Department of Telecommunications & Information Services
Operations & Infrastructure Division
Network Architecture version 3.0

Date: July 14, 2008

Subject: **Networking Requirements & Standards for City RFP's**

Departments and agencies within the City and County of San Francisco attain IT systems through a procurement process. Part of the City's procurement process is the issuing of RFPs or "Request for Proposals". Proposed systems/applications may be used on a single LAN (local area network) within a department or may be utilized by several departments in addition to the primary department and in some cases are 'enterprise' applications, in which case all or nearly all departments need some access.

The following lists various City & County network requirements, standards, and policies with regard to applications that run on the City network. While most of these requirements and standards pertain to applications that are utilized by more than a single department, or at minimum traverse the City's WAN (wide area network), other requirements may pertain to the ability of a vendor to comply with City standards/preferences in order to gain access to and provide ongoing support for a system.

1. Wide Area Network: TCP/IP

- All applications/system that must utilize TCP/IP as their native protocol.
- The City does not allow Netbeui or Netbios to traverse subnets. Running TCPbuei is not allowed.
- The City's WAN does not currently allow Microsoft CIFS based 'file sharing' across WAN links.

2. Web enabled applications

- The City prefers user interfaces based on open WEB standards, commonly accessed via ports 80 and 443. Applications that are accessed from more than one subnet (LAN) must provide a WEB based interface for its users.
- Because of internal firewalls and other security mechanisms, web based applications are the easiest to manage across the City's network. If a vendor's application utilizes a non-web interface then some additional requirements must be meet.
- In responding to a RFP, the vendor must clarify whether or not all users (including the application administrators) will be able to access their portion of the application via a WEB based interface. Some applications require a client-server type interfaces to optimize performance or provide a specialized interface for some types of users, typically administrators. The vendor must provide specific details regarding what parts of their application are only accessible through the client server application interface and which users will need to utilize client-server interfaces in order to effectively perform their tasks.

3. Client-server application requirements

- The vendor needs to provide a list of specific TCP/IP ports (IP and UDP) utilized by their application. In providing the list of ports, the vendor must include a description of what function or use a particular port supports. The vendor must assume that all ports not specified will be blocked.
- The vendor needs to specify whether or not the application can use specific IP ports. Some applications by default may use a specific port to initiate communications and then use a random high-numbered port for the actual data communications. The vendor needs to specify whether or not their application can be configured to use specific ports or a small range of ports rather than any random port. DTIS WAN Engineers manage availability of high numbered ports open across specific WAN connections based upon the specific applications.

4. Virtualization Support

- Reducing data-center costs and GreenIT initiatives are important for City's environment. The vendor must indicate whether or not their application will run in a virtual server (VmWare, HyperVisor, etc.) environment. Please provide performance statistics for application in a virtual environment.

5. Redundancy & Business continuity

- Based on the application critical rating, the vendor must provide a recommendation of the best-practice for application redundancy (Load balancing, replication, etc) and business continuity plan.

6. Citrix and/or Windows Terminal Server Support

- The vendor must indicate whether or not their application can run in a Citrix and/or Windows Terminal Server environment. Some City employees are mobile and may be utilizing a laptop with a wireless internet connection (with VPN providing tunneling and encryption for security). Such wireless connections are of low bandwidth running 400-700 Kbps. We currently do not have a Citrix or Windows Terminal Server offering. If the vendor requires the use of these offerings they must include the cost for the environment.

7. Public Access via the Internet

- The City requires that servers hosting applications that are accessible to the general public run from and reside in an Internet DMZ subnet. Therefore, a public WEB server resides in the DMZ while data typically resides on a server within the internal city network. The vendor must indicate whether this can be supported and must specify which IP ports are utilized for communication between the DMZ hosted WEB server and internal database.
- The WEB application must be able to access database servers on specific ports (rather than random high numbered ports) since it must traverse a firewall. DTIS will not open up all high numbered ports for a WEB server in the DMZ to access the internal network.

8. Vendor On-Site Access

- Maintenance/support of an application may be provided by an outside vendor. In such cases, when the vendor is on-site to provide support, they will typically bring their own laptop to connect to the network. The vendor's laptop must have a:
    - Commercially available anti-virus software which is current and up-to-date with the latest virus patterns loaded.
    - Currently supported version of Windows (Windows XP) with all current Microsoft security patches installed.
    - All patches and software tools necessary for support loaded onto their laptop.
    - If access to the Internet is needed, vendor must provide wireless broadband access.

9. Vendor Remote Access Support

- Maintenance/support of an application may be provided by an outside vendor. In such cases, the support may require remote access to the servers on which the application runs.
- The City views dial-in access directly to a modem on the server as a security risk. The City provides two means of establishing remote access through the Internet:
    a. The vendor may establish a site-to-site VPN connection with a Cisco VPN Gateway utilizing IPSEC. In this scenario, the vendor must provide a specific subnet on their internal network which is utilized by their technical support team that will be providing access to the City. This subnet must be accessible only to the technical staff that would be supporting the vendor's application running in the City.
    b. The vendor's technical support staff may establish a user VPN session with the City network. The staff would need to load the Cisco VPN client on their PC or laptop. The vendor is responsible for their VPN user account(s). If an employee leaves the company, the vendor is responsible for changing the VPN password so the former employee is no longer able to access the City's network by VPN. The vendor is liable for all activity performed by any person using the vendor's VPN account(s) with the City.
    c. The vendor must renew the VPN account every six months.
- The vendor must provide the specific IP ports needed to access and support their application. In some cases, it may be standard Port 80 access if utilizing a WEB interface or Port 3389 if utilizing Windows Terminal Services on a Windows based server.

10. Databases Standards

The application must support either Oracle or Microsoft SQL as their database. The vendor must indicate which of the two databases are supported. If another Database is supported, then vendor must own support of the database.

11. FTP

To support exporting and importing of data, file transfers must be able to utilize specific IP ports, rather than choosing a high numbered port dynamically. The vendor will need to indicate if the operating systems which are certified for their application can support file transfers utilizing specific IP ports. (Note: some versions of Microsoft Windows cannot support this requirement.)

12. Login / Authentication

City is investigating single sign-on and an enterprise-wide authentication service. The vendor's application must be able to:

- Provide local authentication within the application.
- Provide the option to authenticate users through a centralized directory service such as LDAP, Novell's E-Directory, or Microsoft's Active Directory.
- Provide the option to authenticate users through a SAML2.0 web service.

Users must NOT be required to log on through an application servers local operating system. In other words, they must NOT have to log onto the Windows server as a user, in order to access the application. The application may utilize Window's local accounts to provide user authentication to the application or provide its own internal authentication system. Access rights within the application (what a user can access once he/she has authenticated) must be determined through "rights" management through the application or database.

13. Security

- For applications which provide public access (via a WEB server in the DMZ), it is imperative that the application be able to limit the types of queries and data accessible to the DMZ based WEB server. The application must be able to limit which fields within a database record can be read and/or written to by the public facing WEB server.
- The vendor must state what 'pre-editing' is being done on user input. Is all user input pre-edited prior to transactions occurring? This is to insure that the application limits the potential for SQL injection attacks.
- SSL encryption must be supported for WEB applications.
- Data encryption for storage of confidential data must be supported. Data classification should be flexible and defined by application administrators.

14. Bandwidth Requirements

- The vendor shall provide data regarding bandwidth requirements and or usage for various types of users using either WEB or full client-server application clients. The vendor must provide data regarding how many users on average can access their application across a T-1 link using each client type.
- Sniffer data trace of a typical "login" and use of the application must be provided.