6 month IT Generalist Contractor 6 month IT Generalist Contractor Perryopolis, PA Authorized to work in the US for any employer Work Experience 6 month IT Generalist Contractor Software Specialists, Cranberry Twp., PA 2019 to Present As a Contract Security Control Assessor (SOA) I was responsible for assessing the management and conduct of BeyondTrust Information Risk scans weekly and as assigned to the Security Delivery team. Review and analyze documentation necessary to perform appropriate assessment and conduct necessary interviews in order to collect and review relevant materials necessary to produce the results of the assessment. Clearly and concisely document and communicate risk assessment results with requestor, security architects and management teams, as appropriate. Conduct and formulate appropriate risk scoring, as it relates to threat, vulnerability, likelihood, impact, security controls/counter-measures, etc. Understand and contribute to inventory of vulnerability tracking and associated risk statements. Perform follow up activities related to exceptions, risk acceptance, corrective action plans and additional mitigation activities. Participant with multiple projects and initiatives to apply security requirements, develop architecture solutions, integrate security into solution designs, access risks of security gaps, and develop architecture remediation. Assist Security Delivery team in developing and maintaining appropriate procedural documentation which meets relevant compliance standards, such as NIST, Microsoft CIS, PCI-DSS, Health Information Trust Alliance (HITRUST), and International Organization for Standardization (ISO) 27001. Prepare and present dashboard and remediation reports to different levels of management and varying technical experience. Begin to take lead role in assuring compliance to required standards, procedures, guidelines and processes. Other duties as assigned or requested. Information Systems Security Engineer / Site Lead HP, Enterprise Services / DXC Technology / Perspecta - Herndon, VA 2014 to 2018 As an Information Systems Security Representative (ISSR) who work as a liaison with the Information System Security Manager (ISSM) and multiple Information System Security Officers (ISSO). Inspect continuous monitoring results to confirm that the level of risk is within acceptable limits for the software application, network, or system. As part of continuous monitoring, ensure proposed finding mitigations are being completed by the agreed upon date via the Plan of Actions and Milestones

(POA&M) within the RiskVision application. Providing an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities and vulnerabilities against relevant information assurance policies. Verifying that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct deviations Worked with system owner(s), ISSM and ISSO(s) to accredit both FISMA and non-FISMA reportable FBI information systems so that all systems are maintained and managed within the RiskVision application. Review CJIS's Security Center results to confirm that the level of risk is within acceptable limits for the software application, network, or system. As part of continuous monitoring, ensure proposed finding mitigations are being completed by the agreed upon date via the POA&M. Ensure all FISMA documentation is maintained/submitted as required. Senior Cyber Information Assurance Analyst Northrop Grumman, Information Systems - Fairfax, VA 2013 to 2014 I was part of a team of diverse Cyber Security Engineers performing and enhancing the security assessments of Trusted Internet Connections (TICs) at civilian federal agencies. In this position I provided cyber- security capability validation support to the Department of Homeland Security (DHS) Federal Network Resilience - Engineering Support Services (FNRENSS). These Cyber Security Engineering team uses the latest technology to monitor, analyze, and rate security risks on major Government agency networks. Major contract functions include information security monitoring and risk management, Internet defense, vulnerability assessment and remediation, information technology operations oversight, and security metrics. Senior Professional Computer Sciences Corp - Falls Church, VA 2013 to 2013 Information Security Engineer Sr. Information Security Specialist Integral Consulting Services, Inc - Gaithersburg, MD 2011 to 2013 Biometrics Identity Management Agency (BIMA) Clarksburg, WV Primary responsibility was for the day-to-day operations, training and maintenance of a Cross Domain Solution (ISSE Guardv3.6). I was involved with this project of getting the Cross Domain Solution installed, tested & certified (current CDSA in place) for use on Army networks. I was also the Lead for DoD Continuous Monitoring at BIMA, using LOG Storm. Other duties as assigned included Development of annual Disaster Recovery Drills and Facilitating table-top exercises, POA&M support where I develop, track

& update the POA&Ms for all of BIMA networks; I conduct Retina and Gold Disk Scans of all BIMA IT assets, track vulnerabilities/findings for IAVA compliance through completion &/or mitigation. Perform annual Security Control testing, attend BIMA CCB and support actions assign. I am the Lead for BIMA's Certificate of Networthiness (CoN) process and assist with other IA related issues as needed. Cyber Information Assurance Analyst 4 Northrop Grumman, Information Systems - Johnstown, PA 2006 to 2011 Cyber Technologies Team Lead Lead an effort doing a Security Assessment of a Cross Domain Solution (CDS) to verify it meet or exceeded all current DoD and Best Practices for security engineering. This effort has our team following the NSA INFOSEC Evaluation Methodology (IEM). As such as the lead this team will be conducting several types of scans (Port, SNMP & Vulnerability), Enumeration and Banner grabbing, Host Evaluation, Network device analysis, Password compliance verification, Software compliance verification, Network Sniffing, Personnel interviews, etc. The information produced during this IEM assessment will be used to identify potential problems or shortfalls, Identify system/policy weaknesses and deficiencies, prioritize risk mitigation and risk mitigation activities and support budgetary decisions. Pervious assignments include working on the Future Combat Systems (FCS) Network Management System (NMS) as the Information Assurance (IA) & Security Lead as part of the Systems Engineering Integration and Test (SEI&T) Team. In this role as Embedded Security Engineer my chief duty is to aid the FCS NMS program in applying IA and security engineering expertise into the current 'Build' phase of the project. This is done in order to ensure that developers both software as well as hard have chance to recognize, identify and correct security issues in the requirements as well as identify any security flaws before seeking a certification. I provide the customer with security guidance, including the Common Criteria, DIACAP, as well as DoD and NSA technical configuration guides. I helped integrate security practices into the design, development, testing, and integration of development. I Provide security architecture guidance; secure system design and analysis, DoD Requirements analysis, DITSCAP/DIACAP accreditation support including CT&E and ST&E testing, systems hardening, DISA Gold Disk application, secure software design guidance, DISA Security Technical Implementation Guides (STIGs) recommendation, Security IPT participation, security

technical whitepapers, and security awareness to JSS Software Development team. Keep abreast of latest INFOSEC vulnerabilities and developing threats, gauging security risk to FCS program. Work with Certification Accreditation Working Group (CAWG) on accreditation challenges, design decisions, and C&A Artifact documentation. DoD Information Assurance (IA) Directive 8500.1 requires that all DoD information systems are configured in accordance with DoD-approved security guidelines, as a Subject Matter Expert on a team doing Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGs) reviews, I was able to facilitate the Defense Information Systems Network Video Services-II (DVS-II) obtain Authorization To Connect (ATC) in Ogden, UT. This allowed the Ogden site permission to connect to other DVS-II sites across the Defense Information Systems Agency (DISA) networks. Other sites still awaiting review and ATC. Northrop Grumman, Information Technology - McLean, VA 2005 to 2006 Comp Sec Tech External Preferred Systems Solutions Inc - Fairfax, VA 2004 to 2005 4 Computer System Security Officer National Drug Intelligence Center - Johnstown, PA 1993 to 2004 Johnstown, PA. Assisted the NDIC Information System Security Officer (ISSO) in developing system certification and accreditation (C&A) documentation using the approved DOJ CSAM TrustedAgent toolkit. This support included preparing system security plans, preparing security test and evaluation documentation, performing risk assessments, and developing accreditation plans for all NDIC General Support Systems and Major Applications. As the prime contractor I supported all the security systems at NDIC by reviewing security system logs on a daily basis, and evaluating the security posture of systems through their life cycle. I supported security system design formulation and evaluation and have supported all aspects of system security C&A. Assisted in performing periodic vulnerability assessments and penetration tests using only NDIC approved assessment tools. Was always prepared to address any security accreditation test findings; by proposing new solutions for resolving accreditation deficiencies, and assisting with the implementation of those solutions. Also was instrumental in performing additional information technology security related tasks as NDIC management identifies them. Synectics/QSi/BAE SYSTEMS, McLean, VA, 1993 - 2004 Senior Principal Systems Engineer/ Analyst Subject Matter Expert on a team doing Security

Certification and Authorization Process (SCAP) reviews for the FAA. This task is entails reviewing the SCAPS using the requirements stated in NIST SP 800-37, 800-53, and 800-53a. Duties also include reviewing C&A documentation, such as Security Plans, Risk Assessments, and Contingency Plans including Disaster Recovery processes to ensure that they meet the guidelines outlined in the NIST SP 800-18, 800-30, and 800-34. Previously I was the Technical Lead of a contract at Dahlgren, VA, supporting the US Navy, as part of a team doing all the Certification & Accreditation documentation. This included; several Risk Matrices, and Security Test and Evaluations Processes (STEPs) with the results becoming part of the Vulnerability Assessment Reports, Risk Analysts, Patch Management, and a Security Awareness/Training reviews. Prior to this Contract I was part of a team doing Vulnerability Assessments & Risk Analysts for several classified government and military facilities. This entailed running both Host based scanning software (System Scanner, ESM) as well as Network based scanning software. (ISS, NetRecon, Nessus) We did this with local network equipment and/or configuring laptops that traveled with us. Part of the task included assisting the site using a risk mitigation approach and the preparation of all the required Certification and Accreditation documentation. Part of a team that conducted a "Pilot Study" evaluating Risk Analysts and Vulnerability Assessment tools to be used as part of a "Toolbox" for traveling Assessment teams. This was part of a task for redefining the 'framework' in which Information Assurance is done throughout the Intelligence Community. I have written System Security Authorization Agreement (SSAA) for the Certification and Accreditation documentation to be submitted for the DoDIIS Public Key Interface (PKI) system for the Defense Intelligence Agency (DIA) & Maritime Intelligence Porthole for the Office of Naval Intelligence (ONI). Prior to this assignment I was the Information System Security Officer (ISSO) for the ODCSINT Staff, where I served as the primary technical source of policy Interpretation and procedural guidance for Information System Security to the Networks Division. I was responsible for the security of all 3 Classified LAN's. I maintained a current network or AIS certification/accreditation. I prepared, distributed and maintained the plans, instructions, guidance, as well as the ODCSINTs Standing Operating Procedures (SOP's) concerning the security guidelines for proper use of the governments

computer system operations. I reviewed and evaluated the security impact of system changes, including interfaces with other AIS. I ensured that all interconnected systems complied with the current security requirements levied within Intelligence Community infrastructure and that they did not have a negative security impact on any other systems with which they interact and/or support. I maintained all the access control records and verified that they were reviewed. I also ensured that only authorized personnel were given access to the LAN's. Other previous contract assignments included; A Lead System Administration (SA) Migration effort, incorporating an I&W, CT, CI, Proliferation, and a Defense Industries Systems together, to give the analysis an improved tool to form a better overall picture of a specific issue. I was the lead Indicators and Warnings overall Systems administrator, assigned database administrator/trainer for the MDITDS transition from the DAWS. I was responsible for the installation, testing and integration of the system software. I provided coordination between the Government and the I&W software developer in accomplishing this task. I ensured that any software changes, enhancements, and corrections were both error free and included in each build of the modules, along with ensuring that all changes were completed at all sites around the world. I worked as the System/SYBASE administrator for these systems, keeping all data current and maintaining a high rate of accuracy. Data Processing Technician E3 United States Navy 1986 to 1992 E5 (Various Assignments) During my last assignment with the U.S. Navy, I served as a Lead User Support Analyst. I performed SUN system administration and provided "Help Desk" support in a team environment for a network of approximately 250 workstations and ten servers. I was responsible for installing hardware and software, troubleshooting customer calls, and training end-users. In an earlier Navy assignment as a System Operator aboard the USS Cape Cod AD-43, I controlled and monitored operations of Honeywell computers and peripheral equipment. I was in charge of scheduling system downtime, scheduling personnel, and the training of Operations personnel. Education DP 'A' School - San Diego, CA 1986 AA in Specialized Business Systems ICM School of Business - Pittsburgh, PA 1985 Military Service Branch: United States Navy Rank: E5 Certifications/Licenses Security+ November 2011 to November 2020

Name: Alexis Cunningham

Email: susan26@example.com

Phone: (693)389-0553x25950