IT Lead IT Lead IT Lead - Active Secret Clearance Victorville, CA Work Experience IT Lead Active Secret Clearance November 2018 to Present Monitor all common-user baseline services delivery and support; support specific and unique systems under certain limited circumstances; coordinate service requirements, identify, validate, and negotiate baseline and mission-specific services providing oversight into all IT acquisition efforts. Supervise group of 12 employees and special projects. Periodically evaluate the performance of department personnel as to their individual performance in support of their assigned customer(s). Review resumes and interview potential candidates for new and backfill positions within the department, make recommendations/decisions regarding personnel actions such as hiring, transitions within the department, disciplinary action, and termination. Interact and coordinate with Customer as required to ensure all Customer requirements, support activities, and/or mutual plans of action are being met to their satisfaction. Maintain current operational status information and assessments on projects, financial budgets, training and staffing requirements across the department. Plan the implementation of new systems and applications. Establish performance objectives and evaluates performance in meeting objectives for assigned employees. Develop/deploy/sustain software application systems and utilities as required especially in the area of post flight data reduction and analysis applications by the Stingray CTF to support program requirements. Systems Administration, perform operating system installation, configuration, and backups in support of development environments, for systems such as Windows Server, Windows client (Enterprise or Pro), or Linux. Conform to local processes and procedures for software development, source code control, quality assurance, documentation, and deployment. Advise team and project managers on technical problems. Interact with customers and project managers on a regular basis. Use judgment and initiative in developing analytical and computational technologies and methodologies for solving problems. Interpret customer requirements, develop and analyze appropriate approach to solve technical problems. Assist in the design of the system/software and the associated design documentation. Participate in design reviews. Implement the design through software coding or hardware and documents the implementation appropriately. Plan and executes unit, integration, and systems testing. Assist in

the maintenance and sustainment activities of the system/software. AIR TRANSPORTATION TECHNICIAN AIR FORCE RESERVE 2006 to Present Supervise 22 military members, plan work, set priorities and schedule completion and evaluate performance. Manage, plan and organize air transportation activities, including determining the supplies, facilities, and personnel needed. Establish procedures for loading both passengers and cargo aboard aircraft and implement any necessary safety precautions for handling dangerous materials, special cargo, mail, and baggage. Systems Administrator Northrop Grumman October 2014 to November 2018 Supervise established working group and special projects. Periodically evaluate the performance of department personnel as to their individual performance in support of their assigned customer(s). Monitor all common-user baseline services delivery and support; support specific and unique systems under certain limited circumstances; coordinate service requirements, identify, validate, and negotiate baseline and mission-specific services providing oversight into all IT acquisition efforts. Assist in supervising a group of 6 employees. Review resumes and interview potential candidates for new and backfill positions within the department, make recommendations/decisions regarding personnel actions such as hiring, transitions within the department, disciplinary action. Configure, administer and maintain computer RedHat Enterprise Linux systems RHEL6. Install, Configure and Maintain Centrify Identify & Access Management Solution. Experience distributing, tracking, reporting and executing the installation, configuration and troubleshooting of Windows 2012 servers & Windows 7/10 workstations and associated peripherals. Experience installing, configuring and troubleshooting of VMware ESXi 5.1 or newer. Experience resolving hardware & software conflicts and performing server preventative maintenance, periodic maintenance and break/fix activities. Experience creating operating instructions and procedures for preventative maintenance, periodic maintenance and break/fix activities Assisting VMware infrastructure configuration and VMWare application software and Virtual Server network configurations. Strong experience in MS System Center Configuration Manager (SCCM) administration Implement Security Technical Implementation Guides (STIG). Develop process to meet STIG requirements and documenting responses, and provide analysis and guidance on steps required to become compliant. Implement

counter-measures or mitigating controls. Analyze System problems and identify solutions. Manage and implement DoD Secure Technical Implementation guides (STIG) and STIG viewer, and SCAP Compliance Checker. Implement counter-measures or mitigating controls within a System Plan or Actions and Milestones (POA&M). Responsible for Microsoft OS server installations and network configurations on servers 2008R2/2012R2/2016 and Windows 10 workstations. Manage Microsoft Active Directory to include implementation of GPOs based off STIG requirements, vulnerability results and implement solutions via group policy. Administration of classified Windows systems within strict security policies and procedures. Perform technical research leading to solutions for system or software limitations. COTS SW installation, configuration and maintenance (to include first-level application support for users). Create accurate, detailed technical procedures & installation instructions. Knowledge of NISPOM (Chapter 8) and DCID 6/3-ICD 503 information system requirements. Prepare security documentation for submission to regulatory agencies as required. Experience with National institute of Standards and Technology (NIST) standards and applying Operating Systems (OS), browser and application Security Technical Implementation guides (STIGs). Experience working with SCCM/WSUS, Server 2008 R2, MS Exchange 2010, and VMWare a plus. System Administrator in classified/unclassified Windows Server 2008R2 and Windows 7 environment. Design, implement and upgrade of Microsoft Active Directory environments including supporting infrastructure (DNS, DHCP). Perform Microsoft Active Directory administration including Forrest and Domain management, directory and organizational unit (OU) design, group policy object (GPO) management for an enterprise network. Perform administration activities and troubleshooting in areas including sub-netting, name resolution (DNS), scope management (DHCP) and network device and systems connectivity. Provide support for Citrix XenApp/XenDesktop environment to include hardening. PCM Chevron Alliance Partner San Joaquin Valley Business Unit - Bakersfield, CA February 2014 to October 2014 Scripting (PowerShell) Security Patch Management Maintain and adhere to organizational/division standards, routines and practices Implement, maintain and troubleshoot network and server security, including file/folder permissions Establish and maintain server based storage for user data

and application files Document network designs and maintain records of network changes Evaluation and installation of new hardware and software Optimize functionality of Servers, Network Devices, diagnose and recover failed systems Make appropriate system tuning adjustments to optimize performance of servers Diagnose and isolate System issues Plan and coordinate the installation of new products and equipment Perform System Center Configuration Management (SCCM) infrastructure development, alteration, deployment, and access control. Provide end user desktop environment and telephone customer support Use approved tools and techniques to remotely troubleshoot and resolve end user hardware and software problems Systems Administrator Department of Defense, U.S Navy - Twentynine Palms, CA July 2013 to February 2014 Monitor all common-user baseline services delivery and support; support specific and unique systems under certain limited circumstances; coordinate service requirements, identify, validate, and negotiate baseline and mission-specific services providing oversight into all IT acquisition efforts. Assist in supervising group of 6 employees and special projects. Periodically evaluate the performance of department personnel as to their individual performance in support of their assigned customer(s). Review resumes and interview potential candidates for new and backfill positions within the department, make recommendations/decisions regarding personnel actions such as hiring, transitions within the department, disciplinary action. Active Directory Domain Support Experience in MS System Center Configuration Manager (SCCM) 2007 Knowledge of MS System Center Operations Manager (SCOM) 2007 knowledge of networking devices (switches/routers), and protocols Scripting (PowerShell) Security Patch Management Microsoft DNS Microsoft SQL Windows Server (2003, 2008), and desktop Operating Systems (XP/Windows 7) Perform system administration (e.g. update, patch, backup and restore) for all operating systems. Install IAVAs (Information Assurance Vulnerability Alerts) to ensure network elements, encryption devices, operating systems and application servers are compliant with standards and regulations. Troubleshoot information technology infrastructure technical issues to determine appropriate corrective actions. Manage LAN/WAN resources including: hardware, bandwidth, and performance monitoring Maintain AD user network account to include email, rights, security and system groups

Install and configure servers, workstations and laptops Maintain and adhere to organizational/division standards, routines and practices Implement, maintain and troubleshoot network and server security, including file/folder permissions Establish and maintain server based storage for user data and application files Document network designs and maintain records of network changes Evaluation and installation of new hardware and software Optimize functionality of Servers, Network Devices, diagnose and recover failed systems Make appropriate system tuning adjustments to optimize performance of servers IT Specialist (Information Systems Security Officer) Department of Defense, U.S. Marines - Barstow, CA July 2012 to July 2013 Monitor all common-user baseline services delivery and support; support specific and unique systems under certain limited circumstances; coordinate service requirements, identify, validate, and negotiate baseline and mission-specific services providing oversight into all IT acquisition efforts. Supervise group of 5 employees and special projects. Periodically evaluate the performance of department personnel as to their individual performance in support of their assigned customer(s). Review resumes and interview potential candidates for new and backfill positions within the department, make recommendations/decisions regarding personnel actions such as hiring, transitions within the department, disciplinary action. Implement Risk Management Framework (RMF), make recommendations on process tailoring, participate in and document process activities. Perform assessments of systems and networks and identify where those systems and networks deviate from acceptable configurations, enclave policy, or local policy. This is achieved through passive evaluations such as compliance audits and active evaluations such as vulnerability assessments. Establish strict program control processes to ensure mitigation of risks and supports obtaining certification and accreditation of systems. Includes support of process, analysis, coordination, security certification test, security documentation, as well as investigations, software research, hardware introduction and release, emerging technology research inspections and periodic audits. Perform analyses to validate established security requirements and to recommend additional security requirements and safeguards. Support the formal Security Test and Evaluation (ST&E) required by each government accrediting authority through pre-test preparations, participation in the

tests, analysis of the results and preparation of required reports. Document the results of Assessment and Authorization activities and technical or coordination activity and prepare the System Security Plans and update the Plan of Actions and Milestones POA&M. Periodically conduct a complete review of each system's audits and monitor corrective actions until all actions are closed. Perform system administration (e.g. update, patch, backup and restore) for all operating systems. Operate and maintain the Production Secret Internet Protocol Router (SIPR) and Non-Secure Internet Protocol Router (NIPR) server to ensure proper network security Identify and develop training unit network requirements and diagrams to validate and update network diagrams to ensure the proper building and operation of tactical networks. Troubleshoot information technology infrastructure technical issues to determine appropriate corrective actions. Manage LAN/WAN resources including: hardware, bandwidth, and performance monitoring Supervise a staff of Information Systems Security Officers Provide security configuration and control support on overall network security and performance Perform Retina Scans and initiate remediation steps of vulnerabilities discovered Manage security infrastructure to include firewall systems, router, switches Manage infrastructure security Provide technical advice to senior management on the appropriate application of technology to organizational missions and program requirements Familiar with Workforce Joint Air Force-Army-Navy (IAW JAFAN) 6/3, National Institute of Standards and Technology (NIST), National Industrial Security Program (NISP)-National Industrial Security Program Operating Manual (NISPOM) and other associated United States Government (USG) security regulations, policies, and standards. Support, monitor, test, and troubleshoot hardware and software Information Assurance (IA) problems pertaining to computers, in a network environment and the configuration and management of an enclave network environment in Support of mission planning and classified networks. Develop IA related customer support policies, procedures, and standards. Operates maintain, and disposesof information systems in accordance with established security policies and practices IAW JAFAN 6/3, NISPOM, NIST, the System Security Plan, and other USG requirements, as required. Conduct audits to ensure compliance with established policies and directives. Monitor system recovery processes to ensure that security

features and procedures are properly restored. Document all information system security-related issues and keep data current and accessible to properly authorized individuals. Develop and administer security programs and procedures for classified or proprietary materials, documents, and equipment. Study and administer federal security regulations that apply to company operations. Administer security infrastructure, and participates in formal certification, test, and evaluation activities. Identify vulnerabilities and exploits and make recommendations to address deficient areas. Investigate information compromises and security violations as they relate to accredited information systems processing classified information. Make recommendations for corrective actions and prepares reports specifying preventive action to be taken. Draft, develop, and submit Certification & Accreditation documentation {ICD 503, NISPOM, System Security Plans (SSP), Security Concept of Operations (CONOPs), Security Architectures, and the Privileged User's Guide (PUG)}, along with developing test requirements and Risk Matrices. PC/Network Support Specialist ATK February 2006 to July 2012 Install, configure and maintain Teamcenter environment to include NX CAD, Femap, Autocad, Solidworks. Supported Teamcenter configuration and data management to include hardware, software, documentation. Troubleshoots, assigns and resolves Level I, II and III trouble tickets related to technical difficulties with hardware, software, and the network Maintained servers, desktops, and laptops Perform daily system monitoring, verified integrity and availability of all hardware Review system and application logs, and verify completion of scheduled jobs Interpret/analyze incidents and problems and provides technical support for hardware, software, and telecommunications systems Create, change, and delete AD user accounts per request Apply OS patches and upgrades on a regular basis, and upgrade administrative tools and utilities Perform periodic performance reporting to support capacity planning Perform ongoing performance tuning, hardware upgrades, and resource optimization as required Repair and recover from hardware or software failures Provide primary support for client computer access to network resources Install, configure and maintain computer hardware, peripherals and applications consistent with IT standards and processes Coordinate issues and solutions with other IT support personnel and users Work as a member of a team and provide

off-hours support when required Use tracking system to document issues and resolutions Ensure compliance with established company security policies and accepted risk impact to the business Maintain configuration management documentation Perform system and network administrative functions (review of system logs, backup activity) Troubleshoot hardware and software issues related to desktop systems and peripherals Diagnose and resolve problems in response to customer reported incidents Research, evaluate and provide feedback on problematic trends and patterns in customer support requirements Network Administrator Riverside County Regional Medical Center November 2001 to February 2006 Provide daily IT support in the areas of systems administration, customer support and network services Develop plans for installing, configuring, troubleshooting and maintaining user IT equipment and software Hands-on technical responsibilities include configuring, install and troubleshoot hardware, software and network products; coordinate maintenance of servers, workstations and peripherals Serve as focal point for user requests for IT server and workstation support and responsible for loading, configuring and maintaining OS; creating and managing network use accounts and shared folders; configuring and connecting client workstation to network/services and shared services Implement system diagnostic and maintenance tools to ensure the availability and functionality of systems Support Intel-based computers over life cycle to include setup/configuration, software installation, troubleshooting and maintenance; provide procurement recommendations; implement, manage/maintain Information Systems Architecture Plan, coordinate and execute the installation, configuration, upgrade, and maintenance of major OS operating environments Utilize systems diagnostic and maintenance tools to ensure the availability and functionality of major systems required to support organizational objectives and service level agreements Implement and maintain programs, policies and procedures to protect integrity and confidentiality of systems, networks and data. Perform image deployment using Ghost Reallocate resources in both real and virtual environments Perform Help Desk activities in accordance with service level agreements Manage accounts in a Netware environment, manage network rights and access to systems and equipment Perform System maintenance, system file backup, and system mass storage utilization including

data security Provide primary support for client computer access to network resources Install, configure and maintain computer hardware devices, peripherals and applications Install, configure and maintain network hardware (Cisco routers, HP switches, Network Interface Cards, servers) Technical Analyst The Toro Company January 2000 to November 2001 Provide primary, secondary and tertiary support for users of desktop computers and peripherals Provide primary support for client computer access to network resources Install, configure and maintain computer hardware, peripherals and applications consistent with IT standards and processes Coordinate issues and solutions with other IT support personnel and users Respond to user issues in a timely and effective manner. Work as a member of a team and provide off-hours support when required Use Remedy tracking system to document issues and resolutions Ensure compliance with established company security policies and accepted risk impact to the business Maintain configuration management documentation Perform system or network administrative functions (review of system logs, backup activity) Troubleshoot hardware and software issues related to desktop systems and peripherals Diagnose and mitigate basic network connectivity issues Deploy new hardware, peripherals (standalone or networked) and software Assist users via remote support tools or at the user's desk. Establish computer connections on existing networks Use operating system tools to mitigate system issues. Install and configure network and stand-alone printers Responsible for the refresh of leased and purchased computers Work with hardware/software vendors for leased/purchased items including maintenance agreements Data backup/archive. Monitor support activity and inform team/manager of any perceived trends, positive or negative, in calls being received and/or solutions being employed Analyze and resolve problems according to shifting priorities, time frames and resources, as well as documenting resolutions in call tracking system. Perform system or network administrative functions (review of system logs, backup activity) Provide local IT support for approximately 600 employees including Executives, office staff, and on-site meetings of senior leadership Primary on-site support for troubleshooting and installation of all desktop, telephony, and office IT issues which includes diagnosing and resolving hardware/software issues Assist with other remote IT staff in support of local office technologies

including server, network, and video systems Support projects and on-going activities for Netware monitoring and reporting systems Install, configure and maintain network hardware (Enterasys Routers and Switches) Education Community College of the Air Force Skills Vmware, Linux, Active Directory, System Admin, System Administrator Military Service Branch: United States Air Force Rank: E6

Name: Tracy Reed

Email: chapmandebra@example.org

Phone: (921)376-5003x21033