Cyber Security Analyst Cyber Security Analyst IT Security Waldorf, MD WORK AUTHORIZATION: U S CITIZEN. CLEARANCE: SECRET A self-motivated and passionate analytic person with excellent communication skills who combines professional and interpersonal skills to accomplish the mission, vision and the goal of organization. Ability to motivate, lead, and work with a team in IT Security. Seeking to utilize background and experience within a progressive and responsible position, attention to detail, passion for excellence to enhance the confidentiality, integrity and availability of the information system Over 5 years of IT Security experience Authorized to work in the US for any employer Work Experience Cyber Security Analyst Datalogic Solution Ashburn VA - Ashburn, VA August 2016 to Present Duties included: ? Performed Security Categorization (FIPS 199), Privacy Threshold Analysis (PTA), E-Authentication with business owners and selected stakeholders ? Documenting and reviewing security plans (SP), contingency plans (CP), contingency plan tests (CPT), privacy impact assessments (PIA), and risk assessment (RA) documents per NIST 800 guidelines for various government agencies. ? Supporting client and creating findings as part of POA&M remediation efforts ? Reviewing of security and privacy compliance aspects of Cloud Customer contracts and inquiries ? reviewing cloud security control documentation ? Reviewing ATO package completed with FedRAMP template and the 3PAO that perform the assessment ? Work with business process owners to ensure timely identification and remediation of jointly ? owned risk related issues and action plans. ? Use McAfee DLP Manager to protect intellectual property and ensures compliance by safeguarding sensitive data. ? Ensure customers are in compliance with security policies and procedures following NIST 800-53 and NIST 800-53A ? Reviewing and updating ATO package documents such as SSP, SAR, POA&M, IR, MOU, ISA, SAP, DRP, BIA, PTA, RA, ISCP, CPT ? Review audit logs and provide documentation guidelines to business process owners and management ? Conduct Risk Assessments regularly, ensured measures raised in assessments were implemented in accordance with risk profile, and root-causes of risks were fully addressed following NIST 800-30 and NIST 800-37. ? Description of the items found during the investigation while researching the events (DLP) ? Assist in establishing an Ongoing Authorization (OA) program design to review the security posture of designated systems

on a continual basis ? Provide input to management on appropriate FIPS 199 impact level designations and identify appropriate security controls based on characterization of the general support system or major applications ? Perform comprehensive Security Control Assessment (SCA) and prepare report on management, operational and technical security controls for audited applications and information systems ? Conducting Risk Assessment (RA) and completing Risk Management Framework (RMF) process to obtain ATO. Use upper case ? Perform vulnerability scanning and penetration testing in accordance with NIST 800-115, using tools like Nessus, Web Inspect and Found stone. ? Perform specific quality control for packages validation of Risk Assessment, (RA), FIPS-199 Categorization, PTA, PIA, SORN, E-authentication ? Assist in developing NIST Compliant vulnerability assessments, technical documentation, and Plans of Action and Milestone (POA&M), and address system weaknesses ? Documenting and reviewing System Security Plan (SSP), Security Assessment Plan, Requirements Traceability Matrix (RTM), Security Assessment Report (SAR), Plan of Action and Milestones (POA&M), Authorization letter/memorandum (ATO). ? Creating and updating POA&M to track and correct audit findings using tools like Trusted Agent FISMA (TAF) and CSAM. IT Security Analyst Virginia state Mental Health Department June 2013 to July 2016 Duties include: ? Performed data gathering techniques (e.g. questionnaires, interviews and document reviews) in preparation for assembling C&A/A&A packages. ? Worked with Certification and Accreditation team; performed risk assessment; updated System Security Plan (SSP), contingency plan (CP), Privacy Impact Assessment (PIA), and Plan of Actions and Milestones (POA&M) ? Updated Plan of Action & Milestones (POA&M) and Risk Assessment based on findings assessed through monthly updates. ? Creating, updating and reviewing System Security Plans using NIST 800-18, Contingency Plans using NIST 800-34, Incident Reports using NIST 800-61 ? Supported client in creating memos for POA&M that past schedule completion date (SCD). ? Conducted assessment of controls on Information Systems by interviewing, examining and testing methods using NIST SP 800-53A as a guide ? Maintain inventory of all information security system assigned ? Supported client in creating SOP (Standards Operating Procedures) as part of POA&M remediation. ? Updated Plan of Action & Milestones

(POA&M) and Risk Assessment based on findings assessed through monthly updates. ? Developed NIST-compliant vulnerability assessments, technical documentation, and Plans of Action and Milestone (POA&M), and address system weaknesses ? Documented and review system security plan (SSP), security assessment report (SAR), security plan of action and milestone (POA&M) ? Provided guidance and training to the system owner and ISSO on the validation process. ? Ensured customers are in compliance with security policies and procedures following NIST 800-53 and NIST 800-53A ? Review technical control and provide implementation response as to if/how the system are currently meeting the requirement ? Review Technical, Operational and Management Security Controls and provided implementation responses as to if/how the Systems are currently meeting the requirements. ? Review organizational policies, standards and procedures and provided advice on their adequacy, accuracy and compliance with the Payment Card Industry Data Security Standard (PCI/DSS). ? Performed security categorization (FIPS 199), review and ensure privacy impact assessment (PIA) document after a positive PTA is created ? Documented and finalize Security Assessment Report (SAR) and communicate a consolidated risk management activities and deliverables calendar ? Assisting in conducting the Security Control Assessment meeting (SCA) Kick-off Meeting and populate the Requirements Traceability Matrix (RTM) according to NIST SP 800-53A. ? Developed and conduct ST&E (Security Test and Evaluation) according to NIST SP 800-53A and perform on-site security testing using vulnerability scanning tools such as Nessus ? Checked Security controls implementation for compliance with FedRAMP and Cloud services - SaaS, PaaS, and IaaS Education BSc in Computer Science in Computer Science University of Sierra Leone 2007 Skills DLP (3 years), Nessus (6 years), Payment Card Industry (3 years), PCI (3 years), Security (6 years), testing, HTML, Cisco, access, Active Directory Additional Information ? Experienced in the development of System Security Plans (SSP), Contingency Plans, Disaster Recovery Plans, Incident Response Plans/Training, and Configuration Management. ? Plans, System Security Checklists, Privacy Impact Assessments, POA&M, ? Familiar with VMware and other Virtual Machine Applications ? Good communication and writing skills ? Experience with Data loss prevention (DLP) Symantec. ? Experience with Vulnerability Management ? Experience

working with Application Security Management. (ASM) ? Experience with Privileged Access Management. (PAM). ? Experience scripting. ? Proactively helping clients create Memos ? Hand -on experience with web gateway/proxy such as McAfee ? Experience working with Cisco FireEye, IronPort, Firepower, ArcSight, CyberArk ? Experience with CDM tools like BigFix, forescout. ? Experience with ISO 2700, 27001 ? Working knowledge of NIST 800-53, NIST RMF, FIPS and FISMA ? Experienced working with NIST SP 800-53 rev 3 and rev 4 ? Experience with ISO 2700, 27001 ? FISMA Reports, Standard Operating Procedures (SOP) as part of POA&M remediation ? Experienced with vulnerability scanning and penetration testing using tools like Nessus, WebInspect and Nextpose ? Experienced with Security Control Assessment and ATO packages ? Experience with reviewing security control ? Experience with Payment Card Industry Data Security Standards (PCI/DSS ? Experienced in Risk Management Frameworks (RMF) processes and compliance using NIST publications and standards ? Experience with FedRAMP and Cloud services ? Experience working with Splunk to Analyze Data ? Experience working with Oracle Database 11g and 12c ? Experience with Amazon Web Services (AWS) ? Experience working with Linux, Unix-Based Systems, Windows Operating system (ALL) Technical Skills: ? Software: MS Office (Word, Excel, Outlook, Access, PowerPoint) ? Security Technologies: Network Security Scanner; Nessus Security Center, IDS/IPS; Log Management, Anti-Virus Tools, McAfee, DLP, Splunk, CDM Tools like RES, BigFix, Forescout, FireEye, Cisco IronPort, Cisco Firepower, ArcSight, CyberArk, Privileged Access Management (PAM) Application Security Management (ASM) PCI/DSS ? Operating Systems: Unix-Based Systems (Solaris, Linux); Windows (all) ? Networking: LANs, VPNs, Routers, Firewalls, TCP/IP ? Ticket Systems: JIRA and Remedy (BMC)

Name: Vanessa Kaiser

Email: johnmelton@example.com

Phone: (413)854-4950