Cyber Defense Infrastructure Support Specialist Cyber Defense Infrastructure Support Specialist Summerville, SC Mr. Hobbs has almost 14-years of progressive experience in the Information Technology industry, six of which are in the Cyber Security Field. Mr. Hobbs also has six years of experience with the Marine Corps, Navy, VA, and the DHA. His work experience is complemented by a BS Degree in Information Technology with a Concentration in Information Security Systems, Security+ CE Certification, Linux+ Certification, MTA, MCP, and he is also a Navy Qualified Validator Level II. Authorized to work in the US for any employer Work Experience Cyber Defense Infrastructure Support Specialist Naval Information Warfare Center (NIWC) - North Charleston, SC May 2019 to Present 40 Hour Work Week Provides CND infrastructure support to projects to include Cyber Defense design, installation, assessment/audit, system hardening, and risk mitigation. Performs system-level, software level, and data-level risk analysis, and documents the IA requirements and policies relating to the network and computer systems. Provides effective risk mitigation strategies for information systems and network components. Provides system integration guidance and technical support as they relate to the application of IA products. Provides technical security documentation such as investigation reports, risk assessments, and security plans/procedures. Runs vulnerability assessment tools and evaluates the results for compliance with Federal and DoD Cyber Security requirements. Security Analyst Cambridge International Systems - North Charleston, SC September 2017 to May 2019 40 Hour Work Week Assisted in preparing for the Command Cyber Readiness Inspection (CCRII) of the Naval Engineering Training Command (NETC) at their locations around the world. Assisted with Cyber Security efforts in engineering and C&A and Assessment & Authorization (A&A) (FISMA, NIST 800-53), ranging from HBSS support, ACAS support, Nessus scans and remediation, test scripting, testing, reporting, STIG hardening, bringing systems to IAVA compliance, and documenting SOP's or other security artifacts. Assisted in baseline testing, pre-testing, recovery, engineering, and security engineering Assisted in testing and engineering Linux, Oracle, PL-SQL, MS-SQL, IIS, Apache etc. Information Security Engineer Telos - North Charleston, SC May 2017 to September 2017 40 Hour Work Week Provided IA support that included providing A&A management, A&A technical, Security Test and

Evaluation (ST&E), and independent verification and validation (IV&V) support to networks/enclaves and programs of record (PORs)/platforms information technology (PITs), automated tool support, A&A assessment and package development support, and incident response support. Provided assistance to enclave personnel in completing required A&A documentation (POAM, RAR, SP), addressing Security Test and Evaluation (ST&E) results, and assisting enclave personnel in preparing Interim Approval to Operate (IATO) and ATO packages for review by the Validator, Certifying Authority (CA), and the Operational Designated Approval Authority (ODAA). Provided assistance to Navy Medicine sites in updating outstanding actions contained in their plans of action and milestones (POAMs); recommending security risk-mitigations (Nessus scan, and SCAP scan remediation); and requesting extensions for expiring IATOs as required. Conduct liaison with Navy Medicine sites in preparation for A&A activities. Made recommendations concerning certification; support and provide minutes and status reports for collaborative meetings with Navy CA/ODAA points of contact to update and enhance A&A documentation accordingly. Prepared recommendations and project timelines for completion of the A&A process; provided A&A metrics; and updated the NAVMISSA status trackers as required. Participated in A&A process improvement activities. Used automated collection utilities that supplement and expedite this information-gathering process by performing system discovery, and hardware and software listings. Conducted IV&V and ST&Es activities at NAVMISSA network/enclave sites and PORs/PITs using standardized procedures and scoring methodology IAW DoD policy and RMF. Validated all applicable IA controls; perform a vulnerability and risk assessment of identified vulnerabilities and identify countermeasures. Consolidated, reviewed, analyzed, and produced reports containing the assessment and ST&E results to Navy Medicine stakeholders. System Security Administrator ASM Research - North Charleston, SC January 2017 to April 2017 40 Hour Work Week Provided systems analysis in support of the Continuous Readiness Information Security Program (CRISP). Established and reviewed documentation for policy and procedures. Researched the latest Information Technology trends. Developed security standards and best practices for the client. Reviewed current processes and made technical/process recommendations for improving efficiency.

Assessed and recommended security enhancements. Assessed the Cybersecurity risk of IT systems, documented them in a formal risk assessment and the supporting artifacts associated with the Assessment & Authorization (A&A) process (POAM, RAR, SP). Organized, developed, and presented briefings, written summaries, and written reports incorporating narrative, tabular and/or graphic elements. Implemented IT security solutions and assured successful implementation. Applied knowledge of security principles, policy and regulations to daily tasking. Researched policies, procedures, standards, and guidance, and applied needed changes under specific conditions for the protection of information and information systems. Information Security Engineer CACI - North Charleston, SC August 2016 to January 2017 40 Hour Work Week Provided Mitigation and Remediation (Nessus scans, SCAP scans, STIG hardening) in support of the C&A/A&A process remotely and/or on-site including reports as required. Conducted in-depth analysis of IV&V/SCA, C&A/A&A, and functional/operational test results for accuracy, compliance, adherence to DoD and Federal IA technical and operational security requirements. Documented residual risks by conducting a thorough review of all the vulnerabilities, architecture and defense in depth and provide the IA risk analysis and mitigation determination results for the Test Report. Worked with system owners to develop specific site and system mitigation plans to achieve an overall reduction in residual risk. Developed C&A/A&A documentation in accordance with DoD policies, NAVFAC policies and procedures to ensure that accreditation packages are complete and system compliance is met for Designated Accrediting Authority. Maintained documentation Plan of Action and Milestones. Developed associated IA Artifacts to include the System Security Plan, System Design and Architecture, Contingency Plan/COOP Plan, Incident Response Plan, Audit Design, Change Control Board, Identification and Authentication, Physical and Environmental, and Remote Access artifacts. Provided guidance and support related to IT Contingency Planning Information Security Engineer (Contract to hire for CACI) Apex Systems, Inc - North Charleston, SC January 2016 to August 2016 40 Hour Work Week Provided Mitigation and Remediation (Nessus scans, SCAP scans, STIG hardening) in support of the C&A/A&A process remotely and/or on-site including reports as required. Conducted in-depth analysis of IV&V/SCA, C&A/A&A, and functional/operational test results for accuracy, compliance, adherence to DoD and Federal IA technical and operational security requirements.   Documented residual risks by conducting a thorough review of all the vulnerabilities, architecture and defense in depth and provide the IA risk analysis and mitigation determination results for the Test Report.   Worked with system owners to develop specific site and system mitigation plans to achieve an overall reduction in residual risk.   Developed C&A/A&A documentation in accordance with DoD policies, NAVFAC policies and procedures to ensure that accreditation packages are complete and system compliance is met for Designated Accrediting Authority.   Maintained documentation Plan of Action and Milestones (POAM).   Developed associated IA Artifacts to include the System Security Plan, System Design and Architecture, Contingency Plan/COOP Plan, Incident Response Plan, Audit Design, Change Control Board, Identification and Authentication, Physical and Environmental, and Remote Access artifacts.   Provided guidance and support related to IT Contingency Planning. Network Operations Lead - Mid Level Northrop Grumman - Camp Lejeune, NC July 2014 to January 2016 40 Hour Work Week   Ensured effective and efficient operation of network systems, architecture and topology through deployment, and oversight of network operations specialists.   Ensured that all operating systems were adequate, functional, and conformed to operation security policies and procedures.   Assisted with the development and application of business processes to ensure appropriate service levels.   Developed and implemented standards, procedures, and processes for the Network Operations Center.   Participated in strategic network planning, steady state operations planning, and development of contingency operation plans.   Planned and supported injection of new technologies and implementation of technology refresh.   Estimated project costs and prepared project plans.   Conferred with and advised administrators, user representatives, and technical personnel regarding development and design of integrated network solutions.   Prepared recommendations based on monitoring results, tools analyses, and forensics.   Participated in the development and implementation of policies and procedures regarding network equipment, maintenance, and monitoring.   Prepared status reports.   Scheduled routine system maintenance, oversaw application of proactive Cyber Security measures, and managed reaction to Network

Defense requirements. Developed and maintains system architecture and operational documentation. IT Specialist Epsilon, Inc - Camp Lejeune, NC December 2013 to June 2014 40 Hour Work Week Provided technical support for software development and integration efforts. Performed in a variety of technical areas including systems requirements analysis, data analysis and engineering, systems design, systems development, computer programming, systems testing and deployment, quality assurance, configuration management, and systems documentation. Rolled out hardware and software to ensure optimal deployment of resources. Developed plans for automated information systems. Analyzed user interfaces, maintained hardware and software performance tuning, analyzed workload and computer usage, maintained interfaces with outside systems, and analyzed proposed system modifications, upgrades and new COTS. Defined the problem and developed system requirements and program specifications. Integrated, tested, and debugged software components. Prepared required documentation including program-level and user-level documentation. Enhanced existing software systems. Provided technical data base support including: data base design; data integration; data standardization; enterprise-wide data architecture specification; and data base management. Help Desk Support Analyst Apex Systems, Inc - Camp Lejeune, NC July 2013 to December 2013 40 Hour Work Week Responsible for providing Tier 1 - Tier 3 Technical support to active duty military personnel and civilians. Responsible for troubleshooting IT equipment. Responsible for maintenance and repair of IT equipment. Responsible for the installation of IT equipment. Responsible for troubleshooting hardware and software on Dell/HP laptops, desktops, Xerox/HP network/desktop printer, installing peripherals (BB's, scanners, printers, etc). Experience with working with the ticketing system Remedy. Experience with working with higher ranking Military Officers and Govt. customers. Property Control Clerk Onslow Memorial Hospital - Jacksonville, NC December 2005 to July 2013 40 Hour Work Week Responsible for securing and maintaining SQL Server and databases used for asset tracking. Responsible for securing and maintaining electronic filing system for hospital assets. Responsible for transportation and storage of hospital records Responsible for transportation and storage of some hospital assets. Responsible for proper disposal of obsolete hospital assets. Responsible for a variety of other hospital projects. OPERATING SYSTEM AND SOFTWARE/TOOL EXPERIENCE: Windows Server 2003 WinDump Windows Server 2008 R2 TcpDump Windows Server 2012 R2 Nmap (Zenmap) Windows SQL Server 2005 Wireshark Windows XP (Professional) Flying Squirrel Windows 7 (Professional, Enterprise, and Ultimate) GRASSMARLIN Windows 8.1 (Professional) CSET Windows 10 (Home and Professional) SCAP Compliancy Checker Ubuntu 14.1 and 16.04 ACAS CentOS Nessus RHEL STIG Viewer HBSS SCCM Education Bachelor's in Information Security Systems University of Phoenix-Online Campus Skills Customer Service, Call Center, Customer Support, Desktop Support, Help Desk, Network Security, Risk Management, Risk Assessment, Validation, Security Certifications/Licenses Security+ CE Linux+ MTA MCPS: Microsoft Certified Professional Navy Qualified Validator Level II Additional Information Mr. Hobbs has almost 14-years of progressive experience in the Information Technology industry, six of which are in the Cyber Security Field. Mr. Hobbs also has six years of experience with the Marine Corps, Navy, VA, and the DHA. His work experience is complemented by a BS Degree in Information Technology with a Concentration in Information Security Systems, Security+ CE Certification, Linux+ Certification, MTA, MCP, and he is also a Navy Qualified Validator Level II.

Name: Kenneth Hines

Email: paula22@example.com

Phone: +1-655-450-0682x36911