

Computer Network Defense IT Analyst Computer Network Defense IT Analyst Independent Contractor - Primerica Financial Services Fredericksburg, VA Active Top Secret Clearance Work Experience Computer Network Defense IT Analyst U.S. Army Reserves May 2019 to Present

NCOIC in the Army Reserves providing IT support to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and information systems. Utilize tools to do automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery. Provide additional duties as required. Currently on a non-drilling (no monthly reporting) status (Individual Ready Reserves). Independent Contractor Primerica Financial Services November 2016 to Present

The mission of Primerica is to help families earn more income and become properly protected, debt free and financially independent. Primerica's clients are Main Street families. Our products and services are tailored to meet the needs of this demographic - the people who need us most. With approximately 5 million lives insured through our life companies, we represent hope to families and help them realize that, by buying term life insurance and investing the difference, they can create a better future. I assist families with debt elimination, retirement savings, education planning for their children, retirement savings protection, estate planning, wills and financial educational needs.

System Administrator/Information Assurance Security Officer HRTAX October 2001 to Present Seasonal- January thru April each year) Installed, configured, manage and maintain local area network (LAN) for the tax business. Provide customer support for the LAN to ensure network connectivity and access. Analyze and evaluate customer requests to provide technical assistance of information management. Troubleshoot problems; make diagnosis of what problem may be, communication interfaces, system software, and application problems. Initiate appropriate action to resolve the problems. Perform system administrative duties to ensure optimal functioning of all automation assets. Maintain software to insure compatibility between operating system, domains, file access methods and installed programs. Maintain control and access of shared resources on the network. Ensure system hardware maintenance, file backup and system security. Performed virus and vulnerability scans on network to ensure the security of the information was not compromised.

Computer Network Defense IT Analyst U.S. Army Reserves August 2015 to May 2016 Defense Information Systems Agency (DISA) NCOIC of Computer Network Defense Team providing support to Defense Information Systems Agency (DISA) Computer Network Defense (CND) to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and information systems. Utilize tools to do automated network vulnerability scanning, configuration assessment, application vulnerability scanning, device configuration assessment, and network discovery. Provide additional duties as required.

Information Assurance Engineer KForce November 2015 to April 2016 Telos Corporation/National Geospatial Intelligence Agency Perform Information Assurance activities supporting XACTA IA Manager Application suite for the National Geospatial Intelligence Agency (NGA). Responsible for supporting NGA in application administration, configuring, deploying, or troubleshooting a large enterprise deployment of XACTA IA Manager and implementation with dependent systems and processes. Utilize domain knowledge and collaborate with team leads, members and clients to translate functional needs into technical security solutions appropriately. Perform integration and configuration management of the XACTA IA Manager Product Suite. Interface with Security Authorization practitioners including the Authorizing Official, Information System Security Officers, System Owners and Engineers to assist with the development of the Security Authorization documentation packages. Interacts daily in person, via email and phone conversations with a large user base to providing user support to government XACTA IA Manager Software users. Document, track and report on user support provided. Strive to improve operational performance, streamline processes and work cooperatively/jointly to provide quality customer service. Perform system administrator functions in a Windows Environment. Perform other administrative support functions, as needed.

Owner Momma Louise's Cuisine, LLC August 2012 to October 2015 Momma Louise's Cuisine is a catering/vending service that serves southern comfort foods. Provided catering for weddings, parties, private dinners, sporting events, out-door events, and special occasions of all kinds. We pride ourselves on having fresh food, hence our slogan, "We Bring Our Kitchen To You." Having the mobile commercial kitchen custom built in a 20-foot trailer allowed us to prepare food on site and not have to be

concerned with on-site facilities. We allowed for special request, so were not limited to the types of foods we prepared. Sr. Information Technology Specialist (Cyber Detachment) U.S. Army Reserves May 2010 to August 2015 1st Information Operations (IO) Command RCIS Served as a member of the Computer Network Operations Team conducting world-wide, full spectrum cyber assessments at various echelons of Army, Joint, and Combatant Commands; responsible for training, planning, and operations support. Replicated an asymmetric opposing force using technical/ non-technical capabilities; exploits vulnerabilities to improve their defensive IO, Information Assurance & Computer Network Defense, and OPSEC posture. SMS Data Products, Deputy Lead Information Assurance Team May 2012 to February 2013 National Geospatial Intelligence Agency (NGA) Deputy Lead for the Information Assurance Team on a GDIT Contract managing the certification and accreditation of all existing and future systems in accordance with DCID 6/3 and transitioning to ICD 503 standards. Performed duties such as risk management, matrix reporting, testing, remediation, and management meetings. To assist team, performed duties as an Information System Security Engineer writing security documentation, attending/running registrations meetings, interacting with Program Managers on requirements for the systems, ensuring updates and remediation were performed on systems in order to ensure accreditation requirements were met. Other duties as necessary Information Assurance Officer SAIC March 2012 to May 2012 National Geospatial Intelligence Agency (NGA) Worked as a dedicated Information Assurance Officer for GeoEye (Enhanced View) managing certification and accreditation of all their existing and future systems. Determined functional needs and evaluate information security on systems. Helped the program to implement information security in accordance with the DCID 6/3 and ICD 503 standards and procedures. Reviewed all certification and accreditation paperwork identify that proper procedure for incident reporting, personnel access, system access and audit logging is properly in place. Reviewed the system design and architecture and ensure that the program adheres to the security requirements based on the analysis of the systems, users and resource requirements. Communicated with the Government and the program to discuss project activities and status. Ensured that risks are identified and managed properly utilizing a Plan of Action and Milestones

(POA&Ms). Performed six months review of the systems POA&M to ensure that vulnerabilities are managed and addressed regularly. Reviewed System Security Plans ensuring compliance with policies and regulations. Experience with both network and system certification and accreditation, doing security scans utilizing Retina, Gold Disk and various other scanning tools. Set up registration meeting in order to get the system registered and uploaded into the XACTA tool for tracking and approvals. Knowledgeable in the DCID 6/3, NISST, ICD 503 and various other policies and regulations required. Worked close with the DAA staff to meet all required standards and procedures to obtain accreditation of information systems. Experience as a Systems Administrator and Network Engineer maintaining various aspects of the network while working with the Corp of Engineers and the Department of the Navy. Security Guard (Unarmed) Inter-Con Security Systems - Newington, VA October 2010 to March 2012 Entrance Control - Operated and enforced a system of personnel identification; Performed roving patrols both inside and outside the locations in accordance with routes and schedules provided; Fixed Post at an entrance to the facility as well as monitoring closed-circuit television; Escort for designated visitors, personnel, and this can be from the facility to the parking garage or within the building; Traffic Control - directed pedestrian traffic; Ensured compliance with building rules and regulations; Maintained law and order; Received, issued and accounted for all emergency and special keys to the facilities. Sr. Systems Engineer/ Security Engineer NW-Systems June 2008 to September 2011 National Geospatial Intelligence Agency (NGA) Worked on a National Geospatial-Intelligence Agency (NGA) contract, assigned to the Mission System Transition Team in the Readiness Division. Worked on the Base Relocation and Closure (BRAC) project that was completed 15 September 2011. Ensured that 228+ systems go through the Certification and Accreditation Process in order to receive an Authority to Connect (ATC)/Authority to Operate (ATO) according to DCID 6/3, NIST, IC and DoD guidance in order to move to their new BRAC location of the ITC, NDC-W, CTI-E, MTL or NCE. Interface on a daily basis with the NSG-SIs, assigned to each system and provide any assistance and guidance necessary for the security of the systems. Review ECPs, Transition Plans, and RFCs to ensure that security requirements are met. Member of the Systems Integrity Team (SIT) where responsibilities

included sustaining integrity for the NGA Enterprise during migration of systems to their new BRAC locations. Ensured plans and processes were implemented and that support maintaining necessary end-to-end functional completeness and continued mission support capability as NGA-E systems is migrated to the NCE. Served as technical arm to the MST Engineering Review Board (ERB); participated in engineering change proposal and customer requirements template (CRT) reviews and validation; and coordinated NGA enterprise testing, accreditation, and readiness in support in NGA BRAC mandate. Certification Engineer SAIC August 2007 to May 2008 National Geospatial Intelligence Agency (NGA) Provided a conduit between the NGA Computer Security Division and the Program Office for all information technology issues like malicious code eradication, configuration management, and certification of current and future systems. Ensured that all NGA and contractor areas (CONUS and OCONUS) have met all DCID and DoD security standards for processing classified information on a data system (Sensitive Compartmented Information (SCI) and Collateral classified information). Familiar with NGA, NRO, IC information Systems architectures, Detected and prevented computer system security compromises in a networked environment, Understand COTS tools that can scan at the physical layer of all media types including but not limited to CDs, Hard Drives, floppies and Zip/Jaz, Experienced with utilization and interpretation of DITSCAP and DCID 6/3 in real world environments, strong ability to elicit, articulate and document information thoroughly, work independently. Provided Automated Information (AIS) security support addressing hardware, software, administrative/procedural, physical and communications, provided recommendations for accreditation of NGA systems processing SCI and collateral information, Prepared accreditation package supporting the accreditation process, assisted in system/technology analysis and assessment, testing and verification and validation, Utilized Gold Disk v2, Retina, SRR to scan systems for any vulnerabilities, prepare SCTR and forward packages for approval. Sr. Network Engineer L-3 Communications March 2007 to August 2007 Worked as a Liaison between the Information Assurance (IA) Team and the Network Team to Secure and obtain accreditation for a NIPRnet (Unclass) and a SIPRnet (Secret) Network. Ran Gold Disk v2 on all nodes, make manual fixes and print report of findings and mitigations taken. If exceptions are

needed, write exceptions according to the regulation for IA approval. Ran Retina scans and mitigates any vulnerability in the order of High, Medium and Low. Printed and maintained documentation on all findings for Network/IA team. Maintained WSUS for both networks and apply any updates necessary to Development, Staging and Production servers. Receive any new IAVA's and apply to servers and desktop machines as necessary. Kept Log Inventory on all machines in order to maintain the baseline, ran security software to ensure passwords meet standards and cannot be cracked, and ran DumpSec program to maintain state of nodes and baselines. Performed Network Administrator duties as the need arises. System Administrator/Information Assurance Security Officer Chugach Support Services May 2005 to January 2007 Worked as a Network Administrator supporting the Topographic Engineering Center at Ft. Belvoir, VA. Managed and maintain Helpdesk database for all client submitted issues. Planned and created user, group accounts and account policies, implement user rights, installed and configured Network Servers, printers, implemented data security procedures and performed backups, configured desktop, laptops, provided application support for Windows 2000/2003 servers, and applications servers. Created and modified Windows XP images for desktop and laptop computers resulting in quick installation of system baseline, trained and assisted new technicians with day-to-day technical operations. Managed and performed upgrades to system hardware and software components as required. Managed backups. Installed and test hardware and software. Managed and maintained all cryptology devices, pickup receipt key materials for KIV-7, KG175, KG94, and KG250 inventory and fill devices. Provided support and involvement in performance monitoring and reporting, problem identification, management and resolution. Maintained accountability for resolving service problems and prioritizing work requests. Managed system activity such as planning, installation, operation and maintenance. Coordinated flow of work between staff to ensure continuity. Consulted with management about persistent problems with infrastructure application or equipment performance. Developed and interpreted guidelines, policies, and regulations. Processed all required forms for personnel obtaining passwords for network access. Ensured all data output is properly screened and sanitized with appropriate security markings. Reviewed, investigated and provided input for

decisions and policies regarding information system security. Monitored all software, patches applied and modifications to the attached host computers, servers and workstations. As the organizations Information Assurance Security Officer, reviewed, and monitored compliance with policies, methods, and procedures pertaining to the Automation Information System Security Program (AISSP) for Automated Information Systems (AIS). Established and maintained automation security, including Network security. Prepared, distributed, and maintained plans, instructions, guidance, and standard operating procedures (SOPs) on the security of automated system operations, security procedures and protocols governing network operations. Reviewed threats and vulnerabilities to assess risk, and determine effective measures to minimize such risks. Identified resources to be protected. Performed vulnerability scans using various tools like Harris Stat, Retina, Hercules and IIS. Corrected infected systems using UPT software to wipe drives and re-build systems with baseline software. Division Secretary Topographic Engineering Center October 2000 to May 2005 Served as Division Secretary for the Division Chief, Topographic Systems Division and Branch Secretary for the Imagery Systems Branch. Performed and coordinated a wide range of management and administrative duties for the organization in regards to management, security, training, and budget for military and civilian personnel matters. Utilized knowledge of administrative regulations, procedures, and policy directives to provide advisory/technical services to management on information pertaining to reporting requirements, administrative procedures and regulatory compliance. Integrated with management to resolve complex and difficult administrative assignments as well as support problems. Utilized Corp of Engineers Financial Management System to support requests for travel, purchase requests, leave records, MIPR's and time and Attendance. Consolidated and managed tracking system of bi-weekly funds availability for labor prior to timekeeping submission. Reviewed budget requests, analyzed estimates and monitored the execution of operating budget. Worked close with Budget team to resolve problems with accounts. Served as training coordinator, maintain employee IDP's and request for training. Maintained filing system for Division Chief. Resolved resource management issues, utilized and maintained control over government credit card small purchases. Maintained reconciliation of

credit card billing statements. Originated, coordinated and supported visit access and requests with internal/external security offices. Proficient in Word, Excel, PowerPoint, Access, Outlook, Army Regional Tools, DCPDS (Modern) and Form Flow. Composed and reviewed correspondence insuring grammatical accuracy and spelling. Served as primary point of contact for information. Performed other duties as assigned. Education Certificate in Information Technology Specialist Dragon Academy January 2015 Master of Science in Information Assurance Stratford University 2013 Master of Science in Computer Information System Strayer University 2006 Bachelor of Science in Computer Networking Strayer University 2005 Skills DNS, SHAREPOINT, INFORMATION ASSURANCE, ACTIVE DIRECTORY Certifications/Licenses Series 6 Present Investment Company and Variable Contracts Products Representative Series 63 Present Uniform Securities Agent State Law Exam Series 26 Present Investment Company and Variable Contracts Products Principal Exam Pre-Paid Legal Present Life Insurance Licensed in Virginia, North Carolina and Florida Additional Information TECHNICAL SKILLS Installation/Configuration of Cisco 2900 Routers & Switches, Routing protocol (OSPF, RIP, EIGRP) configuration, DNS Server set-up, Exchange Server installation/configuration, PKI Implementation, Digital Encryption Devices, Active Directory, Firewall management, Anti-virus Client installation, Information Assurance measures, VLAN configuration, VOIP Configuration, Group Policy configuration, SharePoint installation/configuration, Network Administration.

Name: Keith Wilson

Email: patricia00@example.com

Phone: 611.604.2119x68112