IT Specialist (Security) IT Specialist (Security) IT Specialist (Security) - Department of the Air Force California City, CA Authorized to work in the US for any employer Work Experience IT Specialist (Security) Department of the Air Force - Edwards, CA June 2015 to Present * Serves as the Detachment Lead Cyber Security Operational Test Program Director, applying DoD and Air Force cyber security methodologies, threat identification and test knowledge to the operational testing of major defense systems. Lead a team of cyber security professionals, test engineers and test analysts as the Detachment's recognized expert in the design, development, execution and reporting of cyber operational effectiveness and suitability capabilities of new or modified weapon systems. * Lead team of cyber security analysts to develop initial test designs and plans for the execution of operational testing and reporting on the cyber security capabilities of the F-35 Air System. Provides senior-level expert direction to test team members, developmental test agencies and DoD acquisition and test leadership on highly specialized cyber security operational tests * Serve as the lead cyber security operational test expert, leading a team that applies DoD and USAF cyber operations experience and knowledge in support of F-35 Air System development, testing and acquisition. Researches and designs new techniques for understanding cyber operations employment based on doctrine; tactics, techniques and procedures; and concepts of operations. * Lead Detachment cyber security participant in joint /service capability or modernization planning, development and requirements document coordination to improve organizational direction and focus using applicable planning tools and techniques. * Prepare and deliver oral presentations such as high-level briefings, training sessions, consultations and strategy sessions with other internal/external organizational functions and activities to secure cooperation , resolve controversial matters and convey information relative to proposed changes in assigned programs. * Oversight supervision during operational testing for 51 members of the full Cybersecurity testing force which includes all members of the AFOTEC Det 1 JOTT Cybersecurity team (8 members) and remaining 43 test team member from associate blue and red teams. Information Assurance Security Officer Air & Missile System Simulation & Development Directorate January 2011 to May 2015 *Information Assurance Security Officer for the Air & Missile System Simulation & Development Directorate.

Provided security posturing in regards to DIACAP accreditation and IAVM patch. Verify and maintain accreditation for closed network labs within the Directorate. *Provided guidance to government and contractor personnel on security initiatives with respect to computer security. *Assisted AMRDEC IAM in the enforcement of command policy towards computer security. *Implemented and administered computer security regulations applicable to automated data processing, word processing, scientific computing, data/files management, and facility operations. *Maintain professional and positive contacts, both within and outside the Department of the Army to facilitate the effective implementation and non-implementation of computer security initiatives as it relate to daily activity of the research and development of current projects. *Maintain proper accounting of IT assets within the preview of labs be governed by IASO duties. * Operational supervision of a team of 3 contractors to support AMRDEC Patriot simulation laboratory. IA Analyst Smartronix, Inc - Albany, GA January 2010 to January 2011 *Provided in depth technical support for the analysis and evaluation of security concepts, designs, and tests in support of certifying and accrediting heterogeneous United States Marine Corps applications/systems using the DoD Information Assurance Certification and Accreditation Process (DIACAP). *Developed and maintained DIACAP packages and all other pertinent IA documentation in accordance with Department of Defense (DoD) and all other agency and department guidance throughout the application/system lifecycle. *Identified, implemented, validated, and managed Information Assurance Controls (IACs);*Performing threat assessments, vulnerability assessments, Security Test and Evaluation (ST&E) and risk analysis; *Assessed system vulnerabilities and determine adequacy of security controls implemented and the level of residual risk; *Scheduled and coordinated Information Assurance activities; *Provided the technical capability to analyze problems associated with integration and assist in the correction of security deficiencies of hardware and software used in current and planned systems and networks; *Conducted risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs; *Conducted systems security evaluations, audits, and reviews; *Developed systems security contingency plans and disaster recovery procedures; *Participated in network and systems design to ensure implementation of appropriate systems security policies. Network Security Engineer CSC - San Diego, CA August 2008 to December 2009 *Contractor providing network security for classified research and development network for SSC San Diego. Scan and analyze networked hosts for vulnerabilities. Submit scan results to system administrators for corrective actions as necessary. *Assisted in the monitoring and maintenance of classified network in regards to initial IP requests and certification of new hosts on the network. Verify remediation of Microsoft related product with the use of WSUS. Maintain Symantec SAV server by verifying latest definitions have been applied to server and mitigated across the network. *Designed, developed, troubleshoot, and analyzed moderately complex network security systems, processes, and procedures. Researches, proposes, designs, implements and evaluates information security solutions. *Performed moderately complex security systems modeling, simulation, and analysis to provide appropriate solution. Develops and oversees security software system testing procedures, programming, and documentation to ensure standard use of procedures. *Provided inputs for documentation of new or existing security system procedures and/or programs to ensure information accessibility, as required. Designs, develops, troubleshoots and analyzes software programs to ensure compatibility with hardware systems. *Customized security system software based on research and customer needs as appropriate. Coordinates and facilitates communications with other departments and/or commercial vendors) to investigate and resolve security vulnerability matters of significance and to ensure proper functioning of security systems. *Maintained communication with management and customers regarding status of security system procedures, processes and software development and problems. Acts as technical lead on large projects involving a particular security system initiative or counter measure. Provides leadership and work guidance to less experienced personnel. *Provided the customer base with first level support. Documents security equipment scaling plans and limitations. Develops detailed design using best of breed security equipment including firewalls, intrusion detection systems (IDS), and access control servers. Information Technology Specialist Lone Star Army Ammunition Plant - Texarkana, TX October 2007 to July 2008 *Assigned to Lone Star Army Ammunition Plant (Base is now closed due to 2005

BRAC) * Serve as advisor to the Commander, Contract Operations Officer, and ACO staff on all matters concerning the Army Information Management Program, Information Technology (IT) programs and equipment, and security of installation information technology network connecting numerous sites. Responsible for maintaining databases, reports, and metrics for all production contracts for the installation. Responsible for training ACO staff members on new and existing hardware and software systems. *Reviewed, analyzed, developed and recommended directives and procedures necessary to support a sound information management program at the installation. Responsible for all IT equipment to include authorization, acquisition, utilization, and maintenance. Coordinate with and advise all staff elements on the feasibility of automating functions. Instruct users in the use of software packages, service routines, programming guidelines, and techniques for specific programs. Stay abreast of emerging Army initiatives such as Active Directory and LMP. *Appointed as the installations Information Assurance Manager (IAM) and Information Assurance Security Officer. Conduct risk assessments of the contractor's and Government staff IT systems. Execute the Security Support Authorization Agreement, which requires specific knowledge of computer networks, system virus protection and protective patches, hardware devices, software, connectivity, and firewalls. *Received Information Assurance Vulnerability Alerts and Advisories from higher headquarters, evaluate effect on Government systems and ensures evaluation by the contractor. Installs required security measures on ACO staff IT network and ensures appropriate actions are taken by the contractor to implement required system corrections. *Provided required IT system security training to Government staff and ensure the contractor maintains an effective training program for plant employees. Required to work with higher headquarters to coordinate input to databases or calls for data related to specific IAVAs or taskers. *Maintained IT network for the ACO staff. Maintain network devices and personal computers. Provide Internet access to users as required for commercial websites, as well as secure and non-secure Government network systems. Perform duties as network and systems administrator. Serves as primary COMSEC custodian for Lone Star Army Ammunition Plant. Education Masters in Management Information Systems The University of Alabama at Birmingham - Birmingham, AL January 2018 to August 2019 BS in

Technical Management Devry University - Irving, TX May 2007 Skills Network Administration, Disaster Recovery, Strategic Planning, Customer Service, Active Directory, Cisco Military Service Branch: US Navy Service Country: United States Rank: E6 June 2001 to November 2005 IT Specialist Additional Information Top Secret clearance with SCI eligibility

Name: Ashley Norton

Email: vickimoore@example.net

Phone: 329.741.0983x20882