Written Statement of Avi Rubin, Professor of Computer Science, Johns Hopkins University

Before the
U.S. House of Representatives
Committee on House Administration

For a Hearing Concerning
Feasibility of Using Technology to Conduct Remote Voting in the House

July 17, 2020

Good afternoon Chairperson Lofgren, Ranking Member Davis and Members of the Committee. Thank you for inviting me to participate in today's hearing.

My name is Avi Rubin. I am a professor of computer science and technical director of the information security institute at Johns Hopkins University. For about ten years, the primary focus of my academic research was the security of electronic voting. For five years, I was the director of the NSF Accurate Center for Secure Elections, and I have worked in 6 elections in Maryland as an election judge.

While my work has focused on public elections where I strongly oppose Internet voting, the remote voting contemplated by this committee is very different. From a security standpoint, the primary difference is that remote voting for House members does not require a secret ballot. Maintaining voter anonymity is the predominant challenge in public elections. Thus, most of my concerns about remote Internet voting are not relevant.

I imagine some important features of such a system would include:

- Members of Congress can cast votes on bills over the Internet from a computer or a mobile device
- Votes are tabulated, and then displayed on a virtual board, simulating the large board where votes are shown in the House chamber.
- The public can access the virtual board to see how members voted
- The system needs to work in real-time because some votes lead directly to procedures that are immediately enacted

Without the secrecy requirement, I believe that it is possible to design, build and deploy a reasonably safe and secure remote voting capability for House members that meets these requirements, provided that certain procedures are followed.

When considering the security of a system, one of the first steps is to develop a threat model. Once the threats are identified, they can be ranked in order of severity, and the security designers attempt to address them. I see the following as important threats to consider when designing a remote voting system for members of Congress. I consider a powerful adversary such as a nation state with significant resources.

1. An attacker compromises the Member's voting device (computer, phone, tablet) and forges votes from that member
2. An attacker forges communication from a Member without even compromising their devices
3. An attacker compromises the back-end system that receives and tabulates votes and records votes incorrectly
4. An attacker launches a targeted and selective denial of service attack against a Member's network, preventing them from voting on a particular matter

Certainly there are other threats, but these are the top ones that come to mind. I believe that the first three can be addressed with standard security practices, including using encrypted channels such as those used in banking and e-commerce, and two-factor authentication. Other procedures can be developed to audit the system. For example, Members' staffers can register a mobile device with the system and receive a push notification whenever a vote is received from a Member. The staffers can raise an alarm if a vote is cast that does not represent the Members' intention.

The denial of service attack is more challenging. Perhaps backup connectivity, such as using the cellular network on a mobile phone instead of the Internet on a home WiFi network can be utilized.

In conclusion, technology is available today to make it possible for Members to vote on bills remotely over the Internet. However, care must be taken to employ proper procedures and audit to ensure that tampering is not occurring, and backup procedures should be considered in the event that the system is unavailable at a critical time.