Cyber Security Analyst Cyber Security Analyst Cyber Security Analyst - Support Center Albuquerque, NM Work Experience Cyber Security Analyst Support Center - Albuquerque, NM August 2018 to Present management in the risk management process to: Identify the Center cyber footprint. Identify and understand the Center's cyber risks. Identify how the Center processes and uses unclassified but sensitive information (e.g., OUO, PII, ECI, UCNI, Sandia Proprietary). Identify how the Center processes and uses classified information. Maintain knowledge of cyber requirements within the Center and the Center's mission. Serve as the Center's liaison for Corporate Unclassified Information and PII requirements and can direct Center personnel to available resources: Corporate Dictionary for definition of PII. Corporate Policy IM100.2.5, Identify and Protect Unclassified Information, and IM 100.2.6, Control Personally Identifiable Information. Available Corporate Tools. COM100 Training. Participate in CSR Workgroup, CSO Senate, and Cyber related training. Communicate information regarding cyber security to Center management and/or the Center workforce as necessary. Be cognizant of any foreign national personnel working with, or within, the Center, as well as the rules regarding foreign national access to SNL cyber resources. Coordinate, prepare and maintain the Cyber Security Accreditation Agreement (CSAA) information in NWIS, in accordance with applicable Corporate and Cyber Security policies. Audits: Assist Cyber Security personnel and auditors with. Internal corporate inspections, surveys and audits. External inspections, surveys and audits. Cyber Security self-assessments and risk assessments. Information System Security Officer (ISSO) for classified stand-alone cyber systems within my center, coordinate, prepare and maintain cyber classified Standalone Systems Security plans. Refer Center management or line personnel to external organizations when applicable. Wing Cybersecurity Manager Air Force Global Strike Command - Kirtland AFB, NM January 2018 to August 2018 Conduct Information Assurance Vulnerabilities network security scanning using Assured Compliance Assessment Solution scan tool, ArcSight data security analytics and Host Based Security System to monitor/identify network and system vulnerabilities. Scan unclassified/classified servers, devices, and workstations on the networks to validate compliance in accordance with the information assurance vulnerability assessment program. Manage specialty filters, sensors and/or devices designed to monitor and/or counter specific threats. Coordinate and ensure continued compliance with applicable policy for the security, configuration, operation, maintenance, and installation of intrusion detection system, intrusion prevention systems, firewalls, virtual private networks, host-based security systems, scanning network and system management tools and anti-virus systems. Provide technical guidance support to leadership and unit information technology professionals. Review units and activity plans associated with certification and accreditation of its automated information systems using DoD Risk Management Framework, Enterprise Mission Assurance Support Service, Continuity of Operations Plan, and Disaster Recovery Plan. Prepare and coordinate project authorization documents, operational benefit statement, cost comparisons of alternatives, status reports, requirements documentation, risk analysis, and other technical documentation as required to fulfill network security compliance. Evaluate the security impact of system changes and provide recommendations/directions for networking initiatives. Provisioning of COMSEC services to USTRANSCOM customers. Management of day-to-day operations of an Operational COMSEC account. Perform all duties IAW applicable COMSEC policies Operate Key Management Infrastructure Management Client. Order and maintain COMSEC key material. Requests keying material for new missions and provide disposition instructions for keying material that is no longer required. Maintain 100% accountability of command's COMSEC material. Manage Cryptographic Modernization (Crypto Mod) program for the command. Manage the COMSEC Management System (CMS). Develop, coordinate, and execute USTRANSCOM COMSEC policy. Disseminate urgent, doctrinal, policy, and procedural COMSEC information. Scheduling and conducting Simple Key Loader audits. Familiarization with common cryptographic fill devices (Desired). Conduct COMSEC training. Develop COMSEC training program and administer training to users in the rules for use, safeguarding, controlling, and the proper destruction of COMSEC materials. Submit ad-hoc and recurring reports IAW suspense assigned by the Government (e.g. ad-hoc Practices Dangerous to Security (PDS), monthly Joint Training Information Management System (JTIMS), monthly Defense Readiness Reporting System (DRRS), etc.).

Conducts semiannual program reviews and inventories of assigned assets IAW COMSEC policy. Monitors, evaluates, and participates in exercise, system, and device evaluation; provide After Action Reviews (AARs) regarding COMSEC issues. Publish annexes and integrate command ICP program as required for support to Contingency Plans (CONPLANS) and Operation Plans (OPLANS). Help pass the Air Force Command COMSEC inspection. IT Support Technician II Abacus Technology Corporation - Kirtland AFB, NM December 2015 to January 2018 Created and deployed NIPR, SIPR, WESS, ESN, ESN Gateway, ConWrite, ABSS, ACES, AFBEAT, ARM, ATIMS, BQ, CCaR, CITOMS, CMS, CRIS, DTMS, EITDR, EMASS, EMASS SIPR, HMIRS, iRAPT, ITIPS and NATO secret enclave user account creations. Performed NIPR, SIPR, and WESS computer builds. As Primary Equipment Custodian Officer for the AFNWC organizations, managed, maintained, tracked and returned over 3,500 items on the "0065" account. Purchased all equipment and software within job requirements for the AFNWC organization. Acted as Primary Records custodian for AFNWC/ IT-S organization. As Secondary for the TCO program, helped maintain all DSN numbers on "S09" account with phone installs, disconnections and moves within the organization. As Secondary for the EMSEC program, helped maintain EMSEC specifications within the organization. As Secondary for the Verizon Wireless program, managed, maintained domestic and international plans for the AFNWC organizations, to include VIP personnel (e.g., General Morris). As Secondary for the USLM program, managed and maintained all software that is bought for the AFNWC organizations. Installed and tracked software divided out within the AFNWC ND, NT, and EN groups. Helped manage everyday IT issues within the AFNWC organizations via remedy system. Patched LAN drops for both NIPR, SIPR, WESS, and Comcast enclave on the switch. Performed touch maintenance on the WESS server. Created NIPR "U" drive creations. Helped set up the AFNWC ND and NT organizations network backbone infrastructure, and equipment installation. SIGNAL SUPPORT SYSTEM SPECIALIST US ARMY - Fort Carson, CO March 2013 to September 2015 Supervised and assisted users with battlefield signal support systems and terminal devices Performed installation, maintenance, and troubleshooting of battlefield support system and terminal devices Managed integration of Signal systems and networks Performed maintenance on authorized Signal equipment and associated electronic devices Trained users and provides technical assistance for Signal/COMSEC equipment Operated and performed prevention maintenance checks and service (PMCS) on assigned vehicles Held accountable for Communication equipment Maintain an up-to-date inventory record of the COMSEC material charged to the COMSEC Account, including COMSEC material issued to Local Elements and COMSEC Sub-accounts Limit access to inventory records to authorized personnel Ensure each segment of key is properly destroyed, and reported as destroyed, before reporting the destruction of the complete key; Ensure all copies of key issued to Local Elements and subordinate COMSEC Sub-accounts have been destroyed before destroying the key from which the copies were made Accurately verify the material being destroyed against the Destruction Report Destroy the material using approved destruction methods Establish and close COMSEC Sub-accounts, as deemed necessary, in accordance with the procedures described for opening and closing COMSEC Accounts Provide formal training and interim training for COMSEC Sub-account personnel Maintain a record of the inventory of all subordinate COMSEC Sub-accounts Maintain a file on other associated COMSEC Sub-account information Provide advice and guidance to Sub-account personnel relating to the management of their COMSEC Sub-account Conduct inventory reconciliation annually with each subordinate COMSEC Sub-account Audit COMSEC Sub-accounts at least every two years to ensure that records are accurate and control procedures are correctly applied Programming and local distribution of COMSEC devices to include but not limited to; Secure Telephone Equipment (STE), Sectera vIPer Universal Secure phone, and network encrypt or solutions (i.e. TACLANEs). Order, receipt, loading and management of COMSEC keying material using devices such as the Key Management Infrastructure (KMI) and Simple Key Loader (SKL) and other devices as necessary. Presented with two Army Achievement awards for outstanding work performance Education Bachelor of Business Administration in (BBA) General University of New Mexico - Albuquerque, NM January 2019 to Present Associate in Business in Business Central New Mexico Community College - Albuquerque, NM January 2017 to 2019 Associate of Applied Science in Network Systems

Administration in Network Systems Administration ITT Technical Institute - Albuquerque, NM September 2015 to September 2016 Skills Comptia, Nist, It Security, Cyber Security, Information Security, Linux, Network Security, Siem Military Service Branch: United States Army Rank: Specialist

Name: Stephen Garcia

Email: phillipskeith@example.org

Phone: 855-215-0224x358