In contrast, hardware approaches involve placing a device inside the user's home that is physically connected to the consumer's Internet connection, and periodically running tests to remote targets on the Internet. These hardware devices are not reliant on the user's workstation being switched on, and so allow results to be gathered throughout the day and night. The primary disadvantages of a hardware approach are that this solution is much more expensive than a software approach and requires installation of the hardware by the consumer or a third party.

B. Design Principles and Technical Approach

For this test of broadband performance, the FCC adopted design principles that were previously developed by SamKnows in conjunction with their study of broadband performance in the U.K. The design principles comprise seventeen technical objectives:

Technical Objectives	Methodological Accommodations
1. Must not change during the monitoring period.	The Whitebox measurement process is designed to provide automatic and consistent monitoring throughout the measurement period.
2. Must be accurate and reliable.	The hardware solution provides a uniform and consistent measurement of data across a broad range of participants.
3. Must not interrupt or unduly degrade the consumer's use of the broadband connection.	The volume of data produced by tests is controlled to avoid interfering with panelists' overall broadband experience, and tests only execute when consumer is not making heavy use of the connection.
4. Must not allow collected data to be distorted by any use of the broadband connection by other applications on the host PC and other devices in the home.	The hardware solution is designed not to interfere with the host PC and is not dependent on that PC.
5. Must not rely on the knowledge, skills and participation of the consumer for its ongoing operation once installed.	The Whitebox is "plug-and-play." Instructions are graphics-based and the installation process has been substantially field tested.
6. Must not collect data that might be deemed to be personal to the consumer without consent.	The data collection process is explained in plain language and consumers are asked for their consent regarding the use of their personal data as defined by any

	relevant data protection legislation.
7. Must be easy for a consumer to completely remove any hardware and/or software components if they do not wish to continue with the research program.	Whiteboxes can be disconnected at any time from the home network. As soon as the route is reconnected the reporting is resumed as before.
8. Must be compatible with a wide range of DSL, cable, and fiber-to-the-home modems.	Whiteboxes can be can connected to all modem types commonly used to support broadband services in the U.S. either in an in-line or bridging mode.
9. Where applicable, must be compatible with a range of computer operating systems, including, without limitation, Windows XP, Windows Vista, Windows 7, Mac OS and Linux.	Whiteboxes are independent of the PC operating system and therefore able to provide testing with all devices regardless of operating system.
10. Must not expose the volunteer's home network to increased security risk, *i.e.*, it should not be susceptible to viruses, and should not degrade the effectiveness of the user's existing firewalls, antivirus and spyware software.	Most user firewalls, antivirus and spyware systems are PC-based. The Whitebox is plugged in to the broadband connection "before" the PC. Its activity is transparent and does not interfere with those protections.
11. Must be upgradeable from the remote control center if it contains any software or firmware components.	The Whitebox can be completely controlled remotely for updates without involvement of the consumer PC, providing the Whitebox is switched on and connected.
12. Must identify when a user changes broadband provider or package (*e.g.*, by a reverse look up of the consumer's IP address to check provider, and by capturing changes in modem connection speed to identify changes in package).	Ensured regular data pool monitoring for changes in speed, ISP, IP address or performance, and flagged when a panelist should notify and confirm any change to their broadband service since the last test execution.

13. Must permit, in the event of a merger between ISPs, separate analysis of the customers of each of the merged ISP's predecessors.	Data are stored based on the ISP of the panelist, and therefore can be analyzed by individual ISP or as an aggregated dataset.
14. Must identify if the consumer's computer is being used on a number of different fixed networks (*e.g.*, if it is a laptop).	The Whiteboxes are broadband dependent, not PC or laptop dependent.
15. Must identify when a specific household stops providing data.	The Whitebox needs to be connected and switched on to push data. If it is switched off or disconnected its absence is detected at the next data push process.
16. Must not require an amount of data to be downloaded which may materially impact any data limits, usage policy, or traffic shaping applicable to the broadband service.	The data volume generated by the information collected does not exceed any policies set by ISPs. Panelists with bandwidth restrictions can have their tests set accordingly.
17. Must limit the possibility for ISPs to identify the broadband connections which form their panel and therefore potentially "game" the data by providing different quality of service to the panel members and to the wider customer base.	ISPs signed a Code of Conduct[18] to protect against gaming test results. While the identity of each panelist was made known to the ISP as part of the speed tier validation process, the actual Unit ID for the associated Whitebox was not released to the ISP and specific test results were not directly assignable against a specific panelist. Moreover, most ISPs had hundreds, and some had more than 1,000, participating subscribers spread throughout their service territory, making it difficult to improve service for participating subscribers without improving service for all subscribers.

[18] Signatories to the Code of Conduct are: Adtran, AT&T, Cablevision, CenturyLink, Charter, Comcast, Corning, Cox, Fiber to the Home Council, Frontier, Georgia Tech, Insight, Intel, Mediacom, MIT, Motorola, National Cable Television Association (NCTA), Qwest, TimeWarner Cable, US Telecom, Verizon, and Windstream. A copy of the Code of Conduct is included as a Reference Document attached to this Appendix.