IT Security Analyst IT Security Analyst IT Security Analyst - Department of Labor Prosper, TX Authorized to work in the US for any employer Work Experience IT Security Analyst Department of Labor - Washington, DC May 2016 to Present Created and updated the following Security Assessment and Authorization (SA&A) artifacts; FIPS 199, Security Test and Evaluations (ST&Es), Risk assessments (RAs), Threshold Analysis (PTA), Privacy Impact Analysis (PIA), E-Authentication, Contingency Plan, Plan of Action and Milestones (POAMs) ? Conducted IT controls risk assessments (NIST 800-53A) including reviewing organizational policies, standards and procedures and providing advice on their adequacy, accuracy and compliance with NIST standards ? Managed and coordinated Plan of Action and Milestone (POA&Ms) for DSS accredited approved classified systems. ? Prepare and review Authorization to Operate (ATO) packages (i.e. SSP, RA, CMP, ISCP, DRP, IRP and PIA) for various systems ? Assisted business units with understanding the risks associated with using a particular vendor and recommending solutions to reduce or eliminate risk. ? Prepared written reports after the completion of the assessment ? Categorized systems based on SP -800-60 in order to select the appropriate NIST recommended control SP 800-53. ? Developed, reviewed and updated Information Security System Policies and System Security Plans (SSP) in accordance with NIST, FISMA and industry best security practices. ? Performed Assessment and Authorization in compliance with FISMA/NIST Standards. ? Identified vulnerabilities, recommend corrective measures and ensure the adequacy of existing information security controls ? Reviewed and conducted audits to ensure information systems maintained the compliance baseline. ? Reviewed system-level documentation to ensure system security requirements, including SA&A is incorporated. ? Participated in the development and/or review of System Security Plans (SSP). ? Liaised with ISSO to update POA&M and to ensure that all findings from the SAR are entered into the POA&M to be remediated. ? Coordinated with appropriate personnel to run vulnerability scans on a regular basis and ensure timely remediation actions. ? Reviewed, analyzed, and researched scan findings and coordinated remediation efforts in a timely fashion. ? Liaised with audit team to investigate and respond to Financial and/or IG Audits. ? Performed IT risk assessment and document the system security keys controls. ? Reviewed and revised System Security Plan (SSP), System Security test and Evaluation (ST&E) Risk Assessment (RA), Privacy Impact Assessment (PIA), and the Plan Of Actions and Milestones (POA&M) IT Security Analyst DOE - Washington, DC June 2012 to April 2016 Reviewed security logs to ensure compliance with policies and procedures and identifies potential anomalies ? Develop and maintain C&A documentations, including System Security Plans, Contingency Plans, Risk Assessment Reports and evaluated existing documents and their accuracy ? Experience in using security policies, standards, procedures, guidelines, and best practices from areas such as FISMA and NIST ? Update IT security policies, procedures, standards, and guidelines according to private and federal requirements. ? Develop and/or maintain POA&Ms for all accepted risks upon completion of system SCA, including the utilization of waivers/exceptions where appropriate ? Create remediation strategies for weaknesses based on priorities ? Review and update FIPS 199 (SP 800-60), Initial Risk Assessment (SP 800-37), E-Authentication, PTA, PIA, ST&E, POAM as part of the Security Assessment and Authorization (SA&A). ? Prepare Security Assessment and Authorization (SA&A) packages to ascertain that management, operational and technical security controls adhere to NIST SP 800-53 standards. ? Provide review and progress reports of all Plan of Action and Milestones (POA&M) ? Coordinate with System administrators to provide fixes for vulnerabilities identified in systems. ? Analyze organizational information security policy needs based on stakeholder interactions, develop and publish policy, standards, security handbook, and procedures for implementation ensuring alignment with NIST 800-53 Rev 4 Technical Support (Contractor) Maytag - Fairfax, VA September 2011 to May 2012 Installed software and resolved technical issues ? Displayed courtesy and strong interpersonal skills with all customer interactions ? Resolved customer complaints and concerns with strong verbal and negotiation skills ? Resolved Remedy tickets on a daily basis ? Coordinated with other IT groups for remediation of complex issues Education Business Administration University of Ghana - Accra, GH May 2010 Skills SECURITY (5 years), AUTHENTICATION (5 years), FEDERAL INFORMATION SECURITY MANAGEMENT ACT (5 years), FISMA (5 years), NIST (5 years), It Security Certifications/Licenses CompTIA Security+ AWS cloud Additional Information Core Skills ? Detailed knowledge of security tools, technologies and best practices with more emphasis on Sarbanes-Oxley 404, COSO, COBIT, PCI-DSS, HIPAA, SAS-70, SSAE 16 and ISO 27001/2. ? Over five years of experience in system security monitoring, auditing and evaluation, C&A and Risk Assessment of GSS (General Support Systems) and MA (Major Applications). ? Performed Certification and Accreditation documentation in compliance with company standards ? Developed, reviewed and evaluated System Security Plan based NIST Special Publications ? Performed 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 ? Compiled 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 ? Security Life Cycle and Vulnerability Management, using FISMA and applicable NIST standards.   Technical skills Security Technologies: Retina Network Security Scanner, Nessus, Anti-Virus Tools, Web Inspect, Nessus, Systems: Unix-Based Systems, Windows 9X/NT/2000/XP, Networking: LANs, WANs, VPNs, Routers/Switches, Firewalls, TCP/IP Software/Artifacts: MS Office (Word, Excel, PowerPoint, Access, Outlook), MS Project, CSAM, FIPS 199, SORN, E-Authentication, PTA, PIA, RA, SSP, CP, CIPT, ST&E, SAR, POA&M, ATO, 800-53A, ISA, MOU, CSAM.

Name: Danielle Cook

Email: haydenmelissa@example.com

Phone: 383.352.7941x9972