Senior Systems Engineer Senior Systems Engineer Senior Systems Engineer - Navy Bloodborne Infection Management Center (NBIMC) Work Experience Senior Systems Engineer Navy Bloodborne Infection Management Center (NBIMC) - Bethesda, MD September 2018 to Present Provide daily support as a Systems Administrator for the Navy Bloodborne Infection Management Center (NBIMC) that operates a system called HIV Management Service (HMS) that maintains interoperability with other medical systems. HMS is a certified and accredited distributed internet application with the database and database application residing on a central, dedicated network of servers providing client/server support to selected users Support a Windows 2008 OS w/IIS, Transaction Server that's processes thousands of medical requests/results a day Manage VMware environment of 24 Windows 2008/2012 servers with management tools WSUS, GPOs, Etc Manage 30 TB datastore and clusters storage for virtual environment Manage 13 TB Dell EMC Storage Manage COMMVAULT server/storage/software which backups the VMware environment and send out daily backup reports Experience with vulnerability mitigation using tools such as Nessus, VRAM tool and ACAS Manage user network access to the NBIMC environment via Active Directory Implement Security Technical Implementation Guides (STIGs) and the NSA Guides for the configuration standards for DOD IA and IA-enabled devices/ systems. Patching, documenting and reporting IAVA and CTO compliance Configure Two-factor authentication and Common Access Card (CAC) for all NBIMC servers Monitor NBIMC network health and activity via Solar Winds Orion Assist the PM with Technical interviews of potential candidates for open positions. Create SOP, CONOPS and other documentation as requested by the System owner Senior Systems Engineer Federal Bureau of Investigations (FBI) - Washington, DC September 2016 to 2018 Manage VMware environment via VMware ESXi 6.0 Create, modify, and delete User accounts, Computer Accounts, Groups, Shared Mailboxes, and OU's Create and troubleshoot Microsoft Lync accounts Create, modify, and delete group policy Troubleshoot group policy issues, determine the effect of all group policies on an account or account group, audit Changes to group policy, and maintain a Group Policy Map Experience using Microsoft Active Directory Services, Power Shell, and/or other scripting tools Experience with the application of Federal

Information Services Management Act (FISMA) rules to the AD environment Administer RSA tokens if users are having issues logging into the network Administer Windows Server 2012 or Windows Server 2008 R2 make sure all required GPO are applied Technical writing skills Identify impacts of AD, GPO, OU changes and edit or remove the Group policy if necessary Tasked with putting together plan of action for patching domain controllers and possible move from physical to Virtual Servers Ensure all domain controllers were updated and patched via SCCM Monitor status, health and network connectivity of Domain Controllers via SCOM Tasked with Office 365 pre-migration Active Directory cleanup Ability to effectively share technical knowledge between government and contractor's personnel Provide weekly reporting activities to government personnel. Systems Engineer Department of Transportation (DOT) - National Highway Traffic Safety Administration (NHTSA) - Washington, DC April 2015 to September 2016 Created measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation by installing, configuring, and managing Encryption Protection, Device Control, and Anti Virus software Maintain state of the art servers, service farm of over 600 virtual servers including successful work history on problem resolutions management Responsible for Nightly backup of NHTSA over 600 Production and DR Servers via Veeam Software and 24-hour monitoring and configuring of backups Manage, Configure, Update and administer 2 Veeam Backup and Replication Servers and configure proxies and Linux repositories for backups Provide status reports for Virtual Servers using Veeam One software Troubleshoot database issues related to patches applied to Database Servers Perform system hardening following NIST Special Publication Security Controls and Assessment Procedure View, configure, and troubleshoot Virtual Machines using VSphere Client 5.5 Administer Red Hat Linux storage repositories configured for Veeam Backup and Replication Communication, risk assessments and documenting continuous risk-based management, status reporting, customer satisfaction Responsible for Vulnerability patching of NHTSA Microsoft Windows servers via Shavlik Provide Change request for patching to NHTSA Change Control Board Provide Infrastructure Support for Application Servers: Administration & Configuration Management, Patch

Management   Impact analysis for new requirements and changes to existing requirements   Technical architecting, systems administration and troubleshooting   Monitor Server resource usage via Whatsup Gold   Determining implementation options as well as provide recommendations and level of effort estimates   Interface with both internal and external system stakeholders to resolve interface issues   Work with the database administrator (DBA) to implement structural changes to the schema   Application infrastructure support   Requirements definition and analysis of commercial off-the-shelf/government off-the-shelf (COTS/GOTS) products to meet documented requirements   Hands on technical expert to manage complex, sophisticated federal government websites which require development expertise, maintenance expertise, and problem resolution expertise and be proactive to immediately address emergencies when websites are down   Application development/software development design, production, maintenance, and software fixes   Requirements definition and analysis of commercial off the shelf/government off the shelf (COTS/GOTS) products to meet documented requirements Systems Security Administrator Department of Justice (DOJ) - Litigation Security Group (LSG) - Washington, DC August 2012 to August 2015 Security Specialist and Emergency Planning Staff IT Specialist   Function as System Administrator IT Specialist for the Litigation Security Group (LSG).   Create and Administer Domain Controller, Symantec Encryption, Device Control and File Virtual Servers.   Manage, maintain, and create user accounts, computer names, passwords and software installed.   Approve security patches to be installed on Classified Laptops and Servers.   Experience in computer evidence seizure, computer forensic analysis, and data recovery Computer network forensics using Encase and FTK toolkit Software   Experience in mitigation of Classified Data Spillage using BCWipe software   Create and Update a classified image for LSG stand-alone laptops and desktops in Accordance with NIST Special Publication Security Controls and Assessment Procedure designed to protect the confidentiality, integrity, and availability of the system and its information.   Install, Configure Symantec Encryption and Device Control on LSG Classified systems.   Created Classified images for Apple MacBook Pro OSX and installed and troubleshooted OSX issues   Retrieve Classified evidence information from the computers of defendants in classified cases.

Travel to Secured Classified Information Facilities (SCIF) around to country to patch and update classified computers.   Create and manage files used and system logs of classified laptops.   Give technical recommendations for hardware and software needs to network infrastructure.   Technical POC for outside agency's such as FBI, NSA, CIA, US Marshalls, DOD, and Defense Attorney's in regards to security and capabilities of DOJ classified laptops.   Knowledge of NIST security baselines, and CSAM C&A (Cyber Security Assessment and Management Certification & Accreditation) reporting   Update, configure, and troubleshot secure faxes and STE phones.   Configure Cisco Xenapp software for VPN purposes for LSG Personnel to use while on travel   Recover data from damaged or Government seized for evidence computer hard drives.   Coordinated with USDOJ compliance department to create a disaster recovery plan and data backup location. Senior Systems Administrator - Team Lead U.S. Department of Defense (DOD) - Arlington, VA December 2010 to December 2012 Army Operations Center (AOC) Command Control Support Agency (CCSA)   Provide Level 3 support to the AOC/CCSA Division (700 customers and 1400 computers)   Manage and oversee a staff that provides 24/7 system administrator support on-site for Army and VIP customers   Provide team leadership and mentorship to support personnel and staff   Trusted Agent for PKI and Common Access Cards for CCSA   Document and maintain maintenance records and perform follow-ups as required for routine preventive and demand maintenance for servers, workstations and peripherals.   Implement approved system changes based on IAVA notices   Conduct fault isolation and resolution of network problems, whether cable, workstation, peripherals, or other hardware   Move users and computers between OUs using approved tools such as active directory   Provide administrative maintenance on network and computer accounts   Monitor all enterprise wide servers and services   Create packages and install necessary approved hot fixes and service packs using WSUS, Shavlik, and SCCM   Configure agents on computers to communicate with WSUS and/or SCCM for automatic patching   Provide computer room housekeeping functions including scheduled and on-demand server enterprise backup and restore, system reboots, and system disk defrag   Respond to Tier II desktop problems involving user accounts, passwords and access to data files   Assist users with SharePoint by granting access to sites and helping to create sites for different divisions in the department Manage and update site content in SharePoint along with creating document libraries and lists Monitor the network health and welfare using What's Up Gold and conduct first level fault isolation by using the designated server to determine if the problem is upstream of AOC networks or third party Install, configure, and deploy operating system software as required Analyze and diagnose system failures to determine their causes and make written recommendations for corrective action Test proposed procedures and operating system patches for correctness and compatibility with existing application software and procedures Provide technical support to establish effective operational procedures Proactively conduct security scans of workstations using tools such as Retina, Shavlik, and SCCM to ensure that workstations are patched to mitigate security vulnerabilities as directed by the Network Security Chief Modify security policies on groups/machines for troubleshooting purposes with HBSS Provide documentation and status reports on security incidents and patching compliance using SCCM Coordinate and perform operational activities for system administration functions for users and VIP customers to ensure problem resolution System Administrator U.S. Department of Homeland Security (DHS) - Arlington, VA December 2008 to December 2010 Desktop Support Level II - Special Projects U.S. Department of Homeland Security (DHS) Transportation Security Administration (TSA) Functioned as remote technical support for TSA Headquarters and Regional Offices as well as airports. Managed several special projects for the agency consisting of Symantec Endpoint Protection 11 and Netswitch version 2.7.9.1 upgrades for over 300 users. Managed Altiris configuration issues remotely via Remote Desktop Software and advised OIT Unisys Manager on weekly Altiris software deployment. Managed user profiles via Active Directory, user email accounts via Exchange Server, and user Blackberry privileges via BES Server. Conducted system assessments to determine Credant software security status and monitor compliance with security and encryption standards. Configured, installed, and troubleshot Cisco XenApp desktop software and Credant encryption software. Implemented new standards, patches, and software upgrades. Configured and troubleshot Dell laptops and desktops. Replaced motherboards and other computer parts.

Deployed and configured TRX baggage scanning software to airports and regional airports. Deployed software via Altiris to ensure network computers remained updated with critical software patches. Identified out of date software security and configuration issues and provided resolutions. Resolved Symantec Antivirus installation issues and other technical issues via Peregrine ticketing queue. Resolved VPN Software connectivity issues, Active X security issues, and Java web-based issues. Resolved non-working Altiris clients and ensured proper software and critical patch installments for over 300 users. Provided data recovery for approx.100 users. Updated computer images due to non-supported image versions, Adobe software vulnerability updates, and redaction software deployment and configuration. Created Windows XP computer Image via Norton Ghost. Setup and maintained Norton Ghost cast Server to deploy images to TSA computers. Setup and configured Cisco network switches, video calling software, VPN software, VOIP phones, Blackberry devices, Sprint and Verizon aircards, wireless networks, PC's, network computers, printers, Logitech cameras. Installed and configured Cisco video calling software. Provided expert technical consultation and direction to lower level technical personnel. Provided training to contractors, program offices, and OIT staff on software and hardware configuration resolutions. Developed software troubleshooting and configuration instructions for OIT technicians. Education COMPUTER SCIENCE PRINCE GEORGES COMMUNITY COLLEGE - Largo, MD August 2018 BERKELEY COLLEGE - Woodbridge, NJ September 2001 Skills Active directory, Citrix, Hummingbird, Vmware, Xenapp, Encryption, Exchange, Pci, Scom, Security, Firewall, Ghost, Rsa, Ftk, Nessus, Sql server, Sql server 2008, Replication, Sql, Symantec Additional Information TECHNICAL SKILLS Windows 7, Windows 8, 10, MS Windows Server 2003/20082012, MS-SQL Server 2008, Microsoft Exchange 2003, Redhat Linux, CentOS, VMware Workstation 9.0, Vsphere 5.5, 6.0, Group Policy, Active Directory, Citrix XenApp, Java, RSA SecurID, PCI Smart Cards, Credant, Symantec Encryption Protection and Device Control, FTK Viewer, BCWipe, DBAN, , Milestone Xprotect Smart Client 7.0, Dell, HP, IBM, Apple, Hummingbird DM, Bloomberg MDS, Altiris, Symantec Antivirus and Firewall, MacAfee Antivirus, Acronis Snap Deploy Management Console, Norton Ghost, HBSS (Host Based Security System), Shavlik, WSUS, SCCM, SCOM, Solar Winds, WHATS UP GOLD Server Monitor, Veeam Backup and Replication, Vsphere ESX, Nessus, Dell Kace, Big FIX

Name: Jason Frederick

Email: omoore@example.com

Phone: 611-690-9715x66173