

MAJOR DUTIES AND RESPONSIBILITIES:

% OF TIME

A. Local Area Network (LAN) Management:

50%

- Manages a dynamic, robust Microsoft Windows PC/LAN environment utilizing DS/IRM approved network software like: Windows Server, SQL, SMS, MS Exchange .NET, Antivirus, Internet Information Server and others. Provides support to users of the MS Office suite applications (Word, Excel, Access, PowerPoint and Outlook) and DoS mandated applications. Full ICASS customer service and support extends to the 250+ users located throughout the US Mission LAN sites: the Chancery, Chief of Mission Residence, and the GSO Warehouse. Works with a ISM and two Assistant Network Administrators in the performance and upkeep of these duties.
- Provides full ICASS networking support to other agencies such as the Office of Defense Cooperation, Department of Justice, Department of Defense, Drug Enforcement Administration and others. Interfaces with these departments and parent agencies in Washington D.C. for hardware and software problem resolution. Confers with users to schedule work with minimum downtime and interruption.
- Analyzes Open Net performance on a regular basis to ensure optimum performance and data integrity. This includes, but is not limited to, analysis of disk space on network servers; review of backup procedures and tape retention policies, review of telecommunication links which may require coordination with the Information Resource Management (IRM) and various Department of State telecommunications entities; management of e-mail mailboxes and regular housekeeping of files; monitors server event logs, researches causes of errors and events and develops solutions to rectify problems.
- Maintains networking equipment such as routers, switches, and hubs utilizing common telecommunications and networking protocols such as TCP/IP, FTP, etc. Configures IP addressing and sub netting schemes using the Department standard Cisco Network Registrar as well as industry standard WINS and DHCP. Works with ENMOC program offices to ensure that all routers and switches perform optimally on the network. Regularly monitors and tests the VPN alternate routing circuit and associated equipment to ensure a viable backup path is available. Assists in the documentation for network diagramming. Keeps the ISM and Information Systems Officer (ISO) informed of any problems that are detected.
- Oversees the security of the computer systems and the data resident on the file servers. This involves directing and monitoring ISC operations staff in computer room physical security, devising policies, procedures, and documentation for the issuing, deleting and maintenance of passwords, controlling user access to shared folders and application software, and for ensuring the physical security of off-site tape storage. Ensures anti-virus software updates are always current on the servers and updates are regularly propagated to workstations.
- Develop new and maintain new and existing web enable application based on specific tasking from the Senior Computer Management Assistant or Information Systems Officer. Typical front end coding in web page creation software like Macromedia Dreamweaver, ColdFusion or Microsoft Visual Interdev. The SQL database creation / maintenance requires breaking down a data storage requirement into normalized tables and the wisdom to discern when to "de-normalize" tables to boost query performance.
- Provide user access to the application in accordance with Diplomatic Security guidelines. Study and remain current on Department of State security requirements for Windows 2000 and beyond, and web server hosting software as IIS4, W2K IIS5 and beyond. Analyst must also be responsible for file structure and management, log files, disk space utilization, etc.

B. LAN Security and Development:

30%

- Applies server security requirements for Windows 200X, MS Exchange and other basic applications as required by DS. Applies system policies to networked workstations and defines user profiles. Works with the Information Systems Security Officer (ISSO) and Diplomatic Security (DS) security teams during review processes whether performed locally or remotely.
- Responsible for the installation of service packs and software upgrades of the network operating system and electronic mail servers. Analyzes tests and installs major proprietary application software packages developed by various offices with the Department.
- Responsible for the maintenance and development of the network backbone and upgrade of networking hardware and software to support new services, video, video-conferencing, etc. and ensures security standards are not compromised with the implementation of these technologies.
- Using standard Department guidelines, such as the Foreign Affairs Manuals, telegram instruction and the Open Net Plus connection approval process, develops Standard Operating Procedures (SOP) for network start up and shut down, daily and weekly data backups, file reorganizations, system performance monitoring, MS Exchange directory operations, DHCP and WINS monitoring, and other network operations. Develops and maintains the IT contingency plan to ensure operations are restored in a timely manner in the event of a catastrophe.
- Serves as an alternate primary technical contact for the Bureau of Consular Affairs' automated systems and maintains the CA infrastructure to include server and workstation operating systems, database servers and standby backup equipment. Oversees the daily, weekly and monthly CA routines, and writes Standard Operating Procedures for these routines and ensures other ISC staff members are kept abreast of changes in CA computer operations. Works as an ISC team for CA/Orkand Refresh visits and coordinates all contact with the CA Support Desk for troubleshooting problems and testing application distribution on servers and workstations.
- Acts as an advisor to provide reliable, up-to-date information to the ISM, the ISO and Information Management Officer (IMO) for whatever pertains to network projects, future directions, infrastructure planning, implementation strategies and procedures. Works closely with the Systems Analysis staff to plan the implementation of new procedures, tools, equipment and software for major network changes. Analyzes and proposes requirements for

expansion, modifications, hardware and software upgrades to maintain or enhance network operations. Assists in planning additions/deletions of future and current sub-sites of this post as well as possible migrations to new locations in the realm of contingency planning. Assists in providing implementation procedures and graphic documentation needed for these projects.

- Keeps abreast of new software developments, hardware products and advances in computer operations to give guidance and information to management and users on such technical matters. Gathers information on a wide variety of ADP topics requested by the ISM and ISO. Acts as liaison with external technical support sources and service providers. Represents or assists the ISO at meetings. In coordination with the ISM and ISO, identifies and schedules formal training courses needed to keep the staff technically up-to-date.
- Sets up standalone workstations and designs mini-LANs as needed for special projects, such as VIP visits, Ambassadors /DCM residences or CA on-site training.

20%

C. Software and Network Development:

- Develops logon scripts to facilitate user logons and batch jobs to perform routine network functions. Works with developers of macros and templates to provide wide user availability and appropriate access to improve the work process of offices throughout the Mission.
- Participates in the implementation of newly developed software to the extent necessary to ensure that the operations staff, training personnel and end-users, develops sufficient understanding of the software and its features. Ensures new software has been thoroughly tested for compatibility with the network operating system and conflict resolution with other applications before installation.
- Assists with DVC presentation and intranet website updates.
- Assists in planning, budgeting and procuring hardware and software required for the network, using U.S. government contracts to obtain the best prices.

D. Training and End user Education:

- The incumbent will provide specific application training for end users on both Department of State developed applications, locally developed application and authorized software. This training will be conducted in both a formal classroom setting as well as through developed educational materials.
- Must be able to conduct on end user education of any of the post supported applications and software products.