IT Specialist IT Specialist IT Specialist - Center for Disease Control and Prevention - Laulima Govt. Solutions Acworth, GA Work Experience IT Specialist Center for Disease Control and Prevention - Laulima Govt. Solutions - Atlanta, GA August 2017 to Present * Serve as the IT Security Specialist in the Office of Safety, and Asset Management (OSSAM). * Review, analyze, promote and provide technical and advisory functions to implement awareness of HHS enterprise-wide information technology (IT) security and/or system development life cycle (SDLC) policies and standards. * Provide technical assistance and advice on the overall establishment of information technology security policies, plans and programs. * Conduct risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs. * Evaluate systems policies, procedures and infrastructures to ensure information systems reliability and accessibility to prevent and defend unauthorized access to systems, networks and data. Computer Security Systems Analyst II Center for Disease Control and Prevention - Laulima Govt. Solutions - Smyrna, GA December 2015 to August 2017 * Serve as an advisor to the CGH Information System Security Officer (ISSO) on all matters relating to security vulnerabilities and threats to CDC computer systems. As a result, increasing the productivity line for all CDC Global Systems in compliance with NIST and FISMA from 7% to 100% compliance within 1 year of start date on the contract. This was a huge increase in productivity for the Global Systems Department at the CDC within its 5th year existence. * Initiated new/old systems converting them into the AWS FedRAMP environment. For example, Data Warehouse systems. Which also includes: System Security Plan (SSP), System Assessment Plan (SAP), System Assessment Report (SAR), and Plan of Actions and Milestones (POA&M). * Follow information security policies, methods, standards, Federal Information Security Management Act (FISMA)/National Institutes of Standard and Technology (NIST) standards and practices to organizational information systems, IT reference materials and interpret regulations. * Assessment Report (SAR), and Plan of Actions and Milestones (POA&M). * Ensure User Roles and Access Profiles are still appropriate for the services offered to customers, and the CDC as a contractor. This also includes file access management/access rights. * Assists in developing information security standards to ensure the confidentiality, availability and integrity of

information systems on large and small scale operating systems * Implement security controls, perform ongoing maintenance and prevent, detect, analyze, and respond to security incidents. * Conduct risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs. * Ensure security, continuity, and efficiency of automated data processing operations and work with CDC Centers/Institutes/Offices (CIOs) to identify the need for data and computer security. * Develop corresponding security countermeasures necessary to protect technical, complex, sensitive, and classified information processed on CDC computer equipment. * Participate in identification and analyses of CDC information security policy issues, deficiencies, and problem areas through review and analyses or reports, contacts, surveys, inspections, and facility reviews. * Serve as an agency technical authority for new and advanced computer security software affecting agency-wide systems. * Provide inspection results and reports to the ISSO in the form of briefing and formal reports. Computer Network Detection (CND) Analyst Defense Management Contracting Agency (DCMA) - ICF International - Smyrna, GA March 2014 to April 2017 * Provide network intrusion detection and monitoring, various intrusion detection tools related monitoring and correlation analysis * Execute, draft, edit, and maintain standard operating procedure (SOP) documentation. * Ensure User Roles and Access Profiles are still appropriate for the services offered to customers, and the CDC as a contractor. This also includes file access management/access rights. * Active Directory management of authorizing users roles/responsibilities onto the DCMA network. * Provide coordination of significant incidents to ensure proper analysis is performed and timely and accurate reporting of the incident is affected. * Provide, develop, and maintain a network forensic analysis capability to enhance response to, support of, and investigation into significant incidents to provide a clearer view of the exploits, vulnerabilities, and tactics, techniques, and procedures (TTPs) used to cause the incident. * Provide support for the NSOC's CND Analysis, Fusion, and Monitoring 24x7 support capability during non-core business hours consistent with CNDSP requirements as needed. * Coordinate with Incident Response, Cyber Threat Analyst, IAVM, various intrusion detection tools support operations, and CND Infrastructure. Information Security Engineer (Security Analyst II)

Defense Management Contracting Agency (DCMA) - ICF International - Atlanta, GA November 2014 to December 2015 * Perform assessments in scope of the certification and accreditation process. * Initiated new/old systems converting them into the AWS FedRAMP environment. For example, Data Warehouse systems. Which also includes: System Security Plan (SSP), System Assessment Plan (SAP), System Assessment Report (SAR), and Plan of Actions and Milestones (POA&M). * Ensure User Roles and Access Profiles are still appropriate for the services offered to customers, and the CDC as a contractor. This also includes file access management/access rights. * Develop and maintain a robust authorization security program that incorporates required security controls and best practices. * Maintain the Risk Management Framework, which incorporates identity management and vulnerability management. * Report to ISSO on ATO preparation packages, software validation (Level III), annual business continuity exercises and test, annual assessments, audits, and change management. * Serve as business continuity coordinator, perform business impact analysis to determine the acceptable system down time, and ensure systems never go beyond that threshold. * Maintain a software management program.Lead various projects to ensure timely delivery and that security is considered within the SDLC. Scan applications, code, and systems using AppScan and Nessus to identify vulnerabilities, and ensure remediation has taken place on unacceptable risks. Information System Security Analyst I Center for Disease Control and Prevention - SRA International, Inc - Atlanta, GA June 2014 to November 2014 * As a Cyber Security Analyst I support the Centers for Disease Control and Prevention (CDC) Certification and Accreditation (C&A) program in support of the Office of Chief Information Security Officer (OCISO). * Ensuring that federal computer systems have met the initial security requirements. Ensuring that federal systems are protected in the areas of Confidentiality, Availability, and Integrity; allowing the public to have access to vital public health information. * Ensuring that information systems are operating with appropriate management review, that ongoing security control monitoring occurs, and that re-accreditations take place periodically or when there is a significant change to an information system or its environment. Also ensuring that the C&A methodology closely adheres to the evolving standards of NIST SP 800-37 Rev 1 and that our clients remain fully FISMA-compliant. * Ensure

User Roles and Access Profiles are still appropriate for the services offered to customers, and the CDC as a contractor. This also includes file access management/access rights. * This is done by: Fostering cyber security awareness, and ensure necessary data protection and security controls are in place. * Effectively using the C&A data repository, work collaboratively with 6 other SRA Cyber Security Analysts and CDC staff and stakeholders to perform Certification and Accreditation activities. * Providing guidance and assistance to the stakeholders across the spectrum of C&A activities (e.g., analyzing vulnerability scanning results and POA&M development and management). * Reviewing C&A correspondence at least twice daily, and take appropriate actions including logging receipt of C&A packages, forward emails for action, and respond to requests; including self-assessments, confirmation that appropriate NIST and FIPS controls were tested, we will confirm that the necessary documentation is contained in the package (e.g., System Security Plans), and that the documentation is complete and accurate. * Collecting and update the C&A data repository, to ensure accurate daily, weekly and monthly status reporting. * Communicate regularly with stakeholders for updates on outstanding items. * Utilizing experience with use of Trusted Agent, to assist CDC with further implementation of the tool as practices evolve. Education MSIA in Cyber Security University of Maryland University College - Adelphi, MD BS in Business Administration Voorhees College - Denmark, SC Certification Central Michigan University - Mount Pleasant, MI Skills DLP, ISO, NIST (2 years), PCI, SNORT Additional Information Mr. Westbrook has over 7 years' experience working in the field of Information Systems Security in a DoD environment. He has several highly recognized IT Security certifications: CEH and Security+. Mr. Westbrook also has an inactive TS/SCI Top Secret Clearance, Secret Level Clearance, and Public Trust. Mr. Westbrook also has a Master of Science degree in Information Systems Management with a focus on Cyber Security. He served over 9 years in the U.S. Army (5) years serving as an Intelligence Analyst/Instructor. Mr. Westbrook is self-motivated with proven leadership skills. His IT background consists of: Security Risk Management Frameworks (NIST, FISMA, HIPPA and FIPS), Intrusion Detection/Prevention, DLP, Incident Response, Firewall analysis, suggestive rule tuning, and familiarity with computer forensics. Skills/Expertise * AWS Training (FedRAMP) compliance *

MS Office * Wireshark * HBSS * SourceFire * ArcGIS * Strong written/verbal communication * Knowledge of PCI DSS, HIPPA, ISO, NIST, and IT Controls * Snort * FireEye * Symantec DLP * CheckPoint * NetWitness * ForeScout * Proficient in Microsoft Office Suite (Word, Excel, Project, PowerPoint, Visio)

Name: Jasmine Sanchez

Email: kent21@example.net

Phone: (334)418-1674x4116