Prepared Statement of William P. Crowell
Partner, Alsop Louie Partners

"Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House."
July 17, 2020 – The Committee on House Administration, U.S. House of Representatives

PREPARED STATEMENT OF WILLIAM P. CROWELL, PARTNER, ALSOP LOUIE PARTNERS

INTRODUCTION

Thank you for the opportunity to comment on the Committee's investigation of the "Feasibility and Security of Technology to Conduct Remote Voting in the House." In the wake of the extraordinary pandemic of COVID-19, there is clearly a need to be able to conduct House business in ways that minimize the potential hazard to the members and their staff and families.

As an introduction to my testimony, I would like to briefly share my background to establish my credentials for commenting on the feasibility to safely and securely conduct remote voting. I began my first career at the National Security Agency where I held a number of technical positions including software development on signal processing, astrophysics and geographic information systems, signals collection, signals intelligence analysis and intelligence reporting and cryptography. My management positions included Research and Development of Tactical Systems, Science and Technology of Space and Weapons Systems, the Analysis of Soviet Signals Intelligence, Resources and Planning, Chief of Staff, and Deputy Director for Operations. I concluded my career as the Deputy Director of NSA (1994 through 1997). I also interrupted my NSA career briefly to work in the Aerospace Industry on special designs for satellites.

Upon retiring from NSA, I moved to Silicon Valley and joined a public company, Cylink Corp., that specialized in network security systems including encryption, authentication, and public key cryptography serving the banking, government and enterprise markets. I became CEO of Cylink eight months later and served as CEO for five years until its acquisition by SafeNet Corp. I then served on a number of boards of both public and private companies in both the network and physical security fields. I also served as a Consultant in Information Technology and Security to a number of Technology Companies around the country. In 2012, I became a partner in Alsop Louie Partners, a Venture Capital Firm headquartered in San Francisco that is focused on disruptive technologies including security, artificial intelligence, augmented reality, financial support systems, gaming technology, and space and rocket motors.

THE TECHNICAL, SECURITY AND OPERATIONAL CHALLENGES OF REMOTE VOTING

In analyzing the challenges of creating and operating a trusted system for remote voting, I have chosen to parse the problem into four major areas:

- Video Conferencing Systems – with the available functionality and security to meet the needs of the House of Representatives

- Voting Systems - with the required functionality and security to carry out the legal obligations of the Constitution, Existing Legislative Authorities, House Rules and the needs of the people that you serve
- Technical Issues - including available connectivity, operating capacity, security systems (including end to end encryption and multifactor authentication), and auditing of legally mandated records of proceedings, storage of documents and the ability to support litigation
- Funding – adequate funding authority to acquire, maintain, operate, and certify the system that is deployed

VIDEO CONFERENCING SYSTEMS

A quick search of the Web for video conferencing software turns up more than 70 different systems that are commercially available. They vary widely in features and functions as well as the level of security that they provide. In addition, there are several fully integrated hardware systems that are dedicated video conferencing systems. Only a very few have end to end encryption and none are certified for classified information. Also, very few are able to interoperate with other similar systems, so once chosen you are locked into that particular system and functionality. Among the many different systems there are only about a dozen products that are well known recognized brands, but many of them were either developed outside the United States or have considerable operating and support coming from outside the U.S., which raises extra concerns about their security and reliability. Also, since COVID-19 has significantly increased the use of video conferencing, a number of these systems have been subjected to cyber attacks, underscoring the lack of cyber resilience of this method of staying connected.

Some of the leaders in the video conferencing systems field that are in wide use for virtual meetings and are full featured are: Microsoft Teams, Cisco WebEx, Google Meet, Zoom, Amazon Chime, BlueJeans (by Verizon), Adobe Connect, and GoToMeeting (by LogMeIn). One company, Wickr (https://wickr.com), offers video, audio, document sharing and secure archiving with automated enforcement of data retention policies, all with strong authentication, encryption and audit, but it is not purpose built for legislative processes. (Disclosure: My venture capital firm, Alsop Louie Partners, is an investor in Wickr.)

VOTING SYSTEMS

During this COVID-19 pandemic at least twenty-four State legislative bodies have embraced various approaches to both remote voting and remote hearings. No common approaches or standards have been adopted although there has been wide adoption of a number of video teleconferencing systems as means of conducting remote hearings and the use of video streaming over the Internet to provide for public participation and transparency.

A wide variety of techniques have been used as voting platforms. In some cases, very low-tech means have been used for the voting, such as proxy appointments from a remote member to a member present in the chambers. Email has also been used to record votes, but it is very cumbersome, does not adapt well to the clerk management of the workflow and processes and is largely not a secure means of

recording votes. A few states have tried to use the Chat function of Video Conferencing Systems, but those have largely failed.

The most attractive technical solution for remote voting is a purpose-built software package that incorporates all of the attributes associated with the Congressional process including Committee Management, Remote Hearings, Document/Bill markup and archiving, public access to proceedings and recorded votes, and, of course, Remote Voting. Because of the sensitivity of some of the Congressional processes, such a system should also incorporate a number of security features as well to include two factor authentication, end to end strong and certified encryption and immutable logs of all votes, documents and actions. The system should be integrated with many of the video teleconferencing systems that are already in wide use by members and as much as possible mimic the existing processes associated with in person Congressional voting processes.

There are a large number of software applications that provide remote/online voting for organizations, but very few of them are designed around legislative processes. They are primarily aimed at nonprofits, companies, unions, churches and many other organizations that have voting processes in place to conduct their business. Some are also used for online surveys and internal communications with employees. Two companies appear to have launched "purpose built" systems for use by legislative bodies and that incorporate end to end encryption, authentication and verification of the votes: Markup (https://markup.law/) and Tallan (https://tallan.com). Both can be integrated with the leading video conferencing systems. Other companies have solutions that can be used for remote voting but lack some of the security and process features in their present form.

TECHNICAL ISSUES

As with many software applications in the market, there can be technical issues that limit or interfere with their successful use. First on that list is the fact that members and staff do not all use the same device(s) either in their Districts or on the road. Accommodating all of the available devices can be technically challenging, particularly for a small population of users. In addition, the internet service providers (ISP's) in their Districts provide differing levels of performance. Wi-Fi and Ethernet connections can be problematic in some regions of the country and disruption of services are not uncommon.

Security issues are one of the most pervasive technical issues in the digital age. Specifically, multifactor authentication, end to end encryption, and verification or audit of all of the votes, documents, and proceedings must not only be present in the solution, but be accredited or certified to work as specified. Today, cyber attacks are an hourly and daily fact and many of them are successful against well designed, but flawed product implementation or use. These attacks have become commonplace and carried out by nation states, criminal, hacktivists, as well as hackers just seeking the thrill of successful attacks. A remote voting system must be resilient against all of these bad actors, particularly nation states seeking to disrupt our democratic processes. This presents a real need for initial certification in an area where there are few standards and continued testing throughout the useful life of the system.

FINANCIAL ISSUES

There are two fundamental financial challenges to implementing remote voting. The first is that although the current pandemic has heightened the need for remote operations of legislatures everywhere and therefore has created a larger market for software to achieve this end, it is still not a very large market and it will be a market with a lot of different functional and operational requirements. This fact will limit the profitability of such software and complicate the financing by developers of in-depth testing and certification. It may be necessary to create a funding stream to cover these expenses in order to assure that products meet the rigorous standards outlined in the Technical Issues portion of this statement.

The second financial issue is the availability of appropriated funds for FY2021. If the Congress does not pass an Appropriation Bill for Legislative Operations, a Continuing Resolution will limit the availability of funding to cover the expenses of conducting a proof of concept, testing and deployment of a remote voting solution, possibly until after the next Congress is convened.

CONCLUSION

Clearly, there are many factors that have to be evaluated to successfully deploy an emergency remote voting solution in the House. I hope that my parsing of the problem is useful to the deliberations of the Committee on House Administration on how to frame the House Rules and Regulations governing certification of the methods to be used in accomplishing this goal.