Information Specialist Information Specialist IT Specialist Mountain View, HI Authorized to work in the US for any employer Work Experience Information Specialist US Army - Hilo, HI November 2018 to Present Process port allocation for incoming troops to have a network connection while they are on ground. Process contractors temporary or long term passes to access the base for contractual work. Desktop support and network printer configuration and installs. Cyber security. Run Vulnerability scans for non-army entities to help non-army entities to be current on patching vulnerable systems. IT Specialist Native Hawaiian Veterans November 2016 to November 2018 Pohakuloa Training Area Provides computer hardware, software, email, internet and networking support to include but not limited to: 1) troubleshooting and diagnosis of desktop, laptop, printers, digital senders, Blackberries/Smart Phones and peripheral hardware problems; 2) Installing and supporting licensed software, to include, but not limited to, Microsoft Office 2007, Outlook 2007, Internet Explorer, Norton and McAfee Anti-Virus, Adobe Acrobat Reader, Pure Edge, Lotus Notes, Defense Collaboration Online (DCO) and Cisco Virtual Private Network (VPN) and any subsequent software/client upgrades; 3) Troubleshooting and fixing email (to include Blackberry Enterprise email), internet access and networking issues. Contractor shall make initial contact with the customer within 4 duty hours of the submission of an IT work order ticket with the exception that Command Group calls are considered priority and touch labor shall occur within 2 hours. Touch labor shall occur within 2 working days of the submission of an IT work order request. Resolution or restoration of capability will be provided within 2 working days of engagement with the exception of problems pending end user response, and those referred to 30th Signal Battalion or vendor for resolution. Contractor shall proceed with repairs for equipment covered under the manufacturer's warrantee, and advise the Contracting Officer representative (COR) of repairs and replacements not covered under warrantee. USAG-HI will budget and fund for procurement of computer hardware/software needed for repairs and replacement, troubleshooting tools and equipment. USAG-HI staff and COR will input IT support requests in a work order database. Shall ensure 100% Information Assurance Vulnerability Alert (IAVA) and Army Gold Master (AGM) compliance for USAG-HI computers and laptops. Contractor shall apply software and security patches and perform

Army mandated AGM upgrades prior to deadlines established by USARPAC and/or Signal Commands. Major projects such as end mass migration of operating systems may require working outside normal duty hours to meet deadlines. Trusted Agent System Manager (TASM) for RAPIDS CAC Pin Reset computer. IT Specialist Apex Systems September 2016 to November 2016 Kona and Hilo Airports Working for TSA for Kona and Hilo Airports as the IT Specialist to Configure Windows 7 & 10 enterprise computers, desktop and laptops, Track deployment of computers and computer equipment deployment. Imaging computers. Troubleshoot, Repair and install network printers and various software. Dishwasher Volcano House March 2016 to May 2016 Wash dishes cooks and servers bring in from restraint customers. Clean area with cleaning solvents and other cleaning materials. Sweep and mop Refers and floors at the end of my shift. Monitor Technician Volcano House March 2016 to March 2016 Spoke with managers from each site of the Inventory of Wells Fargo buildings to find anything that has network connectivity to the internet or out to the public LAN. Physically walked around each area to find any connectivity, if any exists. Fill out the spreadsheet with the information I found at each location and uploaded the spreadsheet to a SharePoint location. This was a 1 day contract for each location, (Kailua-Kona and Hilo, Hawaii) 2 days only. Switched out POS systems for Wal-Mart in Kauai and Hilo and configured to insure connectivity to Wal-Mart Point of Sale servers for accurate pricing. IT Specialist/CND Support Analyst U.S Army November 2011 to October 2015 2210 Titles: CND Threat Analyst Grade: GS09 Series 2210 Ph # 808-438-7999 May Contact Primary Duties: Coordinate with Information Operations for the Regional Cyber Cell Pacific (RCCP), Intelligence, and Network Operations staff elements to determine cyber related threats and entities in the theater. Monitor actionable intelligence and cyber threat information to ensure RCCP leadership and Army awareness. Liaise with the Regional Network Enterprise Center (NEC) and develop technical courses of action in response to Information Assurance/Computer Network Defense IA/CND threats and attacks. Understand underlying commercial infrastructure in the cyber domain and support development of solutions to protecting critical infrastructure. Develop staff and execute cross-directorate plans of actions for future CND operations around the theater. Liaise with joint and inter-agency organizations on-island to share knowledge of technical capabilities across the relevant staffs. Function as a member of the IO Cell during execution of Pacific LanWarNet (PLWN) and as part of the JTF. Support RCCP monitoring systems operation as part of Computer Network Defense (CND).

Provide Knowledge Management support for efforts related to Information officer (IO), Intel and Cyber operations. System Administrator for Intrusion Detection Systems using ACAS\Nessus Vulnerability Management, IBM software Siteprotector and Real Secure, Managed and maintained system health and availability for IDS, Retina Vulnerability Scanners and Nessus scanners. Run compliancy scans across the Pacific for out dated 3rd party software and out dated versions of Anti Virus, HBSS and SCCM Clients. Analyze data and create Remedy tickets for NEC to mitigate issues from scans. System Administration of (2) Windows 2003 WSUS servers (Dell Power Edge 1950) - (9) Retina Servers (Dell Power Edge R-200) - (9) Intrusion Detection System (IDS) servers (Dell Power Edge R-200 Enterprise) HBSS, HIPS & Epo configuration knowledge. BMC Remedy Enterprise knowledge of ticketing service. System Administrator for ACAS Nessus scanners with one Security Center using Red Hat Linux for data repository. Draft reports, create briefing slides, update servers with latest patched and audit files. IA Security Analyst DS Information Systems Corp May 2010 to September 2011 Contractor Phone: 808-485-5353 May Contact RCC-P Manage and monitor Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS). Report attacks to RCERT (CND) and contact DOIMs about possible security breaches and if needed to seize users accounts or computer for further investigation. Run Log collectors against local computers that where violations were found on. Ran QTIP scans for unauthorized software on DOD computers. Report to supervisor of findings and to bring to the attention of the government. Create Incident reports (IR) for RCERT for further analysis. Run Vulnerability scans using Government approved programs and post results on our OPSEC portal for each DOIM in the Pacific Theater for mitigation of Vulnerabilities or removal of service of non-compliant systems. Monitor and report an HBSS finding of possible viruses and comparing hash to make sure no files has been tampered with. Network security monitoring team for system alerts and logs collected by automated tools, such as Snort, Arcsight, McAfee Epo console and Wireshark. Monitors traffic for indications of security problems. Perform first-level monitoring using Arcsight and related IDS/IPS tools. Open up proxy logs to see if users are going to sites that are not secure. Use the Find command to download and determine which user has committed, if any, violation and submit our findings to RCERT for further investigation or legal actions. Correlate and react to security events. Maintain and document communication with analysts using Remedy. Evaluates vendor provided signature packages and install when required. Research current vulnerabilities and techniques to maintain security on the DOD network. Perform vulnerability scans of theater assets using standard Army tools. Administer and maintain IA hardware and systems. Be able to quickly respond and resolve outages. Trusted Agent for VPN accounts and maintains VPN database for active and inactive VPN accounts Builds, Configures, Manage, Monitors and maintain Intrusion Detection Systems (IDS) Complete Army Taskers that come in requiring us to investigate if any user has been to malicious or unwarranted sites, investigate websites that customers request to unblock to be able to tell if the site is malicious or safe to be unblocked. System Administration of (2) Windows 2003 WSUS servers (Dell Power Edge 1950) - (9) Retina Servers (Dell Power Edge R-200) - (9) Intrusion Detection System (IDS) servers (Dell Power Edge R-200) IA Security Analyst Ventura Technologies January 2009 to May 2010 Contractor Phone: 808-678-3900 May Contact Manage and monitor Intrusion Detection Systems (IDS) and Intrusion Protection Systems (IPS). Report attacks to RCERT and contact DOIMs about possible security breaches and if needed to seize users accounts or computer for further investigation. Run Log collectors against local computers that where violations were found on. Ran QTIP scans for unauthorized software on DOD computers. Report to supervisor of findings and to bring to the attention of the government. Create Incident reports (IR) for RCERT for further analysis. Run Vulnerability scans using Government approved programs and post results on our OPSEC portal for each DOIM in the Pacific Theater for mitigation of Vulnerabilities or removal of service of non-compliant systems. Works as part of a 24x7 security monitoring team for system alerts and logs collected by automated tools, such as Snort, Arcsight and Wireshark. Monitors traffic for indications of security problems. Perform first-level monitoring using Arcsight and related IDS/IPS tools. Correlate and react to security events. Maintain and document communication with analysts using Remedy. Evaluates vendor provided signature packages and install when required. Research current vulnerabilities and techniques to maintain security on the DOD network. Perform vulnerability scans of theater assets using standard Army tools. Administer and maintain IA hardware and systems. Be able to quickly respond and resolve outages. Trusted Agent for VPN accounts and maintains VPN database for active and inactive VPN accounts. System Administration of (2) Windows 2003 WSUS servers (Dell Power Edge 1950) - (9) Retina Servers (Dell Power Edge R-200) - (9) Intrusion Detection System (IDS) servers (Dell Power Edge R-200) PAC-TNOSC JR IA Computer Analyst CACI INC October 2007 to December 2009 Contractor Phone: 703-841-7800 May Contact Support Army customer as Information Assurance Officer for the Army Pacific Headquarters Network Operations Center. Provided Information Assurance (IA) consultation and technical knowledge to ensure secure operation of systems on Army Pacific Network. Developed program to ensure all systems connecting to Army Pacific Network are operating securely through the conducting of vulnerability assessment scans, and monitoring of assets, resources, and users through Active Directory services to ensure compliance with DoD Information Assurance Controls. Developed the following Certification & Accreditation documents for Army Pacific TNOSC: System Security Authorization Agreements, Security Test & Evaluation Plans, Risk Assessments, Contingency Plans, Security Awareness Plans, and Incidence Response Plans. Provided systems analysis of IT infrastructure and enterprise architecture through Information Assurance Program which documented network topology allowing for increased effectiveness in troubleshooting and maintain secure configuration management of network. Maintained Information Assurance of firewall through Connection Approval Process and validation of: source and destination IP addresses, non-malicious ports, IAVA compliance. Program manager for testing, validation, and deployment of Microsoft Security Updates to over ten thousand users throughout the Army Pacific region. Trusted agent (TA) to approve VPN users on the Army Pacific Region for the entire Pacific. Maintain VPN database for inactive users. System Administration of (2) Windows 2003 WSUS servers (Dell Power Edge 1950) - (9) Retina Servers (Dell Power Edge R-200) Computer Programmer TMI Management September 2006 to July 2007 Contractor Phone:

Unknown (Company Closed) This level, initial assignment is designed to expand practical experience in applying PC systems techniques and procedures. Uses established fact finding approaches, knowledge or pertinent work processes and processes, and familiarity with related computer programming practices, system software, and computer equipment, Medical related documents. Carry out fact finding and analysis as assigned, usually of a single activity or a routine problem, applies established procedures where the nature of the system, feasibility, computer equipment and programming language have already been decided; may assist a higher level analyst, may research routine user problems and solve them by modifying the existing system when the solutions follow clear procedures. Purges all data from obsolete computer systems throughout Tripler Army Medical Center. Ensures all memory from systems is unrecoverable. Inspects computer systems and prepares documentation for proper turn-in to the respective Agency. Supervisor defines objectives, priorities, and deadlines. Incumbents work independently and as a group to resolve problems and deviations according to established practices; and obtain advice where precedents are unclear or not available. Completed work is reviewed for conformance to requirements, timeliness, and efficiency to operate a forklift for warehouse duties. SECURITY CLEARANCE: Active DoD Top Secret (TS) (SBI/SSBI) clearance; Education certificate in Office Administration and Technology Windward Community College - Honolulu, HI November 2002 Skills SECURITY (10+ years), INFORMATION ASSURANCE (7 years), IDS (6 years), INTRUSION (6 years), INTRUSION DETECTION (6 years), It Specialist, Help Desk, Desktop Support, Information Technology, Comptia Additional Information HIGHLIGHTS OF QUALIFICATIONS Extensive knowledge of Information Assurance concepts for Department of Defense Information Systems Network (DISN) implementation, configuration management, and Life Cycle Program Management processes. Possesses CND experience in the security of at Army Pacific Network. Worked as a team at the RCC-P Information Assurance Triage station. Configured and built the Enterprise Intrusion Detection System (IDS) for the Pacific Theater. Monitor and report findings from Intrusheild Protection System (IPS) Monitored and reported findings from McAfee HBSS ePO console Created Remedy work tickets upon findings of intrusion or malicious files. Create VPN accounts, upkeep of VPN database, troubleshoot VPN issues. System Administrator for Enterprise Windows Server 2003 and 2008 for WSUS, ACAS\Nessus, Retina Scanner and Intrusion Detection system (IDS) Diagnoses, manages, and optimizes system performance, including functionality of networks and systems. Installs, supports, and maintains the operating environment including hardware, software, operating systems, upgrades, network systems and Voice over Internet Protocol (VoIP). Plans, evaluates, and ensures security of operating environment and network is in compliance with established security policies and protocols. Provides customer support for troubleshooting and resolving most customer problems with user workstations, network issues, and access. Operating Systems: Various Windows Server and Client configurations, System Security Authorization Agreement (SSAA) Preparation Training Trained to conduct Vulnerability Assessment with the following tools (Retina, ACAS) Qualifications: -5+ years of experience and technical expertise in Computer Network Operations planning and execution in a real world environment (Government experience) Enterprise Theater Army Wide Experience in cyber intelligence reporting Knowledge of US intelligence community, DOD organizations and other US computer focused organizations TS/SCI clearance required

Name: Veronica Kennedy

Email: mark11@example.com

Phone: (283)465-3626