IT Security Engineer IT Security Engineer IT Security Engineer - EMCS LLC Upper Marlboro, MD IT Security Specialist with an exceptional ability to provide technical and policy related guidance regarding information security compliance, security events, managing and protecting enterprise information systems, network systems and operational processes through information assurance controls, compliance verifications, Risk Assessment, Vulnerability Assessment in accordance with NIST, FISMA, and industry best security practices Work Experience IT Security Engineer EMCS LLC - Suitland, MD November 2014 to Present Responsible for information security engineering in the network environment using in-depth understanding of access control, authentication and authorization, security auditing, and security configuration technologies. Perform IT Security Administration functions, including the administration, maintenance, and deletion of end user accounts, permissions, and access rights for network access, following established procedures. Maintain hardening of Operating Systems, applications, and network infrastructure using FISMA and related Security Technical Implementation Guides Develop, contribute to and implement internal Security Assessment Plan (SAP), Risk Assessment Report (RAR), System Security Plans (SSP)and other artifacts supporting system for Assessment and Authorization Coordinated with System Analysts, support staff, and vendor representatives to ensure DoD-Wide PKI DoD Instruction project execution and development met DoDI 8520.2, HSPD-12 and FIPS 201-1 policies, capabilities, and requirements. Conduct daily system integrity monitoring using Tripwire, Altiris, and Active Directory Designed, installed and Implemented Cisco Identity Service Engine across multiple back-up sites Ensure secure and robust infrastructure systems by analyzing, configuring and integrating firewall change requests into existing firewall policies and performing efficient troubleshooting. Perform security architecture review of the network and ensure that we are always ahead of potential threats through research, analysis and escalation of the syslog (Log Logic) reports from security and networking devices such as firewalls, routers, radius, TACACS and Kerberos servers Evaluate the effectiveness of security controls, and develop findings and remediation recommendations with Plan of Action and Milestones (POA&Ms) Perform Security Impact Assessment (SIA) for proposed system change requests Participate in the planning and updating of NOAA enterprise Business Continuity Plan and Disaster Recovery Plan. Perform vulnerability assessment and vulnerability remediation/mitigation research Have a hands-on role in building security solutions as well as improving existing security threat mitigation and response using SolarWinds Orion Suite and Palo Alto NGFW devices Work with the security Incident Response Team in various cases for DDoS mitigation, phishing attempts, black holing IPs, and implementing hot site failover exercises. Provide 24/7 support and document network security designs and Microsoft Visio diagrams Evaluate new security products, security audits, patch management implementation, configuration controls and as required, design security for current information systems. Monitor patch and security advisories releases and review and develop deployment plans Midwife yearly Security Control Assessment (SCA) exercises Implement security policy, processes, procedures, and guidance documentation Provide security guidance and ongoing research to drive infrastructure decisions in collaboration with other technical and management stakeholders to ensure security policies and principles are being upheld and addition of new and emerging security technologies that may benefit the security posture of strategic goals in compliance with established NIST policy and industry guidelines. Performs other security related duties as required. Strong organization, written and oral communication skills. Strong ability to function independently or as a part of a large, integrated cross-functional team. Intellectual curiosity and a willingness to learn new things Information Security Analyst Easylink Solutions LLC - Germantown, MD January 2012 to December 2014 Joined project team performing security assessments and providing consulting support to assist clients in meeting FISMA and FedRAMP requirements. Assist in daily administration of security controls, compliance, monitoring and enforcement program. Performed project security assessments. Developed Security Authorization Packages that are compliant with FedRAMP and DoD requirements under the supervision of senior staff members. Package components include: System Security Plans, Contingency Plans, Configuration Management Plans, Incident Response Plans, Privacy Impact Assessments, Security Assessment Plans, and Security Assessment Reports. Assisted in the review and analysis of Security Authorization Packages for completeness and compliance with

FedRAMP and DoD requirements. Participated in client interviews to complete Security Authorization Packages and Security Assessments Established schedules and deadlines for assessment activities. destruction. Partnered with other Security teams to conduct security risk assessments on new solutions and systems Worked with team to Prepare and submitted Security Assessment Plan (SAP) to CISO for approval. Developed and updated security plan, plan of action and milestone (POA&M). Prepared and reviewed documentation to include SSP, SAP, SAR, and POAM Packages Assist in daily administration of security controls, compliance, monitoring and enforcement program. Manage vulnerabilities with the aid of Nessus, Retina, and TAF scanners detecting potential risks on a single or multiple asset across the enterprise network Conduct kick-off meetings with customers and system stakeholders prior to assessment engagements to determine the security posture of the system Country IT Project Manager Online Integrated Solutions Inc - Rockville, MD February 2009 to November 2011 Responsible for ensuring timely and quality implementation of projects across the US as per the contribution agreement signed with the partner (work plan, guidelines, SOPs, deliverables). Organize debriefing sessions with the team and the stakeholder missions. Manage the Project's budget and ensure expenditures are forecasted, monitored and charged accordingly Ensure coordination between the office in Dubai, the contact center in Abuja and the main office in London Ensure all contracts are in place for the different service providers and contribute to making the necessary changes/amendments Ensure compliance for all HR, Admin, Finance, procurement and logistics Ensure changes occurring throughout the course of the project are incorporated and teams are briefed on new operation modalities Contribute to the development of the project's database and ensure all data is compiled and stored properly Liaise with the donor-government's representation (embassy), and if/when necessary with the host government. Contribute to the revisions of the contribution agreement and budget Represent OIS Americas at global collaborative sessions when requested by the GM/RPC Participate in country strategic reviews, linking with the project itself and any potential future program developments) of similar nature. Education Masters in Economic Development and Entrepreneurship University of Texas May 2015 Graduate Certificate in

Competitive Intelligence American Military University June 2012 Skills CISCO (3 years), FIREWALLS (3 years), SOLARWINDS (3 years), IPS (3 years), SECURITY (6 years) Additional Information Functional Areas of Expertise Information Systems Security Vulnerability Assessment Information Assurance Network Engineering Business Systems Analysis Security Life Cycle Systems Risk Assessment Systems Development Life Cycle Project Management Policy and Process Development Technical Skills SolarWinds NPM, NCM, NTA Orion Storage Resource and Server & Application Monitors Tenable Nessus Security Center Nipper Studio CSAM Itracks DCIM Cisco ACS and Identity Service Engine (ISE) Palo Alto Firewalls - PA5050 and PA5060 Cisco firewalls -ASA 5500 series and IPS Wireshark Tcpdump Juniper IDP 200,600, 800 and 8200 series

Name: Mark Cook

Email: zkelley@example.com

Phone: 001-391-510-6633x76190