Cyber Information Assurance Security Analyst Cyber Information Assurance Security Analyst Cyber Information Assurance Security Analyst - TMPC Riverview, FL Work Experience Cyber Information Assurance Security Analyst TMPC - Tampa, FL October 2018 to Present Performs assessment and authorization coordination. Advises and assists the customer with Risk Management Framework (RMF) and develops a Plan of Action and Milestones for resolving network compliance against controls listed in DODI 8500.2 and creating A&A packages. Performs assessment, compliance, and validation of IT systems to support the Cybersecurity program at USSOCOM, its Component Commands, TSOCs, and deployed forces. Execute a comprehensive assessment, compliance and validation of customer networks to ensure compliance with regulations and security and standards; to ensure the integrity of customer systems by identifying and mitigating potential shortcomings and vulnerabilities. Key Achievements: * Analyze, evaluate, and build an accreditation roadmap for new SIE networks and systems. * Develop and maintain supporting documentation for new networks, systems, and technologies as they are introduced into the SIE. * Perform risk and vulnerability assessments of IT and IS for accreditation; prepare risk assessment reports for submission to the Security Controls Assessor/Certification Authority (SCA/CA) and Authorizing Official/Designated Accrediting Authority (AO/DAA) in accordance with DoD, DIA, USCYBERCOM, USSOCOM, Component Command, TSOC, and deployed forces' policies, procedures, and regulations. * Coordinate with USCYBERCOM, DoD, DIA, NSA, DISA, and subordinate organizations to support the resolution of issues with security, A&A, connection approvals, and waiver requests. * Perform network security authorization, as well as the application and execution of policy, including project management support services. * Validate the patching of systems, perform validation scanning, develop Plans of Action & Milestone (POA&Ms), and report as directed by applicable policies, procedures, and regulations. * Develop and maintain an Information Security Continuous Monitoring (ISCM) Plan. This plan shall address ongoing awareness of information security, vulnerabilities, security controls, and threats to support organizational risk management decisions. * Develop and implement required processes, procedures, and capabilities to mitigate vulnerabilities and weaknesses for software and hardware deployment. Cyber Systems Engineer IV, Indications &

Warnings Analyst Perspecta - Chantilly, VA April 2018 to October 2018 Oversaw communications directed by the Cyber Security Operations Center (CSOC) and others. Apply Kill Chain analysis, Cyber Intelligence Preparation of the Environment (CIPE) modeling, in addition to diamond modeling of cyber threat activity. Analyze NRO threat activities and review threat intelligence and open source reports, in addition to documenting impacts to NRO operations and creating special reports and assessments. Conduct intelligence briefings and presentations, contribute to daily intelligence reports, web sites, and bulletins. Key Achievements: * Contributed to joint and combined military exercises, Federal Cyber Center (NCTOC, IC-SCC, Cyber Command, CNMF, CPT, JFHQ-Cyber, NCIJTF, DHS US Cert) or Corporate CIRT; performed NETFLOW or PCAP analysis; communicated as directed by CSOC leadership to a wide variety and number of organizations, as needed. * Created and communicated all-source integrated intelligence analysis to support DODIN and defensive cyberspace operations. * Performed analysis identifying indications of adversary activities and communicate warnings to leaders; evaluate international events, all-source and open-source intelligence, in addition to operational information required to assist the assessment of potential impacts to the DODIN and alert the JFHQ-DODIN staff and leadership of potential risks. * Utilizing web-based research tools, matched potential threat candidates with identified activity, created reports/briefs, constructing intelligence-derived recommendations to the watch floor for defense of affected network. * Advised leaders to proactively confront emerging challenges, leverage opportunities, avoid the unexpected, and produce strategic outcomes favorable to the US and allied interests. * Employed open source tools for tactical analysis of threats; gathered information and analyze malware to report technical indicators and TTPs. * Analyzed and delivered technical data to prioritize malware/threats and assist in detection methodologies and rules, in support of SOC and Incident Response Team. * Conducted research and evaluated technical and all-source intelligence, emphasizing network operations; analyzed network operations and cyber warfare tactics, techniques, and procedures aimed at threat to networked weapon platforms; analyzed network events identifying impact on current operations, conduct all-source research to determine advisory capability and intent. * Constructed assessments and cyber threat profiles of current

events, reflecting sophisticated collection, research and analysis of classified and open source information. * Combined and analyzed all-source information and intelligence to deliver quality intelligence products, papers, presentation, recommendations, and findings for senior intelligence and network operations officials. Cyber Systems Engineer III, Continuous Monitoring Team Lead Take2 Consulting, LLC - Chantilly, VA October 2017 to April 2018 10/2017 - 4/2018) Lead a team of personnel managing and ensuring enterprise cyber security and risk analysis for federal client, NRO, serving on Continuous Monitoring (ConMon) team. Regularly monitored enterprise cyber risk posture for real-time security posture awareness. Collaborated on development of monitoring strategies, procedures, policies, and tools; created and implemented Plans of Action and Milestones. Analyzed and monitor risk posture of key enterprise information systems; reviewed and maintained risk data and Risk Management Framework (RMF) activities in Xacta. Key Achievements: * Drove top notch product / systems alignment with NIST SP 800-27 and compliance with NIST SP 800-37, NIST SP 800-137, ISCM, and ICD503. * Developed documentation and updated procedures, policies, and processes; updated metrics and situational awareness presentations * Defined security control subset to form new / existing ConMon capabilities; reviewed relevant artifacts, ConMon Plans and Reports, privacy controls, and conduct impact analysis. * Leveraged Red Seal and EVSS ACS in RSA Archer to manage RMF activities and Body of Evidence (BOE). * Performed security control assessment for applications, infrastructure, and network; tracked plan of action and milestones (POA&M) vulnerability scan and security assessment findings. Information Assurance Officer U.S. Army - Fort Belvoir, VA December 2016 to October 2017 Advanced through progressively responsible, 9-year US Army tenure to spearhead enterprise network vulnerability assessments, performing security requirement analysis and validation to determine optimum security controls; utilized Assured Compliance Assessment Solution (ACAS) / Tenable Network Security methodologies. Assisted with Disaster Recovery (DR) and Continuity of Operations (CoP) planning; created audit reports and Plans of Action. Separated at the rank of Staff Sergeant (E-6). Key Achievements: * Led implementation of RMF; conducted Certification & Accreditation (C&A), System Assessment & Authorization (SA&A) as part of NIST SP

800-37 system and application accreditation. * Conducted cybersecurity testing and security control validation and assessment of technical and non-technical security features on systems and networks; advised the customer based on reports from vulnerability assessments. * Spearheaded comprehensive assessments of management, operational, and technical security controls to evaluate overall effectiveness of the controls. * Played integral role in security documentation - producing SSAAs, COOPs, and SOPs. * Performed assessment and authorization efforts in line with the NIST Risk Management Framework. * Conducted analysis, reviewed and validated cybersecurity documentation and technical controls. * Achieved career honors regarding the Joint Service Achievement Medal, 5 Army Achievement Medals, 5 Certificates of Achievement, and Military Outstanding Service Medal. Program Manager/Senior Information Security Specialist US Army, Camp Arifjan - KW December 2015 to December 2016 Served as Naval Base Direct Signal Support Team/ Seaport of Debarkation and Embarkation Program Manager for forward-deployed Theater Signal Company in Kuwait, performing hardware / software installation, issue resolution, technical training, and information security (INFOSEC) management. Provided technical support for Tier II devices. Key Achievements: * Managed approximately 20 contracted personnel and 15 Soldiers at multiple locations * As a subject matter expert (SME), developed from inception to conclusion project plans for moderately complex systems, in addition to implementing new procedures to reduce touch labor for INFOSEC initiative. * Oversaw project timeline and deliverables, ensuring timely delivery of all solutions. Identified emerging technology and defined use cases. * Managed inter-connected projects, and coordinated program activities. * Managed Program contractors and vendors. * Prepared reports for senior military leaders. * Constructed program plans with team leads to effectively manage deliverables. * Configured, managed, and generated reports for TACLANE-Micro (KG-175D) and TACLANE (KG-175G) encryptors; implemented keys and firmware. * Delivered technical guidance for security control compliance in Lifecycle Management (LCM). * Spearheaded team in conducting system analysis and evaluations, including preparing recommendations for improvements, optimization, development and/or maintenance efforts in the following disciplines: risk management, software life-cycle management,

telecommunications, automation, networking, and information systems architecture * Worked with customers in understanding operational protocols, including service cycles and equipment returns/replacements, upgrades/updates. * Consulted directly with vendors to validate resource availability and allocations. * Applied best practices in managing program and maintained accountability for program success. Program Manager/ Senior Information Security Supervisor US Army, White House Communications Agency - Washington, DC November 2011 to November 2015 Selected for high-profile support of secure / non-secure information systems, in addition to operational support and emergency response to military aids and senior White House staff for the President of the United States (POTUS), Vice President (VPOTUS), and First Lady (FLOTUS); Operated Mobile Communications Vehicle (MCV) for travel and maintained TACLANE encryptors, keys, and firmware. Earned Presidential Service Certificate / Award for outstanding support of POTUS. Key Achievements: * Presidential Emergency Relocation and Evacuation Program Manager: Managed and coordinated Emergency Relocation and Evacuation Program. ? Oversaw the development and implementation of Emergency actions for Senior Government Officials. ? Conducted research and developed security policies relevant to the environment; analyzed external threats relevant to national security. ? Developed plans, documented procedures and provided training materials based on program specifications. * Senior Information Security Supervisor / LAN Manager: Managed software contracts, overseeing adequate accountability of maintenance costs, related functions of license acquisitions, and purchase orders. ? Directed IT operations across client delivery, incident management, problem management, root cause analysis, and problem determination, supporting computers and mobile devices. ? Developed project documentation and user training materials according to the organizations specifications. ? Conducted research, evaluated, and made recommendations on emerging technology ? Oversaw, and evaluated the validation and accreditation processes. ? Analyzed systems and recommended mitigation measures relevant to information security vulnerabilities based on knowledge of the current security threats. ? Provided support on the development phases of information systems development life-cycle. ? Supported design, development and creation of information security policies; provided

support on information security activities including compliance inspections, audits and reviews. ? Reviewed and interpreted Federal guidelines, policies and industry best practices. * Presidential Emergency Operations Center Supervisor: Conducted communications security (COMSEC) for military aides and Presidential Response Officer. ? Maintained Presidential Emergency Operations Center communication systems and ensured COMSEC for military aides and Presidential Response Officer; activated, implemented, and monitored White House contingency programs. ? Conducted comprehensive assessments of management, operational security controls to determine the overall effectiveness of the controls. ? Conducted assessments of threats and vulnerabilities and recommended techniques and procedures for acceptable configurations. Information System Security Manager US Army, 43rd Signal Battalion - Heidelberg, DE 2009 to 2011 Germany IT Specialist Trainee US Army, Camp Arifjan - Fort Gordon, GA 2009 to 2009 Education Bachelor of Science in Information Systems Security in Digital Forensics American Military University Manassas - Manassas, VA May 2022 Associates Degree in General Studies in General Studies American Military University Manassas - Manassas, VA Skills Nist, Siem, Information Security, Cyber Security Links http://www.linkedin.com/in/darryl-dixon-9557b279 Military Service Branch: United States Army Rank: SSG Certifications/Licenses CISM May 2019 to January 2023 Security+ February 2018 to February 2021 Network+ February 2018 to February 2021

Name: Tara Wilson

Email: susan85@example.com

Phone: 527-551-3446