Remote Terminal Access System Protection Measures

Remote terminal access by system participants must be approved by the Office of Justice Programs (§23.20(i)(1) if the system is subject to 28 CFR Part 23 due to the funding requirement. Below are the system protection measures that should be implemented for remote terminal access (1993 Revision and Commentary, Operating Principles - §23.20(i)).

1. Procedures for identification of authorized remote terminals and security of terminals.
2. Authorized-access officer (remote-terminal operator) identification and verification procedures.
3. Provisions for the levels of dissemination of information as directed by the submitting agency.
4. Provisions for the rejection of submissions unless critical data fields are completed.
5. Technological safeguards on system access, use, dissemination, and review and purge.
6. Physical security of the system.
7. Training and certification of system-participating agency personnel.
8. Provisions for the audit of system-participating agencies, to include file data supporting submissions to the system, security of access terminals, and policy-and-procedures compliance.
9. Documentation for audit trails of the entire system operation.

A "remote terminal" is hardware that enables a participating agency or user to input into or access information from a project's criminal intelligence database without the intervention of project staff. While the security measures set forth in §23.20(g)(1)-(5) should minimize the threat to system integrity from unauthorized access to and use of system information, special measures are called for when direct remote-terminal access is used.