Information Systems Security Manager (ISSM) Information Systems Security Manager (ISSM) Circuit Enclave ISSM Oklahoma City, OK Authorized to work in the US for any employer Work Experience Information Systems Security Manager (ISSM) US Department of the Air Force - Tinker AFB, OK October 2018 to Present Information System Security Manager (ISSM) Routinely researches, interprets, analyzes, and applies Chairman Joint Chiefs of Staff (CJCS), Department of Defense (DOD), Committee on National Security Systems (CNSS), Air Force, National Institute of Science and Technology (NIST), and other national guidelines, policies, and regulations to integrate IA/Cybersecurity concepts into NIPR and SIPR circuit enclave plans, policies, procedures, and ensures guidance issued promotes correct and consistent application of laws, rules, and regulations across the enclaves Organizes, prepares, and assesses NIPR and SIPR enclave ATO packages on a cyclical basis as approved by the AO ensuring deadlines are adhered to, and generates and updates Plan of Action and Milestone (POA&M) items as necessary Coordinates and effectively communicates with applicable personnel in generating accurate assessments and monitoring activities of NIPR and SIPR circuit enclave ATO packages and provides timely and detailed information to base personnel on enclave information assurance efforts and requirements Implements continuous monitoring strategies on the Tinker NIPR and SIPR enclaves and coordinates monitoring activities in a cohesive manner with designated personnel and by tracking compliance of NIST 800-53A security controls using Defense Information Security Agency (DISA) Security Technical Implementation Guides (STIGs) and Assured Compliance Assessment Solution (ACAS) scans, as well as by coordinating routine inspections and assessments Cybersecurity Program Manager Effectively disseminates cybersecurity related information to base personnel ensuring a positive impact on the organization and/or improve quality of the mission and ensures interactions with internal and external officials and/or customers are diplomatic, convincing, professional, and promote effective working relationships Effectively ensures participation and outcomes of special projects resulting in positive impact on the organization and mission needs Conducts inspections on 31 base tenant units to assess compliance with cybersecurity policy and directives Manages 500+ Information Assurance Officers (IAO s) ensuring that they are properly

upholding the COMPUSEC program at the unit levels Manages system access control by verifying and safekeeping regulatory access control documentation to include DD Form 2875 and AF Form 4394 and provisioning and deprovisioning accounts for authorized users using NetIQ Directory and Resource Manager (DRA) and Information Assurance Officer (IAO) Express Creates security groups, organizational accounts and distribution lists and manages memberships of such through NetIQ DRA and IAO Express Vulnerability Analyst Rome Research Corporation - Tinker AFB, OK April 2018 to October 2018 Identified known vulnerabilities and compliance deviations of all networked clients using ACAS scans Ran SCAP scans on network to ensure system STIG compliance Developed and implemented approved security patches on networked clients using BCM Client Management, in accordance with NIST SP 800-70 to ensure compliance with Department of Defense cyber security standards to include DISA STIG s Coordinated development of automated software installs through BMC Client Management with software licensing managers and core server support to streamline vulnerability patches and compliance configurations. Production Analyst Maxcess International - Oklahoma City, OK July 2017 to April 2018 Participated in Kaizen Burst Event as a member of a five person core team. Identified defects in overall operations, to include security operations, and developed and implemented process improvement plans Identified the need for and developed department policies and procedures, where none previously existed, in accordance with International Organization for Standardization (ISO) framework which mitigated downtime generated by employee turnover IT Technician Carter Healthcare - Oklahoma City, OK April 2016 to September 2016 Managed group policies as well as the accounts of 1,000 end users through Microsoft Active Directory Mitigated device vulnerabilities in hardware and software applications by ensuring approved system updates and software patches were installed on workstations via Microsoft System Center Configuration Manager (SCCM) Imaged mobile workstations via the Microsoft Deployment Toolkit Provided hardware, software, and peripheral support to approximately 1,000 end users and resolved approximately 50 support tickets a week to include, but not limited to: network connectivity, OS boot errors, and hardware failures IT Technician OKC Zoo - Oklahoma City, OK December 2015 to June 2016 Participated in

overhaul of 200 IT systems during major software and hardware upgrade that consisted of workstations, point-of-sale systems and VoIP devices Improved the security posture by assisting with the implementation of new and strengthened network security policies configured through Barracuda Firewall and proxy settings Setup and configured new user workstations, meeting baseline security requirements, by installing and configuring the selected antivirus software suite Managed tickets for 300 end users and provided on-site support for issues regarding, but not limited to, network and VPN connectivity, printers and software applications Educated users on use of various hardware and software functions, including CCTV equipment Cyber Security Technician United States Air Force - Pittsburgh, PA September 2013 to November 2015 Administered NSA directed audits on Simple Key Loader (SKL) looking for indicators of compromise such as unauthorized login attempts or missing log files, ensuring confidentiality, integrity and availability (CIA) of cryptographic equipment Operated and maintained key distribution hardware, software and peripherals Distributed cryptographic key material using the data management device (DMD) Performed all necessary backups, system updates, reconciliations, and inventories IAW with applicable COMSEC instructions Restricted unauthorized access to cryptographic material by ensuring personnel maintained a valid security clearance and need-to-know Administrative Assistant US Navy - North Versailles, PA September 2009 to September 2013 Developed and maintained a records management program for official documents and personnel records, digitizing physical records and enforcing accountability and security of Privacy Act information Education Bachelors of Science in Cybersecurity Program Manager Western Governors University - Tinker AFB, OK October 2018 to Present Certifications/Licenses (ISC)2 SSCP CompTIA Security+ CE Driver's License

Name: Chad Bennett

Email: lancewhite@example.net

Phone: +1-990-594-2111