Appendix 5
Summary of NIH Policy On Remote Access to the NIHnet

Purpose: Establishes the necessary policy and procedures for NIH remote access approval and use, and establishes good management controls that can be used by managers NIH-wide in managing their remote access accounts/users. Remote Access is defined as: Electronic access to the NIHnet by authorized users not located at their normal worksite, e.g., traveling with a laptop computer or working at home.

Below is a summary of some of the major issues covered in the complete policy at http://www3.od.nih.gov/oma/manualchapters/acquisitions/26101-26-08.

CIT Role – CIT is responsible for managing the NIHnet and overseeing the NIH remote access program.

IC Role – The IC EOs or designee(s), in conjunction with their IC CIOs, are responsible for approving the use of and managing remote access resources in accordance with the NIH Remote Access policy; this includes taking disciplinary action, as appropriate, when resources are used inappropriately.

IC shall use more rigorous remote access procedures for systems with highly sensitive information such as patient records. See NIH Sensitivity Level Designations at http://irm.cit.nih.gov/policy/DHHS_SecLev.html. For example, stronger authentication through technologies such as biometrics or smart cards may be warranted in some instances (NIH Password Policy, http://irm.cit.nih.gov/security/pwd_guidelines.html).

Remote Access User and Role - Individuals who have been approved by their respective IC management to use the NIHnet and resources through remote access are responsible for ensuring that adequate safeguards are implemented to protect the integrity of the NIHnet and associated resources. All Remote Access Users must adhere to the NIH Remote Access Security Standards and Procedures which detail the appropriate operation and use of remote systems and the NIHnet by all parties involved in the remote access process http://irm.cit.nih.gov/security/sec_policy.html.

Individuals who have been approved by their respective IC management to use the NIHnet and resources through remote access are responsible for ensuring that adequate safeguards are implemented to protect the integrity of the NIHnet and associated resources. Users must exercise good judgment and use NIH-owned resources in accordance with the Limited Authorized Personal Use of NIH Information Technology Resources Policy at http://www3.od.nih.gov/oma/manualchapters/management/2806/.

Procedures
Procedures and requirements for acquiring the various NIH-provided remote access services are described at http://irm.cit.nih.gov/nihsecurity/NIH_RAS_Pol.pdf . Also, IC IT computer support responsible for establishing remote access connections for an IC user should be familiar with the NIH Remote Access Security Standards and Procedures at http://irm.cit.nih.gov/nihsecurity/NIH_RAS_Sec_Stand_Proc.pdf and/or contact their IC Information System Security Officer to ensure that access is appropriately established and secure in accordance with the aforementioned policy documents.

Use of Appropriated Funds for Data Lines - ICs may use appropriated funds for the installation of data lines in private residences. Current legislation restricts the use of appropriated funds for telephone (voice) line installation in private residences unless the individual is approved to work under an approved Telework or Flexible Workplace program.

Appendix 5
Summary of NIH Policy On Remote Access to the NIHnet

Management Controls - In an effort to establish or strengthen the existing management control aspects of the remote access program, the following mechanisms have been implemented:

- Remote Access User Agreement – to protect NIH remote access resources and the NIHnet. Users MUST read, sign and renew ANNUALLY a Remote Access user agreement form (http://irm.cit.nih.gov/security/RA_User_Cert_Agreemt.doc) which summarizes the remote access policy and user responsibilities. The approving official (EO) must also sign this form before remote access can be established or continued. Users should abide by all NIH (and other fed) policies/regulations that apply, e.g., IT—security, appropriate use, personal property, etc.

- Approved method(s) for accessing the NIHnet - remote access to the NIHnet must be routed through secure, approved services provided by CIT (NIH VPN or PARACHUTE) or an IC-provided service that has been approved as an exception by the NIH CIO and complies with DHHS security requirements and the NIH Remote Access Security Standards and Procedures. The policy requires all remote access users, including NIH employees, contractors, and other authorized users, to sign the NIH Remote Access User Certification Agreement (http://irm.cit.nih.gov/security/RA_User_Cert_Agreemt.doc).

- Web Sponsor **-**
  Accounts - Users must apply for CIT-provided or supported remote access service accounts covered in this chapter (Parachute, cable modem, etc.) via their Account Sponsor (Web Sponsor). Before application is made, the individual must have supervisor approval.

  Reports – IC Account Sponsors will now be able to review user data on all CIT-provided or supported services through the Web Sponsor database as needed. Hardcopy reports are e-mailed to the IC Eos for verification/validation.

ICs are responsible for reviewing (and documenting their review of these reports) and completing a more comprehensive review of the accounts on an at least annual basis.

General Information and Technical Assistance on Remote Access Services - For additional information on remote access connectivity options, costs, and other services, see the NIH Remote Access web site at http://remoteaccess.nih.gov or call **GO-CIT** (301-594-6248).