WRITTEN TESTIMONY OF DAVID WAGNER, PH.D.
COMPUTER SCIENCE DIVISION
UNIVERSITY OF CALIFORNIA, BERKELEY
BEFORE THE COMMITTEE ON HOUSE ADMINISTRATION
U.S. HOUSE OF REPRESENTATIVES
JULY 15, 2020

Chairperson Lofgren, Ranking Member Davis, committee members, thank you for the opportunity to testify today. My name is David Wagner. I am a professor of computer science at U.C. Berkeley[1]. My area of expertise is in computer security and the security of electronic voting. I have published extensively on both subjects, with over 100 peer-reviewed papers in the scientific literature and two books, and I have worked with election officials at the local, state, and federal level for over 15 years.

My message today is that it is technologically feasible for the House to conduct roll-call votes remotely, if it chooses to do so. This comes with some risk, but I believe the technical risks can be managed. In short, I do not see any technology barrier to voting remotely, though considerable work will need to be done to secure the process. I will describe today some methods that might be useful for managing the risk.

If the House chooses to adopt technology for remote voting, I recommend securing the vote using a combination of people, process, and technology[1]: all votes should be made public immediately, so that Members or their staff can check that their vote was recorded accurately; the House should establish policies that govern the use of remote voting, including how to handle technology failures; and the technology should be selected to support cybersecurity. I outline in my testimony further details in each of these areas. I would particularly like to highlight remote video-based roll-call votes as one option worth considering.

I suggest four principles to protect the integrity of the system against hacking:

- **Make votes public immediately and verify them.** One of the most reliable safeguards against hacking is to ensure that any security breach will be detected and corrected. Votes in the House are a matter of public record. Consequently, I recommend that Members' votes should be made public immediately, and Members or their staff should be trained on how to check the preliminary record of votes to ensure they were recorded accurately and how to report any discrepancy. It would be helpful to check the preliminary record of votes from a separate device from the one used to cast the vote, as a safeguard against compromise of that device. It would be helpful for party whips or others in each party to also verify the preliminary record of votes and contact Members if they suspect a vote might have been misrecorded. Such verification defends against both security risks and against other technology failures.

- **Establish policies and processes that support cybersecurity.** I recommend establishing a process so that, if a Member notices that their vote was not recorded accurately, the Member can contest it and correct the record of their vote. Careful attention will be needed to consider how to correct any discrepancies, how to deal with the potential for false claims that a vote was misrecorded, how to deal with technology issues if a Member is unable to cast their vote, and to establish a time period after which the record of votes is considered final and can no longer be contested[2].

[1] I do not speak for UC Berkeley or any other organization. Affiliations are provided for identification purposes only.

When deploying information technology for the first time, it is often helpful to begin with pilot projects or an initial deployment of limited scope. Accordingly, the House might consider a phased deployment of any remote voting technology, to identify any issues that might arise.

- **Select a technology partner with cybersecurity expertise.** Before adopting technology for remote voting, the House might consider identifying a technology partner with technical expertise in cybersecurity. It would be useful to have technical experts who can assist with an independent security evaluation of technology products and solutions, analyze the security risks of each option, offer advice on how to deploy it securely, and provide a red-team penetration test of the resulting system. There are a number of organizations in the US government with strong technical expertise in cybersecurity who could be considered for partnership, including the National Security Agency, Department of Homeland Security, and National Institute of Standards and Technology.

- **Adopt good cybersecurity practices.** Selection of technology should take cybersecurity into account, and infrastructure to support remote voting will need to be secured. I outline specific technical measures below.

I see several options that could be considered for how technology could be used to support remote voting:

- **Vote via remote videoconferencing.** A promising option for voting securely would be to conduct roll-call votes by a remote video call between the Member and the office of the clerk. This would enable verification of the Member's face and voice. Video verification is not perfect, as real-time video "deepfakes" are possible, but when combined with the opportunity for Members to verify their votes it would mitigate many of the cybersecurity risks associated with remote voting.

  It would be possible to provide additional security if desired through code voting. Each Member could be issued with a one-time-use secret code number for each option (e.g., 672013 for Yes, 019231 for No, and 926885 for Abstain), different for each Member and each vote taken. The Member could then provide the secret code to authorize their vote. The combination of video verification and a secret code provides stronger protection than either alone: the video ensures it is the Member voting, not a member of their staff standing in for them, and the code provides additional protection against deepfakes and outsiders. The primary disadvantage of code voting is the extra logistical burden to distribute and keep track of the secret codes.

  When selecting a videoconferencing product, it would be useful to select one that provides end-to-end encryption and strong authentication (e.g., two-factor authentication using a security token provided to each Member). It would enhance security if Members cast their vote using a secure device that was configured and provided by the government, rather than their own personal devices.

  The primary advantage of this approach is that it could be deployed fairly rapidly, as the House would not need to develop, select, or vet a new product or app. The primary disadvantage of this approach is that it may be slower and more labor-intensive than other options.

- **Commercially available voting products.** Another option would be to procure a system for remote voting from among the options on the market. If this route is taken, it will be important to ensure the House has its own technical experts who can conduct a security evaluation of the options, including a design review and source code analysis, as the quality and security of solutions available on the market varies widely, and many systems have suffered from significant security problems[3]. I recommend looking for a solution that uses good cybersecurity practices, including use of end-to-end encryption, two-factor authentication, and secure software development practices. To authenticate members, each Member could be supplied with a personal security authentication token. There is a thriving commercial market in security tokens, and there are relevant industry standards, including U2F and FIPS-140 certification. Any solution should ensure that votes are made public and can be verified, as highlighted above. I recommend retaining an independent cybersecurity expert to conduct an security evaluation of any product before procuring it.

- **Develop a new system.** Finally, the House could consider developing a new system or app of its own. For instance, one possibility would be to develop a custom app that runs on each Member's government-issued iPhone. The Member could be authenticated using a separate security token before voting on the app, votes could be communicated securely using end-to-end encryption over the Internet, and all votes could be displayed in real time on the app and online so that Members and others can verify their votes were recorded accurately.

  However, I expect that developing and vetting a new solution might be time-intensive and might require considerable technical expertise, so this might not be an attractive solution for dealing with the COVID-19 situation.

These solutions should only be used for public votes in Congress. Internet-based remote voting technology is not secure enough to be used for elections among the general public or whenever a secret ballot is needed[4].

There are other issues that may warrant attention[5]. Voting from the floor provides Members a safe place to vote, where they are free from interference or undue influence; these protections are weakened when voting remotely. Also, there may need to be a fallback process if Members are unable to cast a vote, whether due to technical issues, failures of the network, or a malicious denial-of-service attack aimed at preventing them from voting. One risk of any technology-based solution for remote voting is that technology failures might prevent Members from voting. Similarly, denial-of-service attacks might be able to prevent specific Members from voting. There is no fully effective defense against denial-of-service attacks. The most effective mitigation for both of these risks is to provide a fallback way to cast a vote.

The security of a system is, like a chain, only as strong as its weakest link. Thus, it is important to secure the devices Members use, the communication networks, and the back-end infrastructure that supports voting. Using government-issued and securely-configured devices for voting would help protect against attacks on the Members' devices. The combination of strong two-factor authentication and end-to-end encryption provides effective protection against including man-in-the-middle attacks and digital spoofing. As a general rule of thumb, Internet-based applications can be more secure than the public telephone network, as Internet-based applications can adopt these protections, but telephony cannot. For these reasons, I do not recommend relying on email, fax, or telephone calls for voting in Congress. Securing the infrastructure and software is more challenging and will require special attention from technical experts.

In conclusion, it is my assessment that it is technologically feasible to conduct House votes remotely in a secure way. However, work will be needed to ensure that appropriate safeguards are in place.

Notes

[1] Nicole Goodman, Aleksander Essex, "Online voting entirely possible for MPs during times of crisis", Policy Options, March 25, 2020.

[2] Andrew Appel, "Can Legislatures Safely Vote by Internet?", Freedom to Tinker, April 10, 2020.

[3] Scott Wolchok, Eric Wustrow, Dawn Isabel, and J. Alex Halderman, "Attacking the Washington, D.C. Internet Voting System", Proceedings of the 16th Conference on Financial Cryptography and Data Security, 2012.
Lewis, Sarah Jamie, Olivier Pereira, and Vanessa Teague. Jason Kitcat, Harri Hursti, Margaret MacAlpine, and J. Alex Halderman, "Security Analysis of the Estonian Internet Voting System", Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, 2014.
J. Alex Halderman, Vanessa Teague, "The New South Wales iVote System: Security Failures and Verification Flaws in a Live Online Election", Proceedings of 5th International Conference on E-Voting and Identity (VoteID), 2015.
"How not to prove your election outcome", Proceedings of the 41st IEEE Symposium on Security and Privacy, 2019.
Drew Springall, Travis Finkenauer, Zakir Durumeric, Michael A. Specter, James Koppel, Daniel Weitzner, "The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections", Preprint, 2020.
Michael A. Specter, J. Alex Halderman, "Security Analysis of the Democracy Live Online Voting System", Preprint, June 2020.

[4] "Securing the Vote: Protecting American Democracy", National Academies of Science, Engineering, and Medicine, Academies Press, 2018.
"Risk Management for Electronic Ballot Delivery, Marking, and Return", Election Assistance Commission, National Institute of Standards and Technology, Federal Bureau of Investigation, Cybersecurity and Infrastructure Security Agency, May 2020.

[5] "Majority Staff Report Examining Voting Options During the COVID-19 Pandemic", U.S. House of Representatives Committee on Rules Office of the Majority, March 23, 2020.