Analysis of Proposed Consent Order to Aid Public Comment
In the Matter of ASUSTeK Computer, Inc.

iii. prevent consumers from using weak default login credentials. For example, respondent allowed consumers to retain weak default login credentials to protect critical functions, such as username “admin” and password “admin” for the admin console, and username “Family” and password “Family” for the AiDisk FTP server;

b. perform reasonable and appropriate code review and testing of the software to verify that access to data is restricted consistent with a user’s privacy and security settings;

c. perform vulnerability and penetration testing of the software, including for well known and reasonably foreseeable vulnerabilities that could be exploited to gain unauthorized access to consumers’ sensitive personal information and local networks, such as authentication bypass, cleartext password disclosure, cross-site scripting, cross-site request forgery, and buffer overflow vulnerabilities;

d. implement readily

arrangement, or any other circumstances that it knows or has reason to know may have a material impact on its security program.

Part III of the proposed consent order requires ASUS to obtain, within the first one hundred eighty (180) days after service of the order and on a biennial basis thereafter for a period of twenty (20) years, an assessment and report from a qualified, objective, independent third-party professional, certifying, among other things, that: (1) it has in place a security