), Contingency Plans (CP), Incident Response Plans (IRP), and other tasks and specific security documentation. (SA&A) Security Assessment and Authorization using NIST SP 800-53 rev4/FIPS 200 (Security Controls), NIST SP 800-53A rev4 (Assessing Security Controls). Alarm Monitor/ Junior cybersecurity analyst Paragon Security Systems - Arlington, VA December 2009 to February 2012 * Assisted team with security control assessments utilizinf NIST 800-53a * Assisted the SOC team in documenting and reporting vulnerabilities by utilizing tools such as Splunk and SNORT. * Developed security reports and presented to supervisors as needed. * Participated in sensitive briefings on security issues and classified information. * Alarm Monitor: (telephone /base station radio/handheld radio) * Monitor all alarms generated, dispatch appropriate rover to investigate any alarms generated due to unknown cause, report to rovers of all appropriate actions to ensure the security of the door or room. * Log alarms in the security log. * Installs, configures, and troubleshoots personal computer hardware components. * Provides technical support for Information Services customers. * Installs and configures software components including operating systems and client applications. * Documents,

maintains, tags, inventories, upgrades, or replaces hardware and software systems. * Searched and reviewed scientific and technical journal articles daily to ensure that quality and data meet Patent Examiner standards. * Provided an accurate count of the number of documents reviewed weekly. * Ensured weekly delivery deadline and/or assignments as directed by manager were achieved Education High School Diploma Northeast High School - Philadelphia, PA 2004 to 2008 Skills NESSUS (6 years), NIST (8 years), SPLUNK (2 years), AUTHENTICATION, SCANNING (3 years), It Security, Cyber Security, Information Security, Compliance, Comptia Certifications/Licenses CompTIA Cyber Security Additional Information Skills summary: FIPS 199, FIPS 200, NIST 800-53 Rev4, NIST 800-30, NIST 800-37, NIST 800-39 E-Authentication, Privacy Threshold Analysis (PTA), Privacy Impact Assessment (PIA), Risk Assessment (RA), SSP, ISCP, ST&E SAR, Plans of Action and Milestones (POA&M), Authorization to Operate (ATO) Letter Nessus Vulnerability Scanning Tool WebInspect Splunk DbProtect

Name: Kelly Hubbard

Email: taragarcia@example.com

Phone: 001-732-318-9630