ATTACHMENT J-12

SDPS SITE PLAN AND INVENTORY

December 17, 2007

SDPS INFRASTRUCTURE PLANNING

OVERVIEW

This document contains minimum guidelines each site should follow in preparing their site for the installation of the SDPS systems.

SDPS SYSTEMS

- Wide Area Network Equipment (WAN)
    - Router
    - CSU/DSU
    - Infrastructure Cabling
- Local Area Network Equipment (LAN)
    - Switch
    - Server
    - Desktop
    - Printer
    - Infrastructure Cabling

GENERAL GUIDELINES

Technology is constantly changing. Therefore the standards contained within this document represent minimum recommended standards. Cabling infrastructure should be designed to support the network requirements for 10 to 15 years. Installing additional infrastructure capability today adds minimal expense compared to adding more in the future.

The Electronic Industries Association (EIA) and the Telecommunications Industry Association (TIA) have drafted a standard for commercial building wiring. The EIA/TIA-568 standard addresses voice, data and video cabling.

- Backbone Cable Plant -- the connection between the communication closet and the equipment room within a building, and the connection between buildings.

- Horizontal Cable Plant -- the connection between, and including, the outlet and the termination in the communication closet. Category 5 (CAT 5) cable and two fiber (duplex) 62.5/125 micron multi-mode fiber terminated with SC connectors are the minimum cable standards

    - The horizontal cabling plant should adhere to the standard for distances and media interface as defined in the IEEE 802.3 Ethernet standards.

Copper Standards

- CAT 5
  - Max Data Rate -- 1000 Mbps
  - Usual Application – Ethernet 10/100 Mbps
  - *Maximum Segment Length – 100 meters

- CAT 5E
  - Max Data Rate -- 1000 Mbps
  - Usual Application – Ethernet 10/100/1000 Mbps
  - *Maximum Segment Length – 100 meters

- CAT 6
  - Max Data Rate – 400 MHz
  - Usual Application – Super-fast broadband applications Most popular cabling for new installs
  - *Maximum Segment Length – 100 meters
- CAT 6E
  - Max Data Rate – 625 MHz
  - Usual Application – Support for 10 Gigabit Ethernet
  - *Maximum Segment Length – 100 meters

- *Note - A segment includes all cables from switch port to NIC

Fiber Standards

- Multimode Fiber
  - Multimode fiber optic cable can be used for most general fiber applications. Multimode cable comes with two different core sizes: 50 micron or 62.5 micron.
- Single-mode Fiber
  - Single-mode is used over distances longer than a few miles. Single-mode cable features an 8.5-micron glass core.
- Fiber termination
  - SC Connectors

- Work Area Cable Plant -- an area containing a station and the connection between the station and outlet.

  - Patch cords are available in various lengths and are manufactured from all cable CAT types.

- The entire cable plant should be documented for future maintainability. All newly installed cables should be labeled on both ends with a location identifier and the cable type.

WAN ACCESS

The local Telco will deliver the SDPS circuit to the demarcation (demarc) point in the building. A demarc is the transition point between the Telco and the local administrator circuit responsibility. Normally, the demarc is located in space controlled by the building management and the space will support all tenants in the building. An extended demarc extends the transition point from the demarc to your office space where the network equipment will be located. The local Telco is responsible for any problems up to the extended demarc. Your administrator is responsible from the extended demarc back to the LAN equipment.

The extended demarc should be located within a few meters of the network equipment. The WAN network equipment preferably should be mounted in an equipment rack but may be mounted on the wall or shelve. From the extended demarc a straight through twisted pair cable is connected to a CSU/DSU. This could be a separate device or integrated into the router WAN interface. If the CSU/DSU is a separate device, a serial cable is required to connect the CSU/DSU to the serial interface of the router. The Ethernet interface of the router is connected to the network switch.

LAN ACCESS

The network switch connects to all network devices. Network devices include but are not limited to desktops, laptops, servers, printers and VTC equipment. Depending on the number of users and equipment, your site may have one switch, several switches stacked together in one location or switches located in multiple locations (remote closet). The LAN network equipment should be mounted with the WAN network equipment. In the communication closet the horizontal cable run will terminate at a patch panel position. The other end will terminate at a RJ45 wall plate in the office areas. Both cable ends must be properly terminated using TIA 568 standards. The same standards, TIA 568A or TIA 568B must be used on both ends of the cable. The patch panel position and the corresponding wall plate should be labeled with location identifiers. A patch cable will be used to connect a network device, (e.g. workstation, printer) to the wall plate of the horizontal cabling plant and then from the patch panel to the network switch.

Attachment J-12 SDPS Site Plan and Inventory

SECURITY

When identifying an area for the SDPS system, consider that equipment should be sheltered from tampering, either accidental or deliberate, and theft. The SDPS computer area should have locks and should be accessible only to authorized personnel. Hinges on the doors should face in toward the locked area. Your computer facility should be protected by use of fire rated walls, ceiling, and doors. Emergency exit doors, where used, should have panic locks, and be appropriately marked.

A great many problems can be eliminated by taking simple precautions in setting up the network environment. Network components should be physically secured. Whenever possible the file server, switch, and other communication equipment should be securely mounted in a rack.

DATA SECURITY

The following are some good practices that are effective in securing company data

- Only authorized personnel should be allowed in the computer room
- The site should maintain backup copies of data on all servers on a regular basis
- The site should have an off-site backup data storage system which will be used to store backup media vital documentation, and archival material
- Whenever possible use UPS devices to protect the electrical supply to computer equipment and air-conditioning
- The site should have a contingency plan to get vital services performed in case of fire or flood
- All site personnel should be educated about computer viruses and virus prevention.
- Users should be required to logoff when they leave their workstations.

COMPUTER CENTER ACCESS CONTROL

The following guidelines are suggested:

- Access to the computer area should be controlled at all times.
- Methods of access control
    - Keyed entry
    - Card reader entry
    - Cipher lock entry
- Visitors should be escorted within the computing facility at all times and must relinquish the temporary badge upon departing the facility
- Visitor badges should be controlled and must be accounted for at the end of each business day.

DOOR LOCKS AND ACCESS CODES

Cipher locks can be used to control access to the computer room and backup storage area. The cipher combination should be changed if one of the following events occurs:

- An employee leaves the organization
- There is reason to believe that an unauthorized person has acquired knowledge of the combination
- A predetermined time interval, such as six months, passes.

If one of the first two events takes place, have the combination changed as soon as possible (usually within 24 hours). The new combination should then be verbally communicated to authorized personnel. Cipher lock combination changes should never be communicated in writing.

ENVIRONMENTAL CONTROLS

Rising temperatures cause computer components to expand and accordingly, falling temperature make them contract. Always maintain as consistent a temperature as possible around computer equipment. Temperature in the CPU is affected by powering the computer down and bringing it back up again. Avoiding powering the equipment up and down unnecessarily will greatly improve the longevity and reliability of your equipment. However, unless your computer area is electronically monitored for loss of cooling (high temperature alarm) it may be required to power equipment off when unattended to guard against potential damage.

Environmental pollutants, such as dust, can be brought into the chassis by the fan, and can cause problem over time. Magnetism can corrupt computer data. The area chosen to house the SDPS system should not be near any large electric forces such as massive electric motors, etc. Magnetic objects should be banished from the computer area.

AIR COOLING AND HUMIDITY CONTROL

The air cooling and humidity control requirements for the SDPS system area are an environmentally controlled room able to maintain:

- A temperature range of 60.8 to 89.6 degrees Fahrenheit (based on a heat generation rate of computed from Figure 4 below)
- A humidity range of 8 to 80 percent.

ELECTRICAL REQUIREMENTS

The site organizations will be required to provide dedicated electric circuits for key SDPS system components. Workstations and printers are not required to be on dedicated circuitry, however, it is recommended. If your organization chooses not to provide dedicated circuits in support of workstations and printers, the following points should be considered:

- Older buildings, with older electrical wiring systems will most likely have more problems with computer down time
- Whenever possible, workstations and printers should not be plugged into the same circuit as non-data processing equipment like copiers and microwaves that could cause power fluctuations
- If in doubt always consult a licensed electrician.
- Each workstation or printer should be plugged into to its own surge protector.

To safeguard SDPS workstations, electric surge protection devices are suggested but will not be provided with the SDPS system.

DISCLAIMER: This document has been downloaded from the CMS Quality Improvement Organization (QIO) Program website on www.cms.hhs.gov/QualityImprovementOrgs/04_9thSOW.asp. This document is current as of January 23, 2008. This document is provided on the CMS website for informational purposes only and should not be used as an official document to prepare a response to CMS' contract proposal solicitation. Please refer to the FedBizOpps website at www.fbo.gov to obtain the official version of the documents that comprise the Request for Proposals (RFP) package to be used when responding to CMS' contract proposal solicitation.