

Lines 1105-1107 say, "Although electronic return methods currently exist, several security challenges and concerns should be addressed when expanding the use of electronic returns to ensure these methods are secure enough to confidently use to vote."

However, it is a well established scientific consensus that "the Internet (or any network connected to the internet) should not be used for the return of marked ballots. . . . no known technology guarantees the secrecy, security, and verifiability of a marked ballot transmitted over the internet." [National Academies of Science, Engineering, and Medicine, "Securing the Vote: Protecting American Democracy", 2018.] In the three years since that peer-reviewed assessment was published, no technological revolution has changed the fact that "no known technology" can make it safe or secure to return voted ballots electronically. In fact, during that time, one after another after another, deployed e-ballot-return systems have been shown to be insecure---which is not surprising in light of the National Academies' scientific assessment of its infeasibility.

Therefore this statement that "several security challenges and concerns should be address" is completely wishful thinking, it asks for an impossibility (by any known technology). These lines should be revised to say,

"No known technology can assure the secrecy, security, and verifiability of electronic ballot return. Although electronic return methods currently exist, all of them are inherently unsecurable, and they should not be used in public elections."

Andrew W. Appel
Professor of Computer Science
Princeton University