Information System Security Officer Information System Security Officer Information System Security Officer - ICE/DHS Washington, DC Authorized to work in the US for any employer Work Experience Information System Security Officer ICE/DHS November 2016 to Present Working alongside System Owners, ISSMs, and a team of system Engineers to uphold the best information security practices for DHS/ICE Systems. Familiarity and the use of the various security tools like XACTA(IACS) and ARCHER (CDMT) to facilitate various security activities and records. Supporting System owners on various system security activities and documentations including the creation of POA&Ms to track security risks, vulnerabilities and remediation actions, drafting of risk acceptance memos, and waivers. Responsible for the preparation of systems and systems' documentation and artifacts in preparation for the annual system assessment. Responsible for the monthly testing of the due security controls in support of the Ongoing Authorization of the system. Responsible for system scan request and system scan result analysis to support various projects, remediation efforts and to support the systems' quarterly scan. Maintenance, review and updating of the SSP, and the various system documentations. Information Security Analyst USPTO March 2016 to October 2016 Working alongside system Technical Leads to maintain and uphold best information security practices for USPTO systems. Responsible for the maintenance, review and updating of the SSP, and assessment documents (SAR, RAR, SRTM, CSAM) Collaborating with the technical Leads to prepare the system for assessment, and collection of the artifacts to support USPTO annual system security assessment. Responsible for the review of the artifacts used to support system security assessment. Participating in the conduction of risk assessment and analysis. Responsible for system scan request and system scan result analysis to support various USPTO projects, and to support the quarterly scan. Developing and reviewing of USPTO system Security Impact Analysis (SIA) and documentation support changes to the USPTO systems. Supporting System owners on various system security activities and documentations including the creation of POA&Ms to track security risks, vulnerabilities and remediation actions, drafting of risk acceptance memos, and POA&M extension request. Security Compliance Analyst Vital Networks INC February 2014 to February 2016 Responsible for conducting security assessment reviews,

interviews, and test to determine the Security posture of the System and to develop a Security Assessment Report (SAR) in the completion of the Security Test and Evaluation (ST&E) questionnaire using NIST SP 800-53A required to maintain company Authorization To Operate (ATO), the Risk Assessment, System Security Plans (SSP), and System Categorization. Performing information security risk assessments and assist with the internal auditing of information security processes. Assessed threats, risks, and vulnerabilities from emerging security issues and also identified mitigation requirements. Conducting security scan on systems using vulnerability scanning tools; Tenable Nessus, and Analyzing the security reports for security vulnerabilities in accordance with the organization continuous monitoring plan and NIST SP 800-137. Providing recommendations in findings with selection and implementation of controls that apply security protections to systems, processes, and information resources using the NIST family of security controls. Working with the Support and Security coordination team to ensure compliance with security processes and controls. Responsible for developing Security Authorization documents and also ensures System Security Plan, Security Assessment Plan, Plan of Action and Milestones (POA&M), Contingency Planning and artifacts are maintained and updated in accordance with NIST guidelines. Validating remediated vulnerabilities. Information Security Analyst VINDS Incorporated, MD December 2011 to January 2014 Ensured all systems are operated, maintained, and information is disposed in accordance with VINDS internal security policies. Conducted users training to ensure systems security and increase user awareness. Responsible for weekly review of security logs and vulnerability scans on Operating Systems, Databases, Applications and developed Plan of Action and Milestone (POA&M). Identified, respond to, and report security violations and incidents as encountered to ensure that senior management is kept apprised of all pertinent security systems issues. Assisted with the development and updating of VINDS security policies. Performed compliance Map and Gap Analysis on VINDS systems. Conducted Risk Assessment on all VINDS system changes. Assisted in daily administration of security controls, compliance, monitoring and enforcement program. Participated in the CCB change, configuration, and release management process to ensure an appropriate security level is in the systems

lifecycles. Ensured security logs and audit trails are reviewed in accordance with established schedules and procedure. IT Support Specialist Lolubyte Consulting April 2009 to November 2011 Performed software/Hardware installation, Maintenance, repair, Update and testing. Installed and configured Microsoft Office on multiple machines. Configured and implemented network interface for windows Network. Troubleshoot and resolved TCP/IP connectivity problems. Provided base level IT supports to both internal and external customers. Logged all complaints and inform customers about issue resolution progress. Responsible for assigning issues to appropriate support group for thorough support and prompt resolution. Executed test scripts and document results. Responsible for defect logs and verify defect fixes. Supported users having data and network connectivity issue. Monitored network performance and troubleshoot problem areas as needed. Responsible for the Installation, configuration and troubleshooting of software. Cross-trained and provided back-up for other IT support representatives when needed. Education B. Eng. in Eng Federal University of Technology Minna 2005 Skills information security (5 years), risk assessment (4 years), SAR (2 years), Security (6 years), System Security (3 years) Additional Information SKILLS AND COMPETENCIES Broad knowledge of Microsoft Windows and LINUX platforms. Vast knowledge in all aspects of Security Authorization and Continuous Monitoring process using National Institute of Standard Publications 800-30, 800-37 Rev 1, 800-60, 800-53 Rev- 3 & 4, FIPS 199 FIPS 200, OMB A-130 App. III. Good knowledge of Federal Information Processing Standards (FIPS) 199 System Categorization, System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR), Risk Assessment (Impact Analysis), Continuous Monitoring and the Plan of Action & Milestone (POAM). Broad knowledge of Information Security Risk Assessments, Implementation of Controls, Security Infrastructures and the entire Risk Management Framework. Proficient in the use of Vulnerability Scanning tools such as (Retina Web Security Scanner, Retina Network Security Scanner, DBProtect, Tenable Nessus) and analyzes security reports for security vulnerabilities. Proficient in working with Protocols such as TCP/IP, HTTP and LAN/WAN. Active Directory and Exchange User Management expert. Microsoft Office expert (MS Word, MS Excel, Outlook and PowerPoint) with excellent

communication and writing skills.

Name: Jessica Rogers

Email: cindyhughes@example.com

Phone: 456-368-1130x1725