

ASPEN user must have both a security profile that allows a specific function to be performed, and be assigned to appropriate Provider Type access before a specific system action may be taken against a provider/supplier type.

- *Secondary Database Access*

*Control:* Since ASPEN provides an Application-centric security model, it is not necessary to assign each ASPEN user an individual Oracle user name, password and Oracle profile. Instead, all ASPEN users share a single Oracle login whose password is known only by CMS. This protects against a significant threat to data integrity: access to the Oracle database using non-ASPEN system tools; thus, preventing accidental or malicious bypassing of the ASPEN security controls through third-party system tools which may be capable of connecting to Oracle databases. ACTS users may only access ASPEN data via the security-controlled environment of the ACTS application.

- *Audit trail:* ACTS maintains an audit trail for key information elements in the database. Any changes made to these elements via the ACTS system are logged. The log includes information on which element was changed, who changed it, the time of change and prior and current values for the element.

#### *B. Physical Safeguards*

All server sites have implemented the following minimum requirements to assist in reducing the exposure of computer equipment and thus achieve an optimum level of protection and security for the ACTS system:

Access to all servers is controlled, with access limited to only those support personnel with a demonstrated need for access. Servers are to be kept in a locked room accessible only by specified management and system support personnel. Each server requires a specific log-on process. All entrance doors are identified and marked. A log is kept of all personnel who were issued a security card, key and/or combination that grants access to the room housing the server, and all visitors are escorted while in this room. All servers are housed in an area where appropriate environmental security controls are implemented, which include measures implemented to mitigate damage to Automated Information Systems resources caused by fire, electricity, water and inadequate climate controls.

Protection applied to the system administration workstations and the Windows 2000 servers, which house the ACTS Oracle database, include:

- *User Log-ons*—Authentication is performed by the Windows 2000

Primary Domain Controller/Backup Domain Controller of the log-on domain.

- *Workstation Names*—Workstation naming conventions may be defined and implemented at the State agency level.

- *Hours of Operation*—May be restricted by Windows 2000. When activated all applicable processes will automatically shut down at a specific time and not be permitted to resume until the predetermined time. The appropriate hours of operation are determined and implemented at the State agency level.

- *Inactivity Log-out*—Access to the 2000 workstation is automatically logged out after a specified period of inactivity.

- *Warnings*—Legal notices and security warnings display on all servers and workstations.

There are several levels of security found in the overall ASPEN system. Windows 2000 servers provide much of the overall system security. The Windows 2000 security model is designed to meet the C2-level criteria as defined by the U.S. Department of Defense's Trusted Computer System Evaluation Criteria document (DoD 5200.28-STD, December 1985). Other non-ACTS CMS functions are supported on the same Windows 2000/Oracle servers as ACTS—such as MDS submission from facilities. Such operations are performed via separate Netscape Enterprise Server, which provides an additional layer of user authentication, security and access control. In this case, Netscape controls all CMS information access requests. Anti-virus system is applied at both the system administration workstation and Windows 2000 server levels.

Access to different areas on the Windows NT server is maintained through the use of file, directory and share level permissions. These different levels of access control provide security that is managed at the user and group level within the Windows 2000 server domain. The file and directory level access controls rely on the presence of a Windows NT File System (NTFS) hard drive partition. This provides the most robust security and is tied directly to the file system. Windows 2000 security is applied at both the workstation and Windows 2000 server levels.

Firewalls have been installed on each State server. Appendix A lists the location of each State server. A firewall is a security feature that does not allow unwanted or unsolicited network traffic to flow to certain parts of the system. A Cisco 3640 router is installed at each state. These routers have been programmed to allow the state IP addresses to access certain locations

within the CMS network. CMS contractors set up and manage the routers. Using CMS specifications, they have installed the allowed IP's to the router tables. If an unauthorized IP tries to access the CMS data, the firewall (router) will pass the request away from its intended destination. That is, if the firewall does not match the IP of the request to an allowed IP in its table, the request will not be fulfilled. CMS contractors monitor the firewalls and review them for anomalies that could represent a hacking attempt or a hardware problem.

#### *C. Procedural Safeguards*

All automated systems must comply with Federal and State laws, guidance, and policies for information systems security, as stated previously in this section. Each State must ensure a level of security commensurate with the level of sensitivity of the data, risk, and magnitude of the harm that may result from the loss, misuse, disclosure, or modification of the information contained in the system.

#### **V. Effects of the Proposed System of Records on Individual Rights**

CMS proposes to establish this system in accordance with the principles and requirements of the Privacy Act and will collect, use, and disseminate information only as prescribed therein. Data in this system will be subject to the authorized releases in accordance with the routine uses identified in this system of records. CMS and the State Survey Agencies will monitor the collection and reporting of ACTS data.

CMS and the State Survey Agencies will take precautionary measures to minimize the risks of unauthorized access to the records and the potential harm to individual privacy or other personal or property rights of individuals whose data are maintained in the system. CMS will collect only that information necessary to perform the system's functions.

To ensure data that resides in a CMS Privacy Act System of Records; to ensure the integrity, security, and confidentiality of information maintained by CMS; and to permit appropriate disclosure and use of such data as permitted by law, CMS and the non-CMS recipient of the data, hereafter termed "User," enter into an agreement to comply with the following specific requirements. The agreement addresses the conditions under which CMS will disclose and the user will obtain and use the information contained in the system of records. The parties mutually agree that CMS retains ownership rights to the data and that the user does not