Senior Systems Administrator Senior Systems Administrator Senior Systems Administrator - SAIC Fort Washington, MD Work Experience Senior Systems Administrator SAIC August 2016 to Present Provides professional operations support to the DoS's IRM bureau infrastructure on the Vanguard 2.2.1 program. Oversees the daily operations and production and domestic Dynamic Host Configuration Protocol (DHCP) systems general maintenance. As Team Lead works in a 24x7x365 operational support environment, oversees new employee onboarding, maintains team schedule, duty assignments, and junior administration training assignments. Meets performance metrics to include: service request completion, incident response, incident resolution, queue management accuracy, and customer satisfaction. Remediates vulnerability findings. Maintains a familiarity with DoS processes and procedures, for both OpenNet and ClassNet environment making full use of the Remedy Service Management System. Ensures required reporting is completed correctly, edited, proofread, and ready for dissemination. Manages the DHCP production environment, using System Center Operations Manager (SCOM) to monitor servers and scope health. Monitors iPost risk scores mitigating findings. Managed production DHCP via InfoBlox troubleshooting. Manages scopes and performs maintenance services to include backup/restore database, and system recovery. Ensures Services Manager is aware of potential system problems or customer issues. Senior Systems Administrator SAIC February 2017 to October 2017 For the Government Information Technology Services supported the Department of Navy (DON), Administrative Assistant - Information Technology Division. Demonstrated comprehensive knowledge of DoD military specifications and standards in the course of overseeing daily operations and general maintenance of the production domestic DHCP systems. Managed server farms of virtual servers existing in 3 environments: MilCloud, Citrix, and Amazon Web Service (AWS). Created new virtual machines and snapshots. Maintained public facing and private internal Windows Servers installed with Internet Information Server, SQL Server, and SharePoint Server. Supported information security management and information systems audit by installing SSL Certificates from the Certificate authority for the server and web applications. Maintained data integrity performing server backups using ArcServe Unified Data Protection. Reviewed monthly new information assurance

vulnerability alerts (IAVA), Information Assurance Vulnerability Bulletins (IAVB) and Computer Tasking Orders (CTO) to develop mitigation plans and compliance matrices. Managed and configured the DoD Assured Compliance Assessment Solution (ACAS) built on Nessus Tenable ensured scans were up to date and findings were remediated in a timely manner. Managed the DoD HBSS built on MacAfee ePolicy Orchestrator. Ensured the latest scan engines and policy files were used. Senior Systems Administrator/Information Assurance Analyst SAIC September 2014 to August 2016 For the V22 Electronic Systems Test Lab (VESTL), conducted activities on multi-platform IT systems for the DON. Working within the Risk Management Framework (RMF) process fulfilled the program office's requirements for information systems and networks. Monitored for IAVA, IAVB, and CTOs. Developed mitigation plans and compliance matrices. Configured automated vulnerability ACAS and HBSS scans. Ensured scans used the correct scan engine and audit identification. Coordinated with the IAM and system owner when implementing patches and updates to remediate vulnerabilities. Managed, and monitored the reporting system (eMASS) Enterprise Mission Support Service Manage, Document. Followed established guidelines while performing administrative tasks. Documented system performance analyzed system logs and identified potential issues that may impact production. Maintained data integrity performing daily backups rotating media for offsite storage. Diagnosed and resolved hardware related issues. Collaborated with enterprise system engineering, DBAs, network, and applications groups to ensure server configurations and network infrastructure adhered to established security guidelines and protocols, including FISMA IA requirements. Installed and configured rack mount servers and network devices. Performed server maintenance. Installed and upgraded Microsoft Server 2008/2012 operating systems. Installed and upgraded applications (Symantec Endpoint Protection 11, Symantec Backup Exec 11). Performed patch management applying hotfixes and updates using GPO. Used Microsoft System Center Configuration Manager (SCCM) 2007/2012. Regularly performed inventory management. Prepared for, planned, and assisted in data center server migrations. Produced documentation detailing operating procedures, systems, events, and associated processes. (RMF) Risk Management Framework Implement, Document, Apply

information security management and information systems audit. applied applicable security compliance system technical implementation guideline standards (STIGs) Senior System Administrator Delex Systems, LLC January 2014 to September 2014 Managed classified environments and information security. Conducted system administration activities on cross-platform IT systems for the DON. Planned and organized work and interacted with technical and non-technical personnel translating user requirements into responsive applications. Demonstrated comprehensive knowledge of DoD military specifications and standards and IA concepts and requirements working within the RMF process on information systems, and WANs governed by the Director of Central Intelligence Directive (DCID), DoD Joint Air Force Army Navy Manual (JAFAN) 6/3 Protection Level 3, and ICD 503/CNSS 1253 Accessibility Level 3 confidentiality and system requirements. Maintained server operational status. Created user accounts and print queues. Installed patches and security updates, and managed Active Directory organizational units and policies. As the Lead Data Transfer Agent (DTA) reviewed and sanitized electronic documents for transfer across security boundaries. Developed the best practices and procedures for effective use of ManTech Document Detective 4.1.2 electronic document security scanner using UNIX regular expressions to identify and highlight prohibited language and tri-graphs within electronic documents. Tier 1 administrator on a PL4 network, via Oracle SUN Solaris with Trusted Extensions. Created and managed user accounts. Produced documentation describing operating procedures, systems, events, and associated processes. Updated and maintained the knowledge base library. Used ManTech Sentris platform to implement document access control, classification labeling, and auditing. Education Diploma Anacostia High School - Washington, DC 1983 Skills Nessus, Splunk, Dns, Tcp/ip, Dhcp, Tcp, Security, Raid, Visio, Symantec, Risk management, Microsoft windows, Microsoft windows 2000, Windows 2000, Microsoft office, Workstations, Microsoft visio Military Service Branch: United States Air Force Rank: Staff Sargent Additional Information RELATED SKILLS Expertise = ("B" - Basic), ("S" - Skilled), ("I" - Intermediate), ("E" - Expert) COMPUTERS/ NETWORKS Years of Experience Proficiency Level OS / APPLICATIONS Years of Experience Level Servers Hardware 17 E Microsoft Windows 2000/XP/7/8/10 17 E Workstations Hardware 17

E Microsoft Server 2003/2008/2012 15 E RAID Disk drive 13 E Microsoft Office 2007/2010/2013 15 E DHCP 12 E Microsoft Visio 2007/2010 8 S DNS 6 S Symantec Endpoint Protection 11/12 5 I TCP/IP 6 S ACAS Nessus Security Center 2 I Risk Management Framework (RMF) 2 I HBSS McAfee ePolicy Orchestrator 2 I InfoBlox (CDCA) 8.1 3 I Splunk (CPUC) 7.x 3 I

Name: Samuel Harvey

Email: hillmary@example.org

Phone: (580)528-9567