

EXPLORING THE FEASIBILITY AND SECURITY OF
TECHNOLOGY TO CONDUCT REMOTE VOTING
IN THE HOUSE

HEARING
BEFORE THE
COMMITTEE ON HOUSE
ADMINISTRATION
HOUSE OF REPRESENTATIVES
ONE HUNDRED SIXTEENTH CONGRESS
SECOND SESSION

JULY 17, 2020

Printed for the use of the Committee on House Administration



Available on the Internet:
<http://www.govinfo.gov/committee/house-administration>

U.S. GOVERNMENT PUBLISHING OFFICE

41-953

WASHINGTON : 2020

COMMITTEE ON HOUSE ADMINISTRATION

ZOE LOFGREN, California, *Chairperson*

JAMIE RASKIN, Maryland

SUSAN A. DAVIS, California

G. K. BUTTERFIELD, North Carolina

MARCIA L. FUDGE, Ohio

PETE AGUILAR, California

RODNEY DAVIS, Illinois,

Ranking Member

MARK WALKER, North Carolina

BARRY LOUDERMILK, Georgia

CONTENTS

JULY 17, 2020

	Page
Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House	1
OPENING STATEMENTS	
Chairperson Zoe Lofgren	1
Prepared statement of Chairperson Lofgren	10
Hon. Rodney Davis, Ranking Member	14
Prepared statement of Ranking Member Davis	17
WITNESSES	
Hon. Cheryl L. Johnson, Clerk of the U.S. House of Representatives	22
Prepared statement of Hon. Johnson	24
Newt Gingrich, Former Member and Speaker of the House, U.S. House of Representatives	27
Prepared statement of Mr. Gingrich	29
William Crowell, Partner, Alsop Louie Partners	33
Prepared statement of Mr. Crowell	35
Jon Green, Vice President and Chief Security Technologist, Aruba Networks ..	39
Prepared statement of Mr. Green	41
Dr. Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology	45
Prepared statement of Dr. Rivest	47
Dr. Aviel Rubin, Professor and Technical Director, Information Security Institute, Johns Hopkins University	50
Prepared statement of Dr. Rubin	52
Dr. David Wagner, Professor of Computer Science, University of California, Berkeley	54
Prepared statement of Dr. Wagner	56
QUESTIONS FOR THE RECORD	
Hon. Cheryl L. Johnson, Clerk of the U.S. House of Representatives, answers to submitted questions	75
Jon Green, Vice President and Chief Security Technologist, Aruba Networks, answers to submitted questions	79
Dr. Ronald L. Rivest, Institute Professor, Massachusetts Institute of Technology, answers to submitted questions	82
Dr. Aviel Rubin, Professor and Technical Director, Information Security Institute, Johns Hopkins University, answers to submitted questions	84
Dr. David Wagner, Professor of Computer Science, University of California, Berkeley, answers to submitted questions ¹	86
SUBMISSIONS FOR THE RECORD	
Electronic Vote Recorder, Patent No. 90,646, Thomas A. Edison	4
Letter, Daniel Schuman, Policy Director, Demand Progress and Zach Graves, Head of Policy, Lincoln Network	87

¹Dr. Wagner did not answer submitted questions for the record by the time of printing.

EXPLORING THE FEASIBILITY AND SECURITY OF TECHNOLOGY TO CONDUCT REMOTE VOTING IN THE HOUSE

FRIDAY, JULY 17, 2020

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOUSE ADMINISTRATION,
Washington, DC.

The Committee met, pursuant to call, at 1:03 p.m., via Webex, Hon. Zoe Lofgren Chairperson of the Committee presiding.

Present: Representatives Lofgren, Raskin, Davis of California, Butterfield, Fudge, Aguilar, Davis of Illinois, Walker, and Loudermilk.

Staff Present: Jamie Fleet, Staff Director; Khalil Abboud, Deputy Staff Director; Dan Taylor, General Counsel; Brandon Jacobs, Legislative Clerk; Matthew Schlesinger, Oversight Counsel; Peter Whippy, Communications Director; David Tucker, Senior Counsel & Parliamentarian; Jen Daulby, Minority Staff Director; Tim Monahan, Minority Deputy Staff Director; and Cole Felder, Minority General Counsel.

The CHAIRPERSON. The Committee on House Administration will come to order, and I have a gavel.

I would now like to call the roll so that we will know that we have a quorum present. First, I am here.

I will ask, Mr. Davis, are you present?

Mr. Davis, I see you. Say "here."

Mr. DAVIS of Illinois. Yes, I am present. I had to get to unmute.

The CHAIRPERSON. Okay. Mr. Raskin.

[No response.]

The CHAIRPERSON. He is not present.

Mr. Walker of North Carolina?

[No response.]

The CHAIRPERSON. Not present.

Mrs. Davis of California.

Mrs. DAVIS of California. Present.

The CHAIRPERSON. Mr. Loudermilk of Georgia.

Mr. LOUDERMILK. Present.

The CHAIRPERSON. Mr. Butterfield of North Carolina.

Mr. BUTTERFIELD. Present.

The CHAIRPERSON. Ms. Fudge of Ohio.

Ms. FUDGE. Present.

The CHAIRPERSON. Mr. Aguilar of California.

Mr. AGUILAR. Present.

The CHAIRPERSON. So a quorum being present, I would like to thank the Members of the Committee and our witnesses——

Mr. DAVIS of Illinois. Madam Chair.

The CHAIRPERSON. Yes.

Mr. DAVIS of Illinois. Just a quick point of order. I do know Mark Walker is on. So, for the initial period of attendance, he is here. He is having difficulty with the video. So I think the team is working on the video for him.

The CHAIRPERSON. Very good. We will note that for the record.

Mr. DAVIS of Illinois. Thank you.

The CHAIRPERSON. We are holding this hearing in compliance with the regulations for remote committee proceedings pursuant to House Resolution 965. Section 5 of House Resolution 965 requires this Committee to “study the feasibility of using technology to conduct remote voting in the House,” and “to provide certification to the House upon a determination that such operable and secure technology exists to commit remote voting in the House.”

Today’s hearing will explore the technological and security issues surrounding remote voting and will inform our study of these issues.

As we begin, I want to remind all our members and participants of a few things that will help us navigate this platform. We are holding this hearing in compliance with the regulations for remote committee proceedings pursuant to the resolution. However, the fundamental nature of the hearing and our rules are unchanged.

Generally, the Committee will keep microphones muted to limit background noise. When we meet in person, in our Committee room, members need to unmute themselves when seeking recognition or when recognized for their five minutes. Witnesses will also need to unmute themselves when recognized for their five minutes or when answering a question.

Members and witnesses, please keep your cameras on at all times. If you need to step away for a moment during the proceedings, please leave your cameras on and do not leave the meeting within the Webex platform.

And at this time, I ask unanimous consent that all members have five legislative days to revise and extend their remarks and that any written statements be made part of the record.

And, hearing no objection, that is so ordered.

This is our first virtual full Committee hearing, and it is fitting that I am joining you from Silicon Valley. In recent months, the House has made important use of new technology, including virtual hearings, to continue operations during the COVID pandemic. These advances are particularly noteworthy because, as an institution, the House has not always been quick to adopt technology to its legislative procedures.

A young inventor once observed that what he called “the enormous waste of time in Congress,” spent taking roll call votes. So that 21-year-old invented an electronic system that would permit instantly and accurately recording Members’ votes “thus avoiding loss of valuable time consumed in counting and registering the votes and names,” and saving time for more important, substantive legislative business.

But when he presented his idea to Congress, he was told it would impair the ability of the minority to influence legislation. So that Electrographic Vote Recorder and Register described in the first of more than 1,000 patents that Thomas Edison was issued was essentially ignored by Congress.

I would ask unanimous consent to enter Mr. Edison's patent No. 9646 into the record.

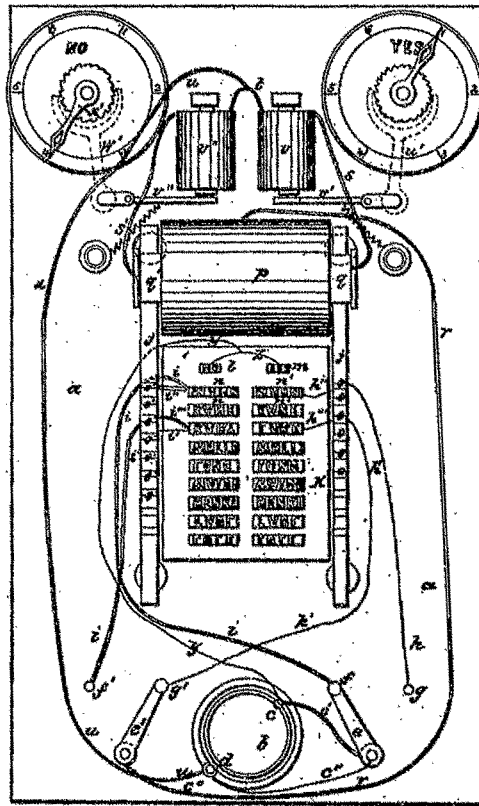
And, without objection, so ordered.

[The information follows:]

T. A. EDISON.
Electric Vote-Recorder:

No. 90,646,

Patented June 1, 1869.



Witnesses.
Charles D. May
Edw. M. Roberts

Inventor.
Thomas A. Edison.

UNITED STATES PATENT OFFICE.

THOMAS A. EDISON, OF BOSTON, MASSACHUSETTS, ASSIGNOR TO HIMSELF
AND DEWITT C. ROBERTS, OF SAME PLACE.

IMPROVEMENT IN ELECTROGRAPHIC VOTE-RECORDER.

Specification forming part of Letters Patent No. 90,646, dated June 1, 1889.

To all whom it may concern:

Be it known that I, THOMAS A. EDISON, of Boston, in the county of Suffolk and State of Massachusetts, have invented a new and useful apparatus named "Electrographic Vote Recorder and Register," of which the following is a full, clear, and exact description, reference being had to the accompanying drawing, which represents a plan view of the apparatus, and to the letters of reference thereon.

The object of my invention is to produce an apparatus which records and registers in an instant, and with great accuracy, the votes of legislative bodies, thus avoiding loss of valuable time consumed in counting and registering the votes and names, as done in the usual manner; and my invention consists in applying an electrographic apparatus in such a manner that each member, by moving a switch to either of two points, representing an affirmative and opposing vote, has his name imprinted, by means of electricity, under the desired head, on a previously-prepared paper, and at the same time the number of votes is indicated on a dial-plate by the operation.

Referring to the drawings, in the central portion of the plate *a a* is secured a block, *k*, upon which are set, in metallic types, two columns of names, *n n'*, the one being headed by the word "no," the other by "yes," each column containing the name of every voter, and the like names standing opposite each other, as Mann under head "no" opposite to Mann under head "yes," &c. The types are separated by intervening spaces.

Along two sides of the block *k*, and parallel with the two columns *n n'*, are two rails, *j j'*, composed of any good insulating material, as hard rubber.

Opposite the intervening spaces between two names the upper faces of the rails *j j'* are intersected by metallic strips *o o o' o' o'*.

On the rails *j j'* are mounted two rollers, *q q'*, insulated from one another, and insulated from and surrounded by the cylinder *p*, in such a manner that the rollers *q q'* project beyond said cylinder *p* and rest immediately upon the rails. These rollers are metallic, and the larger one, *p*, is of such a size as to come in contact with a chemically-prepared paper placed

upon the types, and is, furthermore, in communication with battery *b* by means of conducting-wire *r r*, or in any other suitable manner.

The rollers *q q'* communicate with the two magnets *v v'* by the wires *s s'*, and through them operate the armatures *v' v'''*, the escape-ments *w w'* and the pointers *x x'*, which latter show the numbers of votes on the dial-plates marked with as many figures as there are voters.

The battery *b*, with the two poles *c* and *d*, is connected with and operates the apparatus in the following manner: The pole *c* is in constant communication with the metallic types *l m*, representing, respectively, "no" and "yes," by means of the conducting-wires *y y'*; but the pole *c* is connected by the wires *e e' e''*, with as many switches *s s'* as there are voters.

From the points *f f' g g'* the conducting-wires *i i' h h'* pass to the metallic strips *o o o' o'*, and from thence to the nearest metallic type, or they may pass first to the types and then branch back to the respective strips, as seen in the column to the left.

From the pole *d* of battery *b* communication is established with the cylinder *p* by the wire *r r*, and from the same pole by the wire *u u'* to the two magnets, where the aforesaid conducting-wires *s s'* lead to the two insulated rollers *q q'*.

The apparatus is placed before the recording clerk's desk, and a paper, which is previously chemically prepared for printing by electricity by saturating it in any known solution for that purpose, is placed upon the types, and covering the two columns and their heading.

Every voter is also provided with a switch, *e*, and moves the same *ad libitum*, as the occasion may require, on the point *f* or *g*. Thus an electric current is established between the pole *c* of the battery, the switch *e e'*, and the types *l m*, and the clerk then rolls the rollers *q q'* with cylinder *p* on the paper upon the types. As soon as the cylinder *p* comes on the type of the headings the circuit becomes completed through the paper, (as the wires *y y'* connect the pole *c* with the types, and the wire *r* the pole *d* with the cylinder *p*), and de-

composes the chemicals, thereby discoloring the paper in contact with the types, and thus produces the printing.

When the cylinder *p* comes over the two names—Mann, Mann—the current from pole *c* through switch *e* and wire *t* to the types bearing the name on the left becomes completed through the paper, with cylinder *p*, wire *r*, and pole *d*, and, discoloring the paper, produces the name Mann on the paper; but there is no connection of the other name Mann to the right with the switch and pole *c*; consequently no decomposition takes place, and no name shown.

The roller *p* passing on and leaving the types the circuit becomes broken; but as soon as the rollers *q q'* come in contact with the metallic strips *o o'* the circuit from pole *c* through the switch *e*, wire *t*, strip *o'*, and through roller *q'*, magnet *v''*, wire *t* and *u* to pole *d*, becomes closed, the armature *v'''* attracted the escapement *w'*, and with it the pointer *x'* moved forward, and here one negative vote recorded, &c.

Thus, it will be seen, the names of all the voters are printed on their respective heads, and also the whole number of votes counted in an instant, or as long as it will require time to roll the cylinder *p* over the types containing

the list of all the names in metallic types, with more dispatch and accuracy than it can possibly be done in any other way.

Having thus fully described my invention, what I claim as new, and desire to secure by Letters Patent, is—

1. The combination of a switch or switches *e e'*, types and cylinder *p*, with an electric battery, connected and operating substantially as and for the purpose set forth.

2. The combination of switch *e*, strips *o o'*, types, and the separated and insulated rollers *q q'*, magnets *v v''*, armature, escapement, pointer, and dial-plate, with the battery *b*, connected and operated substantially as and for the purpose above described.

3. The combination of switch, types, cylinder *p*, rollers *q q'*, strips *o o'*, and insulators *j j'*, magnets *v v''*, armature, &c., constructed in the manner and for the purpose above specified.

In testimony whereof I have signed my name to this specification in the presence of two subscribing witnesses.

THOMAS A. EDISON.

Witnesses:

CARROLL D. WRIGHT,
M. S. G. WILDE.

The CHAIRPERSON. It would take another 20 years for anyone to introduce the first bill to permit a form of electronic voting. By the time the House took its first electronic vote in 1973, more than a century had passed since Edison first suggested the idea. It also took more than 40 years from the time Members of the House first appeared on live television to the time when cameras were allowed to broadcast live proceedings on the House floor.

It is not unusual for any institution steeped in history and precedent to resist change. That was the case for the House when it came to advances like electronic voting and televising our proceedings, both of which we take for granted today.

But we can't afford that attitude today in the face of the COVID crisis. That is why the House recently passed a resolution to ensure that we can continue to govern during the coronavirus pandemic. The resolution authorized new ways to conduct our legislative business.

For example, the House authorized remote committee proceedings like this one. The House also authorized remote directed proxy voting on the floor. And the House directed further study of a third possible tool: remote voting. That review is the purpose of today's hearing.

In some respects, these are new tools for governing, but they are within our authority to implement, and they are not intended to replace our regular order. To the contrary, they represent prudent and responsible steps to ensure that the House can continue to lead during this crisis. As the resolution makes clear, they are intended to be used only during extraordinary circumstances. There can be no doubt that these are extraordinary times.

Our Nation and the world continue to grapple with the devastating spread of a historic pandemic, and the spread of the disease in the United States is worsening. Today, more than 3.5 million Americans have been confirmed to have COVID. That is a greater number than the population of 21 individual States.

More Americans have died in the last few months from COVID than were killed in all military conflicts U.S. has fought since World War II combined. Plus, because of the continuing problems with access to testing, we don't know for sure how many Americans have actually contracted the virus, but the experts believe the actual figure could be as high as 20 million.

We are still learning about how highly contagious this deadly virus is and how it is spread, what steps can be taken to mitigate its further spread. New reports have suggested that the immunity gained by those who recover from COVID could be short lived.

As bad as things already are, cases are continuing to rise in more than 40 States. This week, the Director of the Centers for Disease Control and Prevention, Dr. Redfield, said he believes that "The fall and winter of 2020 and 2021 are going to be probably one of the most difficult times that we have experienced in American public health."

This crisis demands legislative action and oversight and the continued work of the Congress, and it also means that we have a responsibility to the institution and the American people to explore additional ways to be able to continue work in the face of the pandemic.

Consider the alternative: In a number of States outbreaks among State legislators have impacted the ability to conduct State business. In Mississippi this week, more than 40 legislators and staff, including at least 30 members, have tested positive for the disease. The Speaker of the House and the Lieutenant Governor, who presides over the Senate, are both positive. That has left the State government in limbo with significant pending business unfinished. In several other States, tragically, legislators have died.

Here in Congress, nearly 60 Members have publicly disclosed that they tested positive, self-quarantined, or had otherwise come in contact with someone who was positive. At one point at the same time, at least 22 Members of the House had either tested positive, were presumed positive, or were in self-quarantine because of someone who they had been exposed to who was positive.

That is in addition to the scores of other institutional leg branch staff who contracted COVID, including personnel from the Capitol Police, the Architect of the Capitol, the GPO, and others.

I am mindful that many people are putting themselves at risk by working on the front lines every day, from doctors and nurses, to police officers, firefighters, and paramedics, to transit workers and truck drivers, among others.

As the daughter of a truck driver and a school cafeteria cook, I deeply appreciate everything people in many critical lines of work are doing to support their communities and the country, even at risk to their own health. However, we in Congress have an option that most of these vital frontline workers do not have: we can do our work remotely in a safe, secure, online format.

We have already taken a number of significant steps to do that. In just two months, the House has held 29 votes, which included remote directed proxy votes. These votes have produced legislation signed into law by the President. House committees have held more than 86 committee hearings and markups.

These events have included more than 185 hours of testimony, questions, statements, and debate. Of those committee events, 78 were hearings, and of those hearings, 49 were fully remote, 29 were hybrid, during which some Members were in Washington while others participated remotely.

More than 226 individuals have provided testimony as witnesses in remote or hybrid hearings. In addition, in April, the Speaker directed the creation of an all-electronic—hopper to permit the virtual submission of all floor documents, including bills, resolutions, cosponsors, and extension of remarks, via a dedicated and secure email system. Since the policy took effect, 1,307 measures have been filed electronically while just 51 were filed using the old process.

And in my capacity as chairperson of the Joint Committee on Printing, I directed the GPO to accept for publication in the *Congressional Record* extensions of remarks submitted with the Member's electronic signature. Under this new, more convenient system, Members have filed 897 extensions of remarks by email.

All of these are remarkable changes in the history of the institution. We have acted swiftly to use technology because when we maximize our remote work, we minimize needless exposure of everyone who works on Capitol Hill, and that includes the Capitol

Police, the cleaning staff, other institutional staff, the press, legislative staff, and Members.

Virtual and hybrid committee events have been, by and large, very successful. Although there have been some relatively small number of technical issues, in considering these, it is important to keep in mind that expanding use of virtual or remote congressional activity where appropriate ensures that we can continue to act in a manner that is safe for the legislative branch workforce while also preserving precious testing equipment and supplies for front-line workers who don't have jobs that can be performed remotely.

The highest levels of all three branches of our Federal Government have recognized the need to adapt our work in the 21st century and that we can do so in a safe, secure, and transparent way.

In addition to the changes we have made in the House, the Senate has held numerous virtual hearings. The Supreme Court, which long resisted modest attempts to increase transparency and public access to its proceedings, has heard oral arguments by conference call.

These important cases involve critical congressional oversight prerogatives, and for its part, the executive branch has recognized the legitimacy of these proceedings by participating in virtual or remote proceedings, both Chambers of Congress, and the Supreme Court.

Now, as I mentioned, I represent Silicon Valley, which has become synonymous around the world for technology and the spirit of innovation. We in Congress must adopt the entrepreneurial spirit and openness to new technology that made my community a global leader and apply it to the procedural and logistical challenges we face in our legislative operations, as well as to strategy to respond to and overcome the coronavirus.

Remote voting could be another powerful tool to permit the House to continue its work. The Committee on Rules has already had significant discussions about the constitutional basis and foundation for using technology to bolster legislative operations during the pandemic. So that is not the focus of this Committee hearing today.

Our purpose is to assess the specific issue of the feasibility of using technology to conduct remote voting in the House.

With that in mind, I look forward to hearing from our esteemed panel of witnesses.

I would now like to recognize our Ranking Member, Rodney Davis, for his opening statement.

[The statement of the Chairperson follows:]

ZOE LOFGREN, CALIFORNIA
CHAIRPERSON

JAMIE RASKIN, MARYLAND
VICE CHAIRPERSON

SUSAN DAVIS, CALIFORNIA
G.K. BUTTERFIELD, NORTH CAROLINA
MARCIA FUDGE, OHIO
PETE AGUILAR, CALIFORNIA

JAMIE FLEET, STAFF DIRECTOR

Congress of the United States

House of Representatives
COMMITTEE ON HOUSE ADMINISTRATION
1309 Longworth House Office Building
Washington, D.C. 20515-6157
(202) 225-2061
<https://cha.house.gov>

RODNEY DAVIS, ILLINOIS
RANKING MINORITY MEMBER

MARK WALKER, NORTH CAROLINA
BARRY LOUDERMILK, GEORGIA

ONE HUNDRED SIXTEENTH CONGRESS

JEN DAULBY, MINORITY STAFF DIRECTOR

Chairperson Zoe Lofgren Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House July 17, 2020 Opening Statement

As this is our first virtual full Committee hearing, it is fitting that I am joining you from Silicon Valley. In recent months, the House has made important use of new technology – including virtual hearings – to continue operations during the COVID pandemic. These advances are particularly noteworthy because, as an institution, the House has not always been quick to adopt technology to its legislative procedures.

A young inventor once observed what he called, quote, “the enormous waste of time in Congress,” unquote, spent taking roll call votes. So, the 21-year-old invented an electronic system that would permit instantly and accurately recording Members’ votes, “thus avoiding loss of valuable time consumed in counting and registering the votes and names,” and saving time for more substantive legislative business. But when he presented his idea to Congress, he was told it would impair the ability of the minority to influence legislation.

So, the “Electrographic Vote Recorder and Register” – described in the first of the more than 1,000 patents that Thomas Edison was issued – was essentially ignored by Congress. I’d ask unanimous consent to enter Mr. Edison’s patent, number 9646, into the record, and without objection that is ordered. It would take another 20 years for anyone to introduce the first bill to permit a form of electronic voting. By the time the House took its first electronic vote in 1973, more than a century had passed since Edison first suggested the idea.

It also took more than 40 years from the time Members of the House first appeared on live television to the time that cameras were allowed to broadcast live proceedings on the House floor.

It is not unusual for any institution steeped in history and precedent to resist technological change. That was the case for the House when it came to advances like electronic voting and televising our proceedings – both of which we take for granted today. But we can’t afford that attitude today in the face of the COVID crisis.

That's why the House recently passed a resolution to ensure that we can continue to govern during the coronavirus pandemic. House Resolution 965 authorized new ways to conduct our legislative business. For example, the House authorized remote committee proceedings – like this one. The House also authorized remote directed proxy voting on the floor. And the House directed further study of a third possible tool – remote voting. That review is the purpose of today's hearing.

In some respects, these are new tools for governing – but they are within our authority to implement and they are not intended to replace our regular order. To the contrary, they represent prudent and responsible steps to ensure that the House can continue to lead during this crisis, and as the resolution makes clear, they are intended to be used only during extraordinary circumstances.

There can be no doubt that these are extraordinary times. Our nation – and the world – continue to grapple with the devastating spread of a historic pandemic. And the spread of the disease in the U.S. is worsening.

Today, more than 3.5 million Americans have been confirmed to have COVID. That's a greater number than the population of 21 individual states. More Americans have died in the last few months from COVID than were killed in all military conflicts the U.S. has fought in since World War II, combined. Plus, because of continuing problems with access to testing, we don't know for sure how many Americans have actually contracted the virus – but experts believe the actual figure could be as high as 20 million.

We are still learning about how highly contagious this deadly virus is, how it's spread and what steps can be taken to mitigate its further spread. New reports have suggested that the immunity gained by those who recover from COVID may be short-lived.

As bad as things are already, cases are continuing to rise in more than 40 states. This week, the Director of the Centers for Disease Control and Prevention, Dr. Redfield, said that he believes “the fall and winter of 2020 and 2021 are going to be probably one of the most difficult times that we have experienced in American public health.”

This crisis demands legislative action and oversight and the continued work of the Congress. And it also means that we have a responsibility to the institution and the American people to explore additional ways to be able to continue that work in the face of the pandemic.

Consider the alternative. In a number of states, outbreaks among state legislators have impacted the ability to conduct state business. In Mississippi this week, more than 40 legislators and staff – including at least 30 members – are positive for the disease. The Speaker of the House and the Lieutenant Governor, who presides over the Senate, are both positive. That has left the state government

in limbo, with significant pending business unfinished. In several other states, tragically, legislators have died.

Here in Congress, nearly 60 Members have publicly disclosed that they tested positive, self-quarantined, or had otherwise come in contact with someone else who was positive. At one point, at least 22 Members of the House had either tested positive, were presumed positive, or were in self-quarantine because they were exposed to someone who was positive.

That's in addition to scores of other institutional legislative branch staff who have contracted COVID – including personnel from the Capitol Police, Architect of the Capitol, the GPO, and others.

I am mindful that many people are putting themselves at risk by working on the frontlines every day: from doctors and nurses, to police officers, firefighters, and paramedics, to transit workers and truck drivers, among others. As the daughter of a truck driver and a school cafeteria cook, I deeply appreciate everything people in many critical lines of work are doing to support their communities and the country, even at risk to their own health.

However, we in Congress have an option that most of these vital frontline workers do not have: we can do our work remotely in a safe, secure, online format. We have already taken a number of significant steps to do that. In just two months:

- The House has held 29 votes which included remote directed proxy votes. Those votes have produced legislation signed into law by the President.
- House committees held more than 86 committee hearings and markups. These events have included more than 185 hours of testimony, questions, statements, and debate.
- Of those committee events, 78 were hearings. And of those hearings, 49 were fully remote, while 29 were hybrid hearings, during which some Members were present in Washington, while others participated remotely.
- More than 226 individuals have provided testimony in remote or hybrid hearings.

In addition, in April, the Speaker directed the creation of an all-electronic hopper to permit the virtual submission of all Floor documents – including bills, resolutions, co-sponsors and extensions of remarks – via a dedicated and secure email system. Since the policy took effect, 1,307 measures have been filed electronically, while just 51 were filed using the old process.

And in my capacity as Chairperson of the Joint Committee on Printing, I directed the GPO to accept for publication in the Congressional Record extensions of remarks submitted with a Member's electronic signature. Under this new, more convenient system Members have filed 897 extensions of remarks by email.

All of these are remarkable changes in the history of the institution. We have acted swiftly to use technology because when we maximize our remote work, we minimize needless exposure of everyone who works on Capitol Hill. And that includes Capitol Police, the cleaning staff, other institutional staff, the press, legislative staff, and Members.

Virtual and hybrid committee events have been, by and large, very successful. Although there have been some relatively small number of technical issues, in considering these, it is important to keep in mind that expanding use of virtual or remote congressional activity, where appropriate, ensures that we can continue to act in a manner that is safe for the legislative branch workforce, while also reserving precious testing equipment and supplies for frontline workers who don't have jobs that can be performed remotely.

The highest levels of all three branches of our federal government have recognized the need to adapt our work to the 21st century – and that we can do so in a safe, secure, and transparent way. In addition to the changes we have made in the House, the Senate has held numerous virtual hearings. The Supreme Court – which has long resisted modest attempts to increase transparency and public access to its proceedings – has heard oral arguments by conference call. These important cases involve critical congressional oversight prerogatives. The executive branch has recognized the legitimacy of these proceedings by participating in virtual or remote proceedings of both chambers of Congress and the Supreme Court.

As I mentioned, I represent Silicon Valley, which has become synonymous around the world for technology and the spirit of innovation. We in Congress must adopt the entrepreneurial spirit and openness to new technology that made my community a global leader and apply it to the procedural and logistical challenges we face in our legislative operations – as well as to a strategy to respond to and overcome the coronavirus.

Remote voting could be another powerful tool to permit the House to continue its work. The Committee on Rules has already had significant discussions about the constitutional basis and foundation for using technology to bolster legislative operations during the pandemic. So that's not the focus of this meeting today, our purpose here today is to assess the specific issue of the feasibility of using technology to conduct re-mote voting in the House. With that in mind, I look forward to hearing from our esteemed panel of witnesses.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson.

This is a great opportunity for us to—let me get my audio stuff taken care of here. I apologize.

Chairperson, thank you for holding today's hearing. I appreciate hearing from the Majority about the different provisions that the House has passed already to deal with the coronavirus. We came together for four very important bills that dealt with saving our economy, making sure that we allowed small businesses to survive and sustain themselves during this pandemic.

But the provisions that were put in place, as was mentioned by the Chairperson, were not done by the House as a whole; they were done by the Majority. Remote voting is being discussed because it is a provision that was recommended by the Majority in the House only. There are many of us who have concerns with the provisions that are in place for proxy voting and for remote and hybrid hearings.

And I appreciate, though, today that we are going to discuss the feasibility of remote voting because, regardless of our concerns, we have to make sure that we debate the merits of any provisions, even if they are pushed through by only the Majority. I think this is an important conversation. I hope the transparent process continues before the Majority decides to move forward with implementation.

I would like to welcome all of our witnesses, especially former Speaker Gingrich. I believe the Speaker offers a unique perspective, and I do appreciate his willingness to participate. I hope with the long opening statements, Mr. Speaker, that this is not a delay game since you are across the Atlantic Ocean and on a different time schedule, but stick with us. I think America needs to hear what you are going to say on this issue.

But before we discuss the possibility of remote voting, I think it is important to lay out where we are now, how we got to this point, and the process that has driven the operational decision making of this institution during the COVID-19 pandemic.

When this coronavirus began spreading across our country and the rest of the world, we knew it was only a matter of time until we would be impacted in the people's House. In March, there was a bipartisan effort to quickly transition thousands of staff to telework. That was an enormous lift and only made possible through the tireless work of the Chief Administrative Officer, which I must add, didn't exist until Speaker Gingrich was Speaker of the House, and then also the Sergeant at Arms offices.

And I would like to thank Chairperson Lofgren for working in a very bipartisan way to make that happen. Then the conversation turned to additional procedural changes that would be required for the House to continue to operate. These efforts did not incorporate bipartisan input.

On March 23rd, Democrats released a report concluding remote voting in any form would almost certainly cause unintended consequences if not done with adequate forethought and discussion, and change cannot be implemented overnight and likely cannot be accomplished in time to address the current crisis.

Well, despite this and without any public hearings or bipartisan support, the majority passed H. Res. 965 on May 15th, which au-

thorized proxy voting, remote committee proceedings, and authorized remote voting pending a certification from Chairperson Lofgren.

Since the implementation of H. Res. 965, 572 proxy votes have been cast on the House floor, dozens of virtual hearings and markups, and a lawsuit filed in Federal court on the grounds that proxy voting is unconstitutional.

During today's hearing, we will hear lots of discussion on IT capabilities that can support remote voting, the types of requirements that a system should have to safeguard against threats, and examples of entities already using remote voting.

Four months before this hearing, when it became apparent the direction of the Democratic majority and where they were heading, I directed my team to formally engage with the GAO to better understand remote voting technologies. This engagement has been productive, and I am confident that there is a technology that exists to support remote voting.

I also have confidence in the Clerk and her staff's ability to execute if directed.

What I am concerned about is that the House seems to be in a very reactionary posture with sweeping changes being made with little consideration around longer-term impacts.

We have already seen numerous hearings and markups disrupted by technical difficulties, resulting in the nature of those proceedings changing; fewer standalone amendments being made in order for floor consideration; increased usage of en bloc amendment packages at committee hearings and on the floor; and dozens of examples of Members from both parties not following the prescribed regulations with no consequences. No one can say with a straight face that these trends are a good thing or that the quality of the deliberative process that is the hallmark of the House hasn't been sacrificed.

Over the last six months, we have seen essential workers across our Nation step up, make sacrifices, and take on risk, all in the name of our collective well-being. I know the grocery store clerks, the truck drivers, farmers, healthcare workers, like my wife, and first responders in my district expect their elected leaders to have the same willingness and patriotic duty to make sacrifices just as they do every shift.

Americans look to their elected leaders to set an example, and they don't appreciate Congress skipping out on their duties to attend events across their States that seem more desirable than the difficult task of governing during a pandemic.

As our country continues to be impacted by the coronavirus, the example I want to set is that we stand side by side with the essential workers of this country, and I don't believe that can be done solely behind a computer screen and over emails.

We have debated scenarios like this before, and Members who are unable to travel can submit statements to the *Congressional Record*. And we have a rule that this Majority adopted at the beginning of this Congress that allows for a quorum to be adjusted in an emergency.

I will end with a quote from the U.K.'s House of Commons leader, Jacob Rees-Mogg, who recently announced they will be scaling

back their virtual Parliament. He said: Rather than suffering the depredations of the muted, hybrid Parliament, we are once again talking to each other in ways impossible when we were scattered to the four winds. Rather than wading through the treacle of the hybrid proceedings, we are once again fleet afoot and dancing a legislative quickstep.

And, Madam Chair, I am glad you didn't ask me to dance here, but thank you, and I yield back.

[The statement of Mr. Davis of Illinois follows:]

ZOE LOFGREN, CALIFORNIA
CHAIRPERSON

JAMIE RASKIN, MARYLAND
VICE CHAIRPERSON

SUSAN DAVIS, CALIFORNIA
G.K. BUTTERFIELD, NORTH CAROLINA
MARCIA FUDGE, OHIO
PETE AGUILAR, CALIFORNIA

JAMIE FLEET, STAFF DIRECTOR

Congress of the United States

House of Representatives
COMMITTEE ON HOUSE ADMINISTRATION
1309 Longworth House Office Building
Washington, D.C. 20515-6157
(202) 225-2061
<https://cha.house.gov>

RODNEY DAVIS, ILLINOIS
RANKING MINORITY MEMBER

MARK WALKER, NORTH CAROLINA
BARRY LOUDERMILK, GEORGIA

ONE HUNDRED SIXTEENTH CONGRESS

JEN DAULBY, MINORITY STAFF DIRECTOR

Ranking Member Rodney Davis Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House July 17, 2020 Opening Statement

Chairperson Lofgren, thank you for holding today's hearing. It is one of the first public-facing discussion on the feasibility of remote voting for the House of Representatives and think it is an important conversation to have. I hope today is the start of a transparent process for evaluating what remote voting options are feasible for the House to consider and what the consequences might be of moving forward with implementation.

I would also like to welcome all of our witnesses, especially former Speaker Gingrich. I believe the Speaker offers a unique perspective of the Congress and will be able to help all of us put the challenges the House is facing today in a larger historical context with other significant moments that Congress faced and yet continued work on behalf of the American people.

I know today's hearing is focused on remote voting, however, I think it is important to lay-out from my perspective how we have gotten to this point and the process that has driven the operational decision making of this institution during the COVID 19 pandemic. Earlier this year as the coronavirus began spreading across our country and the rest of the world, we knew it was only a matter of time until the People's House would be impacted.

In March, there was a bi-partisan effort to quickly transition thousands of staff to telework. This was an enormous lift and only made possible through the tireless work of the Chief Administrative Officer and Sergeant at Arms offices. Shortly after standing up the remote posture, attention was given to providing PPE to offices, initially focused on essential workers on campus and then to district offices. That distribution process has worked well to date, again credit goes to the Architect of the Capitol, CAO, and SAA for a job well done.

The conversation then turned to additional procedural changes that would be required for the House to continue to operate. These efforts did not include bi-partisan input, but what was produced was a report by the Democratic staff at the

House Rules committee. The report was issued on March 23rd and outlined the pros and cons of various options, including remote voting, proxy voting, paired voting, provisional quorum, etc. The report concluded that remote voting in any form would “*almost certainly cause unintended consequences if not done with adequate forethought and discussion*” and “*change cannot be implemented overnight, and likely cannot be accomplished in time to address the current crisis.*”

One month later on April 22nd, having conducted no public hearings and minimal bi-partisan discussion, the Democratic majority introduced a resolution authorizing proxy voting and remote committee proceedings. However, it quickly became clear the majority did not have the votes needed to pass this resolution, owing to the rushed process, and it was pulled from the floor later that day.

The same day, at the request of Speaker Pelosi a bi-partisan working group was formed to try and develop bi-partisan agreement. The group consisted of the majority leader, republican leader, chair and ranking member of the Rules committee, Chairperson Lofgren and myself. The group met three times, it became clear that even after offering thoughtful input and ideas, the majority was going to move forward in a partisan way.

On May 15th, on a party-line vote, the majority passed H. Res 965 which authorized proxy voting, remote committee hearings and markups, and authorized remote voting pending a certification from Chairperson Lofgren. Since late May the implementation of H. Res 965 has resulted in 572 proxy votes cast on the House Floor, dozens of virtual hearings and markups, and a lawsuit filed in Federal Court on the grounds that proxy voting is unconstitutional.

During today’s hearing we will hear lots of discussion on IT capabilities that could support remote voting, the types of requirements such a system should have to safeguard against threats, and examples of entities already using remote voting. Four months before this hearing, when it became apparent the direction the democratic majority was heading, I directed my team to formally engage with GAO to better understand remote voting technologies. This engagement has been productive, and I am confident that there is technology that exists to support remote voting. I also have confidence in the Clerk and her staff’s ability to execute if directed.

What I am concerned about is that the House seems to be in a very reactionary posture, with sweeping changes being made with little consideration around longer-term impacts. We have already seen numerous hearings and markups disrupted by technical difficulties resulting in the nature of those proceedings changing; fewer stand-alone amendments being made-in-order for Floor consideration; increased usage of en bloc amendment packages at committee meetings and on the Floor; and dozens of examples of members from both parties not following the prescribed regulations for H. Res 965 with no consequences. No

one can say with a straight face that these trends are a good thing or that the quality of the deliberative process that is a hallmark of the House hasn't been sacrificed.

Over the last 6 months we have seen "essential" workers across our nation step up, make sacrifices, and take on risk, all in the name of our collective wellbeing. I know the grocery store clerks, truck drivers, farmers, healthcare workers, and first responders in my district expect their elected leaders to have the same wiliness and patriotic duty to make sacrifices, just as they do every shift. Americans look to their elected leaders to set an example. And they don't appreciate Congress skipping out on their duties to attend events across their states that seem more desirable than the difficult task of governing in a pandemic.

As our country continues to be impacted by the coronavirus, the example I want to set is that we stand side-by-side with the "essential" workers of this country and I don't believe that can be done behind a computer screen and over emails. We have debated scenarios like this before and members who are unable to travel can submit excused absences and we have a Rule, that this majority adopted at the beginning of this conference, that allows for quorum to be adjusted in an emergency.

I will end with a quote from the UK's House of Commons Leader, Jacob Rees-Mogg who recently announced they will be scaling back their virtual parliament. *"Rather than suffering the depredation of a muted hybrid parliament we are once again talking to each other in ways impossible when we were scattered to the four winds. Rather than wading through the treacle of the hybrid proceedings, we are once again feet a foot and dancing a legislative quick step."*

Thank you and I yield back

The CHAIRPERSON. The gentleman yields back.

Without objection, other Members of the Committee may have their opening statements included in the record.

I would now like to introduce each member of our panel. Each of our witnesses will be recognized for five minutes, and I will remind our witnesses that their entire written statements will be made part of the record.

Also, please note that there should be a timer on your screen. Please be sure that you can see the timer and are mindful of the five-minute limit. I don't have a heavy gavel, but we do hope to keep within the five minutes.

Let me introduce our witnesses. First, we have Cheryl Johnson, who is the 36th individual to serve as Clerk of the United States House of Representatives. As Clerk, Ms. Johnson has a variety of legislative, ceremonial, administrative, and preservation responsibilities. These responsibilities include but are not limited to certifying passage of House bills and resolutions, maintaining the electronic voting system, and retaining a permanent set of the books and documents generated by the House.

Before being sworn in as Clerk in February of 2019, Ms. Johnson worked for nearly 20 years in the House and 10 years at the Smithsonian Institution.

Next, we have Representative Newt Gingrich. Mr. Gingrich served as Speaker of the House in the 104th and the 105th Congresses. He was first elected to the House in 1978 and represented Georgia's Sixth District from 1979 until 1999.

Mr. Gingrich has served as a member of the Defense Policy Board and was a candidate for the Republican Presidential nomination during the 2012 election. He has also written 36 books. He serves as a distinguished visiting scholar and professor at the National Defense University.

I would note that he is joining us from Rome today, and welcome. I know it is about 7:30 p.m. your time. So we appreciate this. And I just—as a personal note, I would note that my very first day as a Member of Congress was the day that you became Speaker of the House. So welcome. It is good to see you again.

Bill Crowell is an expert in information technology, security, and intelligence systems. He is the former Deputy Director of the National Security Agency and was appointed to this position after serving as Deputy Director of Operations.

After his service at the NSA, Mr. Crowell moved to the private sector and served as CEO of Cylink Corporation, a public e-business security solution company, and Chairman of BroadWare Technologies, a video surveillance software company.

He also served as Chairman of the Director of National Intelligence Senior Advisory Group from 2007 to 2014 and currently sits on the Department of Homeland Security Science and Technology Advisory Board.

Jon Green is a vice president and the chief technologist for cybersecurity and government solutions at Aruba Networks, a Hewlett Packard Enterprise Company. In this role, he is responsible for providing technology guidance and leadership for all security solutions, including authentication and network access control, encryption, firewall, and VPN.

He works closely with the U.S. Government on secure network and remote access solutions and manages both Aruba's Product Security Response Team and its Threat Lab, an internal security research group.

Dr. Ron Rivest is an institute professor at the Massachusetts Institute of Technology. He is widely known as coauthor of the textbook "Introduction to Algorithms" and as coinventor of the RSA public-key cryptosystem. He is also a cofounder of both RSA and Verisign.

An expert in election security and cryptography, Dr. Rivest is a recipient of the ACM Turing Award, the BBVA Frontiers of Knowledge Award, and a Marconi Prize. He has served on the Election Assistance Commission's Technical Guidelines Development Committee and is a member of the Caltech/MIT Voting Technology Project, as well as the Board of Verified Voting.

Dr. Aviel Rubin is a professor of computer science at Johns Hopkins University, where he also serves as technical director of the Information Security Institute. Dr. Rubin is an expert in computer security and applied cryptography and was among the first to expose the vulnerabilities of electronic voting in his book "Brave New Ballot: The Battle to Safeguard Democracy in the Age of Electronic Voting."

Dr. Rubin has briefed Congress and the Department of Defense on election tampering and other national security issues. He served as director and principal investigator for the National Science Foundation's Center for Correct, Usable, Reliable, Auditable, and Transparent Elections, otherwise known as the ACCURATE Center.

Dr. David Wagner is a professor of computer science at UC Berkeley, where he has worked on electronic voting, software security, wireless security, sensor network security, and applied cryptography. He is a part of Berkeley's security research group and is also an active member of the ACCURATE Center.

Dr. Wagner has developed quite a bit of software, including tools to help with the auditing of elections. In addition to his duties as a professor, Dr. Wagner currently sits on the editorial board for the Journal of Election Technology Systems and is part of the Science of Security Project.

These are distinguished witnesses, and we are eager to hear from them.

So I will first recognize Ms. Johnson for your testimony of about 5 minutes. Welcome.

STATEMENTS OF THE HONORABLE CHERYL L. JOHNSON, CLERK OF THE U.S. HOUSE OF REPRESENTATIVES; NEWT GINGRICH, FORMER SPEAKER OF THE HOUSE; WILLIAM CROWELL, PARTNER, ALSOP LOUIE PARTNERS; JON GREEN, VICE PRESIDENT AND CHIEF SECURITY TECHNOLOGIST, ARUBA NETWORKS; RONALD L. RIVEST, INSTITUTE PROFESSOR, MIT COMPUTER SCIENCE AND ARTIFICIAL INTELLIGENCE LAB; AVIEL RUBIN, PROFESSOR AND TECHNICAL DIRECTOR, THE JOHNS HOPKINS UNIVERSITY INFORMATION SECURITY INSTITUTE; AND DAVID WAGNER, PROFESSOR, COMPUTER SCIENCE DIVISION, UNIVERSITY OF CALIFORNIA, BERKELEY.

STATEMENT OF THE HONORABLE CHERYL L. JOHNSON

Ms. JOHNSON. Thank you. Good afternoon. Chairperson Lofgren, Ranking Member Davis, Members of the Committee, thank you for inviting me to participate in this hearing on such a critical topic.

Since 1789, the Office of the Clerk has supported the legislative functions of the U.S. House of Representatives. The Clerk maintains the House Journal, certifies the passage of legislation, verifies the accuracy of each individual vote, records the vote, tallies the vote, and transmits the results to the public.

After 181 years of manual voting, the House passed the Legislative Reorganization Act of 1970, authorizing electronic voting. And while the bill was passed in 1970, it was another 3 years before the system was developed and put into use. That system, the Electronic Voting System, or EVS, is a real-time, computerized information system. EVS resides on its own private air-gapped network, separated from the House network, which affords it a very high level of security.

The voting procedures are as follows: Voting stations are distributed throughout the Chamber and equipped with a vote card slot, voting buttons, and a system readiness indicator. Each Member who chooses to vote electronically does so by inserting a personalized voting card into a voting station and selecting a voting button to cast their vote. Voting results are displayed on screens in the House Chamber.

In 2018, all of the voting stations were upgraded with the latest proximity card reader technology and new capability to assist visually impaired Members. An LED display was added to provide additional vote confirmation to Members directly on the vote station. We also implemented a new network architecture for greater security and flexibility for future expansions.

I am confident that, as the House looks to our office to inform and implement the critical decisions it will make in the coming months and years to preserve and protect the legislative process, we will rise to the occasion.

Recently, pursuant to House Resolution 965, the House allowed its first proxy vote. On our website, we post the letters which designate who holds the proxy for the Member voting by proxy. Our staff worked long and hard to ensure a successful implementation. To date, we have held 29 votes with proxies without incident.

The topic you are discussing today and moving forward is of great importance. However the House decides to proceed on how it

conducts voting, our office will be prepared to advise on the associated costs, benefits, and challenges, and we will be prepared to implement whatever decisions are made to ensure the continuity of this irreplaceable institution.

If the House chooses to pursue remote voting, we will need to perform an exhaustive review of the requirements, available technology, design options, and, once developed, a very thorough testing to ensure its highest level of security, reliability, and availability.

It is critical that we ensure complete confidence of the Members and the public in the way House votes are recorded. As with the initial development of the EVS and with each past upgrade, it will be critical to take the necessary time to implement any remote voting system correctly and securely.

The mission of the Clerk's Office is to support the House in carrying out its legislative responsibilities, and I am committed to these duties with maximum integrity and reliability.

Thank you, and I look forward to your questions.

[The statement of Ms. Johnson follows:]



**STATEMENT BEFORE THE COMMITTEE
ON HOUSE ADMINISTRATION**

**EXPLORING THE FEASIBILITY
AND SECURITY OF TECHNOLOGY
TO CONDUCT REMOTE VOTING
IN THE HOUSE**

THE HONORABLE CHERYL L. JOHNSON

JULY 17, 2020

Chairperson Lofgren, Ranking Member Davis, and Members of the Committee:

Thank you for inviting me to participate in this hearing on such a critical topic.

Since 1789 the Office of the Clerk has supported the legislative functions of the U.S. House of Representatives. The Clerk maintains the House Journal, carries bills to the Senate, delivers enrolled bills to the White House, maintains the official records of the House, and certifies the passage of legislation. The Clerk is responsible for verifying the accuracy of each vote, tallying the vote, recording the vote, and transmitting the results to the public.

After 181 years of manual voting, the House passed the Legislative Reorganization Act of 1970 authorizing electronic voting. And while the bill was passed in 1970, it was another three years before the system was developed and put into use. That system, the Electronic Voting System, or EVS, is a real-time, computerized information system. The EVS resides on its own private air-gapped network, separated from the House network, which affords it a very high level of security.

The voting procedures are as follows:

- Voting stations are distributed throughout the House Chamber and each is equipped with a voting card slot, voting buttons, and a system-readiness indicator.
- Each Member who chooses to vote electronically does so by inserting a personalized voting card into a voting station and selecting a voting button to cast his or her vote.
- Voting results are displayed on screens in the Chamber.

In 2018 we upgraded all the voting stations with the latest proximity card reader technology and new assistive technology for members with visual impairments. We added an LED display to provide additional vote confirmation to members directly on the voting station. We also implemented a new network architecture for greater security and flexibility for future expansions.

I am confident that we will rise to the occasion, as we always have, as the House looks to our Office to inform and implement the critical decisions it will make in the coming months and years to preserve and protect the legislative process.

Recently, many of our staff worked around the clock to develop a new electronic system for filing legislative measures and extensions of remarks, the eHopper. Since the Speaker's April 6 announcement of this new policy, there have been 1,213 measures filed electronically and 51 filed traditionally. There have also been 869 submissions for the Congressional Record.

Similarly, on May 27 of this year, pursuant to House Resolution 965, the House allowed its first proxy vote. On our website, we post the letters that designate who holds the proxy for each Member voting by proxy. As with the eHopper, our staff worked long and hard to ensure a successful implementation. To date, we have conducted 29 votes with proxies without incident.

The topic you are discussing today and moving forward is of great importance. However the House decides to proceed on how it conducts voting, our Office will be prepared to advise on the associated costs, benefits, and challenges, and we will be prepared to implement whatever decisions it makes to ensure the continuity of this irreplaceable institution.

If the House chooses to pursue remote voting, we will need to perform an exhaustive review of the requirements, available technology, and design options. After it is developed, we will need to conduct very thorough testing to ensure its highest level of security and reliability.

It is critical that we ensure complete confidence—both contemporaneously and historically—of the Members and the public in the way House votes are recorded. As with the initial development of the EVS and with each upgrade, we must take the necessary time to implement any remote voting system correctly and securely.

The mission of the Clerk's Office is to support the House in carrying out its legislative responsibilities, and I am committed to these duties with maximum integrity and reliability.

Thank you.

The CHAIRPERSON. Thank you very much. It is great to hear from you.

Now, I would like to recognize our former Speaker.

Mr. Gingrich, we are looking forward to hearing your testimony. You may need to unmute. Can somebody unmute Mr. Gingrich?

Mr. GINGRICH. I think I am now unmuted.

The CHAIRPERSON. There you are. We can hear you.

STATEMENT OF NEWT GINGRICH

Mr. GINGRICH. Okay. Sorry. Let me just say, first of all, thank you, Chairperson Lofgren, and I want to thank Ranking Member Davis. I served for a decade on the House Administration Committee. So it is kind of fun to be back and be part of this process.

I think learning by video is very good and very useful. I think trying to govern by video is a disaster. And the key factor is not going to be all the technology we hear about today. The key factor is how human beings learn and the pattern of the collective dialogue which makes up a legislative body and how, over time, its Members become collectively smarter by interacting with each other.

The Founding Fathers were virtually all members of legislatures before they created the United States, and they believed in the legislature. In fact, if you look at the Constitution, the legislative branch is first and has a long section devoted to the House and Senate before they get around to the executive branch.

The Federalist Papers make very clear that they thought a legislative parliament meeting on a regular basis was a key to protecting freedom. And the reason they thought that is that they had studied carefully the rise of Cromwell as a dictator during the English civil war, and they were very frightened that an executive branch that didn't have a vigorous legislative body would always be a danger and a threat to our freedom.

So their view was that you had to have people who got together regularly; they had to bond together; they had to be prepared to do things, to learn from each other, and to communicate. I remember, when I used to be on the House floor, during the course of one or two votes, you could see 8, 10, 12, 15 different people, learn about things all across the country.

So I want to emphasize from my part—not the technology. You will hear a lot about technology today—although with all the various hacking, I would be worried about it. But I don't worry about technology. I worry about history and the nature of human institutions, and I think they require us to physically be together regularly.

I would just say that I think there are three severe consequences of going to any kind of remote system. The first, as a former Speaker who has been accused on occasion of being very powerful, I think when everybody else is out of town, the Speaker and their staff become virtually a dictatorship because they have all the power; they have all the ability to deal with the executive branch, to deal with the Senate, and I think it puts the average Member at an enormous disadvantage.

Second, the individual Members are isolated. Oh, they may communicate back and forth, but there is an enormous biological power

in people being physically together. And that is why I want to emphasize, if you study history, going back to the Greeks, the Romans, coming up through the Middle Ages, you will see why the rise of legislative bodies, whether it was the Roman Senate or it was the British Parliament, why these institutions always involve people coming into a room, meeting with each other, bonding, sharing ideas, and it is a very simple thing.

I think, third, the legislation will be less well thought through. There is an enormous power to the legislative process as it improves, as different Members bring in ideas, as different people find things that are wrong. That process really matters, and the legislative product gets to be dramatically better the more there is a systemic legislative process. And I think that the natural pattern of having remote voting will be to dramatically weaken that process.

Lastly, I guess, I want to challenge what I sense is an absurd level of fear. Because Callista is the Ambassador of the Vatican, I have been living in Rome. We have lived through the pandemic. Italy closed down. There was a crisis comparable to New York City. But I am very worried by the level of fear that I sense in the United States and this sense of danger.

You know, we used to say—we used to sing, “We are the land of the brave and the home of the free.” I sense we are beginning to be the land of the timid and the home of the fearful. And I recently wrote Franklin Delano Roosevelt’s great admonition that we have nothing to fear but fear itself.

I think the idea that politicians are too precious to come together at a time—as you pointed out, Chairperson Lofgren, truck drivers, people who run grocery stores, people who work in restaurants, the number of Americans every day who are going about their business—you can be prudent. You can wear masks. You can have social distancing. But this idea that the current challenge leads us into a radical disruption of 3,000 years of legislative history I think is a very, very sad commentary on the American system. Politicians are not more important than truck drivers. They are not more important than nurses, or they are not more important than, frankly, people who work in a restaurant or at a Walmart or at a grocery store.

So I wish you would drop this sense of panic, relax, figure out how to get together in a healthy way and show the country by example that we can, in fact, function even under this challenge. Thank you for giving me a couple seconds more than my time.

[The statement of Mr. Gingrich follows:]

Statement by Former Speaker of the US House of Representatives Newt Gingrich
Committee on House Administration
July 17, 2020

Remote Voting

Thank you for allowing me to testify even if virtually. I am still in Rome, where my wife Callista is the Ambassador to the Vatican, and I appreciate the opportunity to participate.

We have all learned through the virus-driven period of isolation and quarantine that there are many electronic systems for distance communication, including FaceTime, Zoom, GotoMeeting, Skype, and a host of competitors. Some major universities and schools have learned to use distance learning with great effectiveness.

I have always favored the use of distance communications for learning. That is why I think it is appropriate to gather information with distance witnesses for committee hearings. However, the question of remote voting in a legislative body raises a different issue that is separate from convenience of technological capability.

Legislative bodies have a long and profound history in the emergence of freedom and self-government. Whether they were in Greek city states or in the Senate of the Roman Republic, the existence of legislative bodies were a powerful invention to involve citizens in their own government and to enable elected officials to work together in understanding and solving problems.

There are two key factors in the very nature of legislative bodies which require them to get together physically to truly function at the highest level they are capable. First, there is the collective learning curve of people working together over time. Second there is the collective power of a legislature when its members have reached a decision they are determined to implement even when faced by opposition from the executive branch.

First, people who get in a room and argue, think, and learn together achieve much greater depth of knowledge than people who are isolated. In the great historic periods of legislative assertiveness, it was mutual knowledge and the sense of mutual collaboration which enabled elected officials to find better solutions than they would have found on their own.

In a well-functioning legislative body, the whole is much greater than the sum of the individual members. It is this synergistic effect by which people from different regions, professions, ideologies, and personal experiences blend into a mutually improving system.

A sound legislative process works when an individual develops an idea. It starts to get put into legislative language. Someone else brings a different specialty or expertise, and the idea is improved dramatically. Then, a third person brings a unique regional or interest group perspective and points out the modifications needed to make the idea really work. It is precisely this system of improvement and maturation – moving from conception, to introduction of legislation, to an amending process at subcommittee, committee, and the floor – that helps legislation meet the needs of the people.

When a bill gets through one body (House or Senate), then the other body follows a similar process. Finally, the House and Senate come together to hammer out a final version which will go to the President.

This process requires human interaction and mutual learning at every step of the way. It is the *process* which ultimately leads to the best *product*. This kind of process requires humans in the same room to really share knowledge and grow intellectually. The Founding Fathers had virtually all served in colonial legislative bodies. They understood the process of winning and losing elections. They understood the process of legislating together in groups.

In fact, the Founding Fathers felt so strongly about the importance of legislatures that in the US Constitution, Article I provides that all legislative power be vested in a Congress consisting of a House and Senate. Section two is the House, and Section three is the Senate.

Only after clearly defining and writing at length about the duties and powers of the legislative branch did the Founding Fathers get around to writing about the President and the Executive Branch.

The Federalist Papers, the great exposition of the Constitution by Alexander Hamilton, James Madison and John Jay makes clear (by repetition and inference) that an elected legislature meeting regularly is central to protecting the liberty of the people.

The Founding Fathers, in addition to their knowledge of Greek and Roman history and their study of various governments in the middle ages, were steeped in English history. They felt deeply that the Magna Carta, tying the King's ability to get money to the permission of the people was the bedrock from which all other legislative power grew. They had studied the erosion of the Parliament's power under King James I, and its resurgence under King Charles I – which led to the Civil War largely as a result of parliamentary opposition to the King.

The Founding Fathers had a particular fear of Oliver Cromwell and the imposition of a dictator who would break outside the agreed charter of self-government. They were determined that the legislative branch would be close enough to the people that it could draw its strength against any effort at despotism by the Executive Branch.

It is this need to get to know each other well enough to have long conversations – and to grow together in the face of threats to our freedom – that led the Founding Fathers to place so much faith in a freely-elected legislative body with two branches.

Given this history, there are three severe consequences of shifting toward remote voting:

First, the amount of power centered on the Speaker will create a virtual legislative dictatorship.

There have been moments of strong Speakers in our history. In each case, when they grew too strong, the legislative body as a group confronted them and forced change (the joint progressive Republican-Democrat coalition that broke Speaker Joseph Cannon's power in 1910 is the classic example).

If every member of Congress is back at home, the Speaker and his or her staff will have virtually unlimited ability to shape the legislation they want, make the deals with the Senate and the President they want, and become virtually unchallengeable. The defense of freedom which the Founding Fathers had made the most important mission of the legislative branch would be destroyed by this single development.

A dictatorial Speaker is potentially just as destructive and dangerous as a dictatorial President. This challenge is not personality-dependent, and it is not particularly aimed at the current Speaker. Lord John Acton warned us over a century ago that “power tends to corrupt and absolute power corrupts absolutely.”

We are not any more immune to that process of corruption than any other people or any other generation. If you leave most of the House members at home, those who do come to Washington will acquire vastly more power and have vastly increased temptation to use their power corruptly.

Second, the individual members will lack the mentorship and the collegiality which has grown so many legislators over the last 244 years.

The legislative process is a continuing apprenticeship and educational experience. Legislating, the act of voluntarily getting free people from many different backgrounds and regions to work together, is one of the most complex things human beings do. It takes years to learn to be an effective legislator.

Ask any third- or fourth-term member how much more he or she understands about the legislative process than when he or she first arrived. Ask how much of that learning came from hanging out and listening to colleagues. I was very honored to go through what might be called “the school of legislating” for over a decade before I joined the Republican leadership.

Without that kind of personal relationship and camaraderie, I seriously doubt if I could have learned enough to develop the Contract with America, passed major reforms like welfare reform, or achieved a balanced budget.

A House that votes remotely will remain remote to itself. Its members will have deeply stunted growth in vital skills and no access to invaluable knowledge.

Third, legislation will become a lot more inadequate – and in some cases, just plain dumb – as the traditional process of working together and sharing information and different perspectives changes into a more distant, irregular, and inevitably disrupted process.

The US Congress would become a detached collection of echo chambers – and America would be hurt by it.

Please let me add one final word about the whole underlying reason for considering remote voting.

Our national anthem says we are “the land of the free and the home of the brave.” Our Founding Fathers risked their lives, fortunes and sacred honor to defend freedom. The Civil War generation lost 630,000 Americans fighting for the Union and to end slavery. The Greatest Generation went across the planet risking its lives to defeat Nazi Germany and Imperial Japan. By the way, through all these events, Congress met in person.

Now, we are told that our members of the House are too precious to risk their lives by coming to Washington.

To these members I would say: If freedom isn't worth the risk, quit the Congress. Someone with more courage will replace you in a special election. The emotion driving the proposal for remote voting is an expression of a kind of cowardice I would never have expected to see in America.

We are asking children and teachers to go back to school, but House members can't come to Washington.

We are asking truckers to crisscross the country bringing us food and supplies, but their representatives have to hide in fear and vote electronically to avoid risk.

We have young men and women risking their lives all across the planet to protect freedom, but their elected leaders can't risk being in a room with immediate access to doctors and remarkably little risk of anything bad happening.

I am embarrassed for this House that such a proposal could even get to a hearing.

I hope you will table it and move on to issues more worthy of the United States House of Representatives.

The CHAIRPERSON. Thank you, Mr. Gingrich.

We will now hear from Bill Crowell.

Mr. Crowell, you are recognized for your testimony. You need to unmute your microphone.

STATEMENT OF WILLIAM CROWELL

Mr. CROWELL. Thank you very much, Chairperson Lofgren. It is a pleasure to be with the Committee, and I appreciate the opportunity. My name is Bill Crowell, and I am testifying today as a private citizen and not on behalf of any entity.

I think that it is reasonable to parse the challenges associated with remote voting into four major categories: The first, videoconferencing systems with the right functionality and superiority. The second, voting systems with verification of the identity of the Members and of their votes and with the functionality required to carry out your legal obligations. Technical issues, such as connectivity, operating capacity, certification of the security of the system, and secure end-to-end encryption and multifactor authentication, and secure storage of all relevant documents and records, is the third item. And the last is adequate funding to acquire, maintain, and operate and certify the systems.

There are many videoconferencing systems. They vary widely in their features and functions as well as the level of security. Only a few have end-to-end encryption, and none are certified for classified information unless operated in a secure facility.

Many of them were either developed outside the United States or have considerable operating support coming from outside the United States, which raises extra concerns about their security and their reliability.

Also, since COVID-19 has significantly increased the use of videoconferencing, a number of these systems have been subjected to successful cyber attacks, underscoring the lack of cyber resilience of this method of staying connected.

With regard to voting systems during the COVID-19 pandemic, at least 24 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 use of a number of videoconferencing systems as a 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. It is my belief that the most attractive solution for remote voting is a purpose-built software package that incorporates all of the attributes associated with congressional process, including committee management, remote hearings, document and bill markup, archiving, public access to the proceedings, and recorded votes, and of course, an easy-to-use remote voting process.

There are several technical issues that also can limit or interfere with the success of our remote voting system. First on that list is the fact that Members and staff do not use the same devices either in their districts or on the road. In addition, the internet service providers in their districts provide differing levels of performance.

Security issues are the most prevalent and pervasive technical issue in this digital age. Specifically, multifactor authentication, end-to-end encryption, and verification or audit of all 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 been commonplace. They are carried out by nation-states, criminals, hacktivists, as well as hackers just seeking the thrill of a successful attack. A remote voting system must be resilient against all of these bad actors, particularly nation-states who are seeking to disrupt our democratic processes.

Last but not least of the four categories is providing sufficient funding to acquire and certify services.

In conclusion, I believe there are many factors that can impede successful deployment operation of remote voting solution in the House, but I also think that many of these can be mitigated. I hope that my parsing of this problem is useful in your framing of an approach that maximizes the functionality needed to make this effort successful.

And thank you very much for the opportunity to provide a perspective on this important topic. I look forward to answering your questions.

[The statement of Mr. Crowell follows:]

**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.

The CHAIRPERSON. Thank you very much.
I will now recognize Mr. Green for his testimony.
Mr. Green, you are welcome to testify.

STATEMENT OF JON GREEN

Mr. GREEN. Thank you. Chairperson Lofgren and Ranking Member Davis and Members of the Committee, thank you for inviting me to testify today as you explore the feasibility and security of remote voting for House Members.

While recognizing that this institution is founded on in-person engagement and voting environments, the current pandemic has made it entirely reasonable to consider technology that allows for secure remote voting.

I have spent the past 17 years working for Aruba, a part of Hewlett Packard Enterprise, and for the past 10 years, I have worked closely with our U.S. and allied partner government customers on secure network and remote access solutions. I hope that experience will help provide relevant information on today's topic.

Before beginning my formal testimony, I want to thank Chairperson Lofgren for her representation of San Jose and Silicon Valley for the past 25 years. HPE and the larger technology community in the Valley are grateful for her consistent support and leadership.

Let me assure you that you are not alone in trying to adapt to the new world of work-from-home orders. Since this pandemic began, we have received thousands of inquiries from our Enterprise customers seeking solutions to enable secure remote working. It is fair to say that very few of them envisioned a world where 100 percent of their workforce would suddenly be working from home.

Such widespread remote working brings with it additional challenges. End users without the benefit of on-site IT support personnel often become frustrated when their technology doesn't work correctly. And without protections provided by IT security solutions, users often turn to that which is convenient, such as personal email accounts, rather than that which is secure. The stakes are very high when it comes to remote voting in the House, so it is critical to provide Members a solution that is both convenient and secure.

In the world of information security, we often speak of the CIA triad. Not to be confused with the intelligence agency, CIA stands for confidentiality, integrity, and availability, the three most important aspects of a secure system. Many people equate security with confidentiality, but in remote voting, the most important principle is actually integrity, the guarantee that information is trustworthy, consistent, accurate, and originated from the correct person.

Second in importance is availability. A Member must be able to cast a vote during the period that voting is open. We have all seen the reports documenting foreign adversary interference in U.S. public elections, and we can't for a minute believe that adversaries would not also try to interfere in congressional voting. For that reason, it is imperative that the House implement the highest degree of security possible.

Fortunately, a model already exists for highly secure remote access. Congress does not have to go first. Ten years ago, the Na-

tional Security Agency introduced a program known as Commercial Solutions for Classified, which has been widely adopted by the DOD, the intelligence community, law enforcement, and others to connect classified systems and devices over untrusted networks using commercial off-the-shelf IT products. The same architecture has been also deployed for unclassified systems when organizations have needed to adopt the best security available. Congress can dispense with months of security analysis by adopting an existing, proven architecture.

Overall, I believe we need to focus on four key principles to ensure a successful remote voting program: First, as previously mentioned, secure remote network connectivity should be provided following the NSA Commercial Solutions for Classified architecture. This ensures that Members of Congress are not connecting directly to malicious or compromised networks.

Second, dedicated voting devices should be issued to each Member to be used only for the purpose of voting. These could take the form of laptops, tablets, or smartphones with a simple application showing buttons labeled yes, no, and present.

Third, multifactor authentication would be mandatory for such a solution. It is critical to ensure that the Member and only the Member is the person casting a vote. Multifactor authentication is already widely used by the Federal Government and is a well-understood technology.

And, fourth, a manual system of vote verification is required. The Member needs a way to verify that the correct vote was registered in real time in a system that is visible to all. This could be as simple as monitoring the vote on C-SPAN.

My remaining caution to you is to focus on availability. We can solve for integrity and confidentiality, but availability is often overlooked. Systems deployed today that use public internet rely on users being lost in a crowd, their internet traffic appearing indistinguishable from others.

If an adversary were able to pinpoint the internet location of each Congressional Member, then targeted denial-of-service attacks could prevent specific Members from casting their votes. To counter this threat, backup systems of voting must remain available and time limits on voting windows may need to be relaxed. As skilled as we are today at engineering reliable networks, the best backup systems are often low tech.

In summary, I believe that should you decide to move forward, remote voting is technically feasible, can be enabled for a reasonable cost, and can be done with an appropriately high level of security.

Thank you again for the opportunity to offer testimony. I look forward to answering any questions you may have.

[The statement of Mr. Green follows:]



3333 SCOTT BLVD
SANTA CLARA, CA 95054

T: 1.408.227.4500
FAX: 1.408.227.4550

WWW.ARUBANETWORKS.COM

**TESTIMONY BEFORE THE HOUSE COMMITTEE ON ADMINISTRATION
HEARING ON
“EXPLORING THE FEASIBILITY AND SECURITY OF TECHNOLOGY TO CONDUCT
REMOTE VOTING IN THE HOUSE”**

**JON GREEN
CHIEF TECHNOLOGIST, CYBERSECURITY AND GOVERNMENT SOLUTIONS
ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY**

JULY 17, 2020

Chairwoman Lofgren, Ranking Member Davis, Members of the Committee, thank you for inviting me to testify as you explore the feasibility and security of remote voting for those of you serving in the House of Representatives. While recognizing that this institution is founded on in-person engagement and voting requirements, the current pandemic has created an unprecedented need to consider technology that allows for secure remote voting capabilities. I am the Chief Technologist for cybersecurity and government solutions at Aruba, a part of Hewlett Packard Enterprise (HPE), where I’ve spent the past 17 years. For the past ten years, I’ve worked closely with our US and allied partner government customers on secure network and remote access solutions, and I hope that experience will help me provide relevant information on today’s topic.

Before beginning my formal testimony, I want to thank Chairwoman Lofgren for her representation of San Jose and Silicon Valley over the past 25 years. HPE and the larger technology community in the Valley are grateful for her consistent support and leadership. I also appreciate the hard work that the Members and staff of the House Administration Committee have done over the past four months to keep the House of Representatives up and running. A functioning legislative branch is critical to successfully addressing the ongoing pandemic, and alternatives for safe and secure voting should be a part of any plan.



As you may know, in 2015 Hewlett Packard Enterprise emerged from HP, an 80+ year old technology innovator in the United States, and you will find our IT products and services interwoven throughout organizations around the world. Based on our experience, I can assure you that you are not alone in trying to adapt to the new world of work-from-home orders. Since this pandemic began, we have received thousands of inquiries from our enterprise customers, both inside and outside the government, seeking solutions to enable secure remote working. The fortunate ones had begun remote working initiatives years ago and only needed to expand their existing footprint, but it's fair to say that very few of our customers had ever envisioned a world where 100% of their workforce would be working from home. Such widespread remote working brings with it additional challenges. End users, without the benefit of on-site IT support personnel, often become frustrated if their technology doesn't work the same way it does inside the office. And without protections provided by enterprise IT security solutions, users often turn to that which is convenient, such as personal email accounts, rather than that which is secure. The stakes are very high when it comes to remote voting in the House, so it is critical to provide Members a solution that is *both* convenient and secure.

In the world of information security, we often speak of the CIA triad. Not to be confused with a US intelligence agency, CIA stands for confidentiality, integrity, and availability – the three most important aspects of a secure system. Many people equate “security” with “confidentiality”, but in remote voting the most important principle is actually *integrity* – the guarantee that information is trustworthy, consistent, accurate, and originated from the correct person. Second in importance is availability – the system must be highly reliable so that a Member is able to cast a vote during the period that voting is open. We have all seen the reports documenting foreign adversary interference in US public elections and we can't for a minute believe that adversaries would not also try to interfere in Congressional voting. For that reason, it is imperative that the House implement the highest degree of security possible, and consider backup options.



Fortunately, a model already exists for highly secure remote access; Congress does not have to go first. Since approximately 2010, I and other industry colleagues have worked closely with the National Security Agency on an architecture and program known as Commercial Solutions for Classified. This program has been widely used by the DoD, the intelligence community, the Department of Energy, law enforcement, and others to connect classified systems and devices over Wi-Fi networks, cellular networks, and the public Internet using commercial off-the-shelf information technology products. This same architecture has also been deployed for unclassified systems when organizations have needed to adopt the best security available. The Congress can dispense with months of security analysis by adopting an existing proven architecture, with reasonable modifications where necessary.

Overall, I believe we need to focus on four key principles to ensure a successful remote voting program:

- First, as previously mentioned, secure remote network connectivity should be provided using a layered approach that follows the NSA Commercial Solutions for Classified architecture. This ensures that Members of Congress are not connecting to malicious or compromised networks.
- Second, dedicated voting devices should be issued to each Member, to be used only for the purpose of voting. These could take the form of laptops, tablets, or smartphones. Some degree of system integration would be required to ensure these devices are as simple to use as possible, but we do not need complicated custom software. Because the network is secure, nothing more than a web browser is needed, with a simple application showing buttons labeled “Yes”, “No”, and “Present”.
- Third, multi-factor authentication (e.g. something you have + something you know) would be mandatory for such a solution. It is critical to ensure that the Member, and only the Member, is the person casting a vote. Multi-factor authentication is already widely



used by the Federal government in the form of smart cards and biometrics, and is a well-understood technology.

- Fourth, a manual system of vote verification is required, to counter against both concerns around central vote tallying systems and the threat of availability attacks. In public elections, concerns over electronic voting machines can often be alleviated through use of machines that instantly print a paper voting record for the voter to verify. In remote Congressional voting, the Member needs a way to verify that the correct vote was registered, in a system that is visible to all. This could be as simple as monitoring the vote on CSPAN or listening to a conference call line as voting results are read aloud.

My remaining caution to you is to focus on availability. We can solve for integrity and confidentiality, but availability is often overlooked in security. Systems deployed today that use the public Internet rely on users being “lost in a crowd”, their Internet traffic appearing indistinguishable from others. If an adversary were able to pinpoint the Internet location, or IP address, of each Congressional member, then targeted denial of service attacks could prevent specific members from casting their votes. To counter this threat, backup systems of voting must remain available and time limits on voting windows may need to be relaxed. As skilled as we are today at engineering reliable networks, the best backup systems are often non-technical.

In summary, I believe that should you decide to move forward, remote voting is technically feasible, can be enabled for a reasonable cost, and can be done with an appropriately high level of security. Once built, such a system can be easily modified should similar emergencies arise in the future to create the need for remote voting. Thank you again for the opportunity to offer testimony and I look forward to answering any questions you may have.

The CHAIRPERSON. Thank you very much for that interesting testimony.

Dr. Rivest, you are now recognized for your testimony.

STATEMENT OF RONALD L. RIVEST

Mr. RIVEST. Thank you. Chairperson Lofgren, Ranking Member Davis, and Members of the Committee, my name is Ron Rivest. I thank you for inviting me to testify regarding the feasibility of using technology for conducting remote voting in the House. My bottom line is that such remote voting is feasible and can be made adequately secure.

I will skip a few paragraphs of my testimony since my bio has already been read. I just note that I have worked for over two decades on voting system security. And I speak here only about the security aspects of the remote voting, not about the appropriateness of remote voting for the House. That question is beyond my pay grade.

I see that the House, under House Resolution 965, is already using proxy voting for remote voting. That resolution authorizes examination of ways to vote remotely in a secure manner, hence today's hearing.

As noted, I think the House is in a good position. There are indeed suitable secure voting technologies available. The most important reason why that is true is that the House votes are not secret. Voting in the House is not based on secret ballots. That makes all the difference, as manipulation or alteration of votes can be detected and corrected.

For the record, I note that, in the U.S., secret ballot voting was first implemented in Massachusetts in 1888. However, implementing secure secret ballot remote voting is still beyond the state of the art.

Back to nonsecret voting, designing a secure voting system requires, first of all, a clear statement of the security objectives. A system can't be said to be secure if there is no specification of what security should mean for that system.

What are the baseline voting system security requirements? Here are four: Only eligible voters can vote and each at most once. Votes are cast as intended. Votes are collected as cast. And votes are counted as collected. Each property should not only be true but be verifiably true. Counting, as noted, tabulation, is not an issue since nonsecret ballots can be posted publicly and the tally then verified by anyone.

One recommended principle for achieving voting system security is that of software independence, a notion developed by John Wack of NIST and myself. This principle basically says that you never want to be in a position where you have to say, well, the result must be right because the computer says so. In other words, the election outcomes must be auditable.

Here is a sketch of a simple architectural approach for secure remote nonsecret voting to illustrate. There is a public website where all cast votes are posted. Each Congressperson composes his or her vote, digitally signs it, and sends the resulting digitally signed ballot for posting on the public website. Many digital signature schemes are available. NIST has developed digital signature stand-

ards. Digital signatures are now implemented in every browser. One approach uses the RSA public-key cryptosystem.

A nice thing about digital signatures is that the signature on a digitally signed document, such as a ballot, is verifiable by anyone. I note that a digital signature is not just a cut-and-paste image of a handwritten signature; it is a mathematical function of the message being signed and secret information specific to the signer.

Digitally signed ballots can be authenticated using public information, both as to the origin, who the voter is, and as to the content, what the ballot says. Vote manipulations are not possible, as forging digital signatures is not feasible. The most an adversary can do is to delete or duplicate votes. An adversary can conceivably delete or duplicate votes even now with proxy voting. If a Congressperson can't submit a ballot, they can't vote.

Detection and correction mechanisms can work for voting with digitally signed ballots much as they work for proxy voting. It is important to note that voters, in this case Congresspeople, can check or audit their votes as correctly recorded on the public website. Missing votes can be restored. This should be checked. This is important.

An approach sketched here bears many similarities to your current proxy voting procedures. The public website becomes the proxy for those voting remotely. Indeed, such a system should provide a smooth and secure extension of your current proxy voting procedures, which need not be abandoned. This sketch is intended only to show that it is possible to use technology to do remote, nonsecret voting in a secure manner. Many other approaches are possible.

This concludes my testimony. I would be happy to answer any questions you may have.

[The statement of Mr. Rivest follows:]

Testimony by
 Ronald L. Rivest
 (MIT Institute Professor, Cambridge, MA)

Venue:
 Hearing held by
 Committee on House Administration
 Chairperson: Rep. Zoe Lofgren (California)

Hearing Title:
 "Exploring the Feasibility and Security of Technology to Conduct
 Remote Voting in the House"

Date:
 Friday, July 17th, 2020

Time:
 1:00pm EST

Testimony (both oral and written):
 =====

Chairperson Lofgren and members of the Committee: I thank you
 for inviting me to testify regarding the feasibility of using
 technology for conducting remote voting in the House.

My bottom line is that such remote voting is feasible and can be made
 adequately secure.

By way of introduction, I am an Institute Professor at the
 Massachusetts Institute of Technology; my background includes computer
 science, information security, cryptography, and election security.

I am well known for the invention, with Adi Shamir and Len Adleman, of
 the RSA public-key cryptosystem, the first (and still widely used)
 implementation of public-key cryptography, enabling both secure
 communications and digital signatures.

I have worked for over two decades on voting security.

I was a member of the Technical Guidelines Development Committee from
 2004--2009, advisory to the Election Assistance Commission; I chaired
 the subcommittee on Computer Security and Transparency.

I am a founding member of the CalTech/MIT Voting Technology Project.

And I am on the Board of Verified Voting, a non-profit promoting voting
 system security, especially through the use of risk-limiting audits.

I speak here only about the security aspects of remote voting, not about
 the appropriateness of remote voting for the House; that question is
 beyond my pay grade!

I see that the House, under Resolution 965, is already using proxy voting for remote voting. That resolution also authorized the examination of ways to vote remotely in a secure manner; hence today's hearing.

As noted, I think the House is in a good position: there are indeed suitable secure voting technologies available.

The important reason why that is true is that House votes are NOT SECRET. Voting in the House is not based on secret ballots.

That makes all the difference, as manipulation or alteration of votes can be detected and corrected.

For the record, I note that in the US, SECRET ballot voting was first implemented in Massachusetts in 1888. However, implementing secure secret ballot remote voting is still beyond the state of the art.

Designing a secure voting system requires, first of all, a clear statement of the security objectives. A system can't be said to be secure if there is no specification of what security should mean for that system. What are the baseline voting security requirements? Here are four:

- (1) Only eligible voters can vote, at most once each.
- (2) Votes are cast as intended.
- (3) Votes are collected as cast.
- (4) Votes are counted as collected.

Each property should not only be true, but be VERIFIABLY true.

Counting (tabulation) is not an issue, since non-secret ballots can be posted publicly and the tally then verified by anyone.

One recommended principle for achieving voting system security is that of SOFTWARE INDEPENDENCE, a notion developed by John Wack and myself. This principle basically says that you never want to be in a position where you have to say, "Well, the result must be right, because the computer says so!"

In other words, the election outcomes must be AUDITABLE.

Here a sketch of a simple architectural approach for secure remote non-secret voting, to illustrate:

- there is a public web site where all cast votes are posted
- each congressperson composes his/her vote, digitally signs it, and sends the resulting digitally signed ballot for posting on the public web site.

Many digital signature schemes are available; NIST has developed digital signature standards. Digital signatures are now implemented in every browser. One approach uses the RSA public-key cryptosystem.

A nice thing about digital signatures is that the signature on a digitally signed document (such as a ballot) is verifiable by anyone.

Note that a digital signature is not just a cut-and-paste image of a handwritten signature; it is a mathematical function of the message being signed and secret information specific to the signer.

Digitally signed ballots can be authenticated using public information, both as to origin (who the voter is) and as to content (what the ballot says).

Vote manipulations are not possible, as forging digital signatures is not feasible.

The most an adversary can do is to delete or duplicate votes.

An adversary can conceivably delete or duplicate votes even now, with proxy voting. If a congressperson can't submit a ballot, they can't vote. Detection and correction mechanisms can work for voting with digitally signed ballots as for proxy voting.

It is important to note that voters (in this case congresspeople) can check, or audit, that their votes are correctly recorded on the public web site. Missing votes can be restored.

The approach sketched here bears many similarities to your current "proxy voting" procedures; the public web site becomes the "proxy" for those voting remotely. Indeed, such a system should provide a smooth and secure extension of your current proxy voting procedures, which need not be abandoned.

This sketch is intended only to show that it is possible to use technology to do remote non-secret voting in a secure manner; other approaches are possible.

This concludes my testimony; I would be happy to answer any questions you may have.

The CHAIRPERSON. Thank you very, very much.
I would now like to ask Dr. Rubin to give us his testimony.

STATEMENT OF AVIEL RUBIN

Mr. RUBIN. Thank you. Good afternoon, Chairperson Lofgren, Ranking Member Davis—or I should actually say, for some of you, it is good morning, right—and Members of the Committee. Thank you for inviting me to participate in today's hearing. My name is Avi Rubin, and I am a professor of computer science at Johns Hopkins University. I am also technical director of our Information Security Institute. I have held these positions for the last 17 years. And prior to that, I was a cybersecurity researcher for 9 years at AT&T Labs and Bellcore.

For 10 years my research focused on election security, and I was director of the National Science Foundation ACCURATE Center for secure elections. I was also an election judge in Maryland, and I worked six elections as an election judge.

I have been asked to comment on the technical feasibility of building a system for House Members to vote remotely. I will not be addressing the political question of whether the House should employ it, just focusing on technical issues relating to feasibility and security.

Remote voting for House Members is very different from remote internet voting where citizens elect their political leaders, which I strongly oppose for security reasons. What makes internet voting difficult is the secret ballot requirement. The House Members' votes are not anonymous, and that makes all of the difference.

I consider important features of a system for remote voting by House Members: The features are that the votes are cast over the internet on a mobile device or computer or even a dedicated device. The votes are displayed as they are cast on a virtual board simulating the large board in the House Chamber that shows the votes. The public has access to the virtual board and can see how Members voted. And the system needs to work in real time because some procedural votes lead to activity based on the results of those votes right away. So a system that detects errors days later would not be that useful.

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, the first step is to develop a threat model. Next, you want to rank the threats in order of severity, and then security designers will attempt to address those threats.

For House Members to vote remotely, here are examples of some of the threats. One would be an attacker compromising a Member's device, whether it is a phone or a tablet or computer, and forging votes on behalf of that Member.

Another threat might be that an attacker forges votes for a Member without even compromising their device. Let's look at another threat. An attacker could compromise a back-end system and cause the votes to be tabulated incorrectly. And, finally, a targeted denial-of-service attack, which was already mentioned, against a

Member's network right when they are trying to vote that prevents them from being able to vote.

Well, against the forged votes and the disruption of the tallies, we can address those with standard security practices. These can include encrypted and authenticated communication lines, multi-factor authentication, and checks.

For example, imagine that a staffer for a Member registers their mobile device with the system and then whenever the staffer votes—I am sorry—whenever the Member votes, that staffer receives a notification on their phone saying the Member has voted and here is how they voted, and that would be one check to make sure that the votes were being cast the way that the staffer knew that the Member could cast the votes. There are many other such safeguards that a designer of a system could put into place.

Now, addressing the denial-of-service attacks is more challenging, but this can be addressed with backup communication capabilities, including voice calls, and in the worst case, alarms can be raised. The key is that any security issues can be detected and addressed in a system such as this.

So, 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 security design 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.

So I am happy to answer any questions during the Q/A portion of the hearing, and thank you very much.

[The statement of Mr. Rubin follows:]

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.

The CHAIRPERSON. Thank you very much.
 Our last testimony will be from Dr. Wagner.
 We are eager to hear your comments.

STATEMENT OF DAVID WAGNER

Mr. WAGNER. Chairperson Lofgren, Ranking Member Davis, and Committee Members, thank you for the opportunity to participate in this hearing today. I am a professor of computer science at the University of California Berkeley. I have published more than 100 peer-reviewed scientific papers on computer security, and I have worked on the security of elections for over 15 years.

I have one message for you today: It is technologically feasible for the House to vote remotely if you decide that voting remotely is in the public interest. There are risks, but my assessment is that the technical risks can be mitigated.

If Members of the House can vote on bills over the internet, a natural concern is that hackers might attack your computers and try to tamper with the votes. Another concern is that technical issues might prevent Members from casting their vote or cause votes to be recorded inaccurately. These are serious risks, but I believe these risks can be addressed through a combination of people, process, and technology.

I would like to walk you through three possible models you could consider for remote voting. One way you could vote online would be for the House to develop its own app. You have heard how this could work. Each Member could cast their vote from an app on their phone with a public vote board showing the votes received in real time. I had suggested each Member have one of their staff crosscheck that the vote was recorded correctly. Maybe party whips could help with that too.

And I discuss in my written statement some security measures that I think would be appropriate for this approach. The primary disadvantage of developing your own app is that it might take many months or even years to develop and deploy your own solution.

A second option would be to buy a commercially available system for voting online. A third option would be to use remote videoconferencing. To record their vote, a Member could make a video call to the Office of the Clerk, and the Clerk's staff could verify the Member's face and voice and record their vote.

I outline in my written statement ways that you could harden this approach against hacking. The primary advantage of a videoconferencing approach is that it could be deployed rapidly using existing tools.

Regardless of which model you adopt, I would like to propose four principles that I think would support security for voting in the House. First, I suggest that you provide a way for Members to check that their votes were recorded correctly, and you encourage everyone to do this. This provides a powerful backstop in the event of technical problems.

If you make it easy for Members and their staff to verify that their vote was recorded correctly, then any technical issues or hacking can be detected and corrected. Any system can potentially

be hacked, but well-designed ones anticipate this and provide a way to detect it and correct the problem.

Second, I think it will be important to consider the policies and processes that govern remote voting. You might consider how Members can report any discrepancies in how their vote was recorded and have them corrected. You might also consider what fallback procedures would be available if the Member is unable to vote due to technical issues and the timeline for doing so.

Third, you might consider selecting a partner with cybersecurity expertise. When you buy a house, you hire a professional inspector to check for any problems. And the same applies here. It might be helpful to have security experts on tap to help, and there are a number of government organizations that might be available to help with that.

Fourth, I suggest following good cybersecurity practices, such as use of two-factor authentication, end-to-end encryption, and providing Members with hardened devices to vote from.

In summary, I believe technology can enable the House to vote remotely in a reasonably safe way if you decide that it would be appropriate to do so. Thank you.

[The statement of Mr. Wagner follows:]

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. Berkeley¹. 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 technology¹: 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 contested².

¹I 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 problems³. 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 a 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 needed⁴.

There are other issues that may warrant attention⁵. 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

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

²Andrew Appel, “Can Legislatures Safely Vote by Internet?”, Freedom to Tinker, April 10, 2020.

³Scott 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.

The CHAIRPERSON. Thank you very much, Dr. Wagner.

And thanks to all of the witnesses for their very informative testimony.

We now have an opportunity to ask questions of our witnesses for five minutes. I would note that Mr. Gingrich has previously advised us that he has a hard stop in about 25 minutes. So I just wanted members to know that if they have questions for Mr. Gingrich.

Mr. GINGRICH. Well, actually, Chairperson, this is so interesting; I will stay. I will just blow off my—

The CHAIRPERSON. Okay. Good. Very good. Very good.

Mr. GINGRICH. Thank you.

The CHAIRPERSON. I am going to turn to the Ranking Member first to recognize him for his five minutes of questions. Mr. Davis.

Mr. DAVIS of Illinois. Thank you, Madam Chairperson.

And thank you to all the witnesses. I appreciate the opportunity to talk about technology and talk about the overall process of remote voting possibly existing in the House.

Mr. Speaker, you touched on this in your testimony, but can you elaborate further on how you see remote voting as possibly centralizing power in the Speaker's Office?

Mr. GINGRICH. I will be glad to. And let me say, I was very impressed with the witnesses, and I have no doubt that if the House decides it is wise, that you can develop a very solid system. And I concur with the Clerk, Cheryl Johnson, that she could easily, I think, develop and guarantee the integrity of that kind of a system. So I think that is an important frame of this.

The challenge you have is basically how humans operate. As you know, you build teams by being together long enough to know each other. You build teams by working out and solving problems together.

I think you have to look at, not just the first week or the first month, but if you start down a road where you are saying that being distant, not interacting biologically in the same room, is an acceptable pattern, then I think you begin to set up a post-legislative body that is something we have never seen before.

Legislative bodies historically aren't just about voting; they are about building a collective understanding and a collective knowledge, and, at times, in taking on Presidents or taking on kings, they are about people who know each other well enough to have courage in situations of enormous danger.

So, as a historian, I worry about the wisdom half of this. As a citizen, I have no doubt, if you decide it is the way to go, you have brilliant people today who are testifying, and collectively, they could produce a—they can guarantee the technology, but I am not sure they can guarantee the historical and sociological side effects.

Mr. DAVIS of Illinois. Mr. Speaker, I agree with you. We are the United States of America. If there is anything that needs to be built in this globe, we can make sure that happens, and the great people who are here today likely could do that. But I agree with you. I still believe it impacts what Congress looks like over the next generation.

Matter of fact, I am on the Committee to Modernize Congress, Select Committee to Modernize Congress. Many of our rec-

ommendations have been built around how we ought to get together more, talk more. That is how we begin to legislate.

But another important process is oversight. Now, you changed the oversight process within the House when you got rid of proxy voting that the committee chairs had before you were Speaker. Did that empower more Member input, and what kind of oversight issues do you think remote voting would give to a legislative branch when dealing with the executive branch?

Mr. GINGRICH. Look, I think oversight is unbelievably important. I don't think we do enough of it, and I don't think we develop enough expertise in it. And, again, I would just say, a lot of these topics, whether it is healthcare or national security or you name it, they require years of learning. Members who spend years working on a particular area very often know more than the executive branch people that they are interrogating.

So I think it is very important. We eliminated proxy voting because what was happening was the chairman would walk in and they would have 15 votes in their pocket. Now, those people didn't sit through the hearing. They didn't ask any questions. Well, when the time came to vote, even if you had had all your people there on some of these committees where they were stacked pretty intensely, the chairman just won. There was almost no reason to go. So that was a big factor in why we went there.

I think our hope was that it would get more Member involvement, more Member engagement, and more Member learning. And as a result, all 435 players could be involved, not just a handful. That was our hope anyway.

Mr. DAVIS of Illinois. We appreciate you doing that. I do believe it has made the House work better. We do, as I know the Members of this Committee have tremendous input. And I also want to thank you for the transformation that you made to the House when you took over as Speaker to move the House from a patronage machine of decades before to a more professional organization with our Chief Administrative Officer and making sure that politics was put out of that process as much as possible in a political House that we work in.

So I appreciate your experience, appreciate your comments. And I will go ahead and yield back, and thanks for taking the time today.

The CHAIRPERSON. The gentleman yields back.

I would now turn to the other Davis on our Committee, the gentlelady from California, Susan Davis, for five minutes.

Mrs. DAVIS of California. Thank you very much, Madam Chair. I appreciate all of our witnesses here today.

And I wanted to start with Clerk Johnson, if I might.

And, Clerk Johnson, I especially wanted to thank you for everything that you and your staff have been doing to make voting and legislative processes possible during this difficult time of the pandemic.

And we need to remember: we are in a national emergency here. We are not just talking about this because we think that, you know, maybe some people would like to do it this way. There is a reason for that, and it is a matter of life and death. And for some

of our families, quite honestly, it is a matter of life and death. So being safe is very, very important.

I wanted to just acknowledge your effort, Clerk Johnson, to make Congress work remotely requires remote voting, of course, that we have been talking about, but also remote legislative processes, including bill introduction and co-sponsorship. And I know that you have worked hard on that, creating electronic signatures.

I want to thank you as well for setting up the email system for bills and sponsorships, and I hope we could continue to work together on that. And you have also been active in setting up some of the small group voting and proxy voting that is also smart and safe for all of us.

I am sure you know and probably the one issue that Members would talk about that is a concern of theirs, especially when they are there and voting right now, again, because of COVID, is being able to vote quickly, get on and off the floor, and perhaps find ways of saving time in between. And I wonder whether you think that there are some more efficient ways of doing that? I want to turn to the Clerk for that.

The CHAIRPERSON. The Clerk needs to unmute her microphone before she answers.

Ms. JOHNSON. Yes.

Mrs. DAVIS of California. Thank you.

Ms. JOHNSON. In looking at the process that is currently in place, I certainly think it is very efficient with the proxy voting. Members are able to come in, and if they are holding proxies for other Members, they announce those proxies on the floor.

At the same time, the tally clerk holds a binder that has a copy of the proxies to make certain that it is reliable and transparent, and Members are able to move on and off of the floor very, very efficiently.

A vote normally takes about 45 minutes, because they are sequential. Members come in probably 15 at a time. They exercise social distancing. And, as I said, we have not had any incidents to date.

Mrs. DAVIS of California. If I may just add quickly, I think the timing in between the votes, and for some of us walking back and forth to offices, it is great. We get more steps in, I guess you could say that.

But I also just wanted to see that if there are some ways that people have suggested shortening some of the time, and maybe that is something that we could all continue to talk about.

But I know that that is the concern that people have expressed, because it kind of forces people to hang out a little bit, and that is not something that we know is necessarily in the best interest of all of us doing that and keeping people safe.

I wanted to turn quickly, because several of our witnesses have talked about this, and I think it is really an interesting concept. How could remote voting be corrupted given that it is not a secret ballot?

And I know that Dr. Rubin has talked about that, Dr. Rivest as well.

Are we talking about corruption here? Or is it that we want to be sure that Members have the ability very, very quickly to be able to check and see if their votes are correct?

It is not a secret system. So the whole world should be able to watch this with us and to be sure that we are correct.

And I ask others on the panel to respond to that.

Dr. Rivest.

Mr. CROWELL. Well, I would just—

Mr. RIVEST. I would be happy to speak to that.

Sure, yes, you are absolutely right, you hit the nail on the head with the key requirement, which is that the voters need to be—the Congress people who are voting need to be able to check that their ballot is correctly reported and posted.

There may be corruption on the way between inside the voter's mobile device and their laptop, whatever they are using. There may be corruption on the routes to the posting. But any of those things can be detected and corrected as long as there is a way for the voter to check that the vote was received as intended and posted correctly.

So I think that is exactly right, there are possibilities for corruption, but as long as you have a detection and correction mechanism, such as you have talked about here, such as we have all talked about, this can work well.

Mrs. DAVIS of California. Thank you.

The CHAIRPERSON. Mr. Crowell, you were going to say something.

Mr. CROWELL. Yeah. I wanted to add to that list disruption, which I think is a very big issue and will have to be addressed, as Dr. Rivest and Dr. Rubin mentioned earlier. Disruption is occurring all the time in the internet, and we have to deal with it.

The CHAIRPERSON. Very good. Thank you so much.

I would now like to turn to the gentleman from North Carolina, Mr. Walker, for his questions.

Mr. WALKER. Thank you, Madam Chair.

Speaker Gingrich, you touched on how working together and hearing different perspectives will be greatly diminished with Members not physically being in D.C.

I know some of my personal work has been bipartisan. Some of those relationships and some of the development on policies, those conversations happen on the House floor.

I can think of two instances during a motion to recommit where colleagues of mine did change their votes going on to the floor after hearing the debate. In fact, there is a verse in Proverbs in the original Hebrew that states: The one who states his case first seems right until the other comes along and examines him.

I don't look at this as a technological debate. I look at this as a procedural debate, a historical debate, a debate of what is best for the American people.

Would you mind expanding on how this remote voting will have a potential corrosive impact on the legislative process?

Mr. GINGRICH. Well, thank you for that question, Congressman Walker.

Look, I approach this from two different perspectives. One is, somebody who did serve 20 years in the House. And, for example,

when I was Speaker most of our major bills had huge bipartisan majorities and they did so because we listened to each other.

And on occasion we got into fights. We had one effort, to reform welfare, that got vetoed. We had to sit back down, talk it through. By the time we were done, literally half the Democrats voted with us. It was 101–101 in the caucus. And that wouldn't have happened if we weren't able to listen to each other.

I can also tell you that I am a big fan of congressional delegation trips, because you get away from your staff, you get away from your constituents, you get away from lobbyists. You are with the other Members for 3, 4, 5, 6 days, learning together, experiencing together, talking together.

So one is my own personal experience biologically having done it.

The other is my experience as a historian, that when you study all of these great demands that involve freedom, if you look at the proceedings leading up to the English civil war, where the Parliament organized itself against King Charles I, if you look at the rebellion against Cromwell, who had become a dictator at the end of that civil war, if you look at why the Founding Fathers—remember, all these Founding Fathers were professional politicians. They had all served in legislatures. They were colonial legislatures, but they were real, and they had all negotiated.

And so they believed that the legislative branch was so important that they made it the number one thing in the Constitution. But in their experience, the legislative branch, for example, for Washington and others, meant you rode down to Williamsburg. You were there for 6 or 8 weeks. You stayed together, you ate together, you talked together.

Constitutional Convention, 55 days without a break, all of it in secret. Talking together, worrying, negotiating, thinking. Finally, at one point having a day of prayer, because they had gotten deadlocked.

I think humans learn from each other, and when you start trying to replace humans with a mechanical interface or an electronic interface you rapidly degrade the long-term wisdom of the collective group.

Mr. WALKER. I certainly agree. All over the country right now we are trying to bring people together. In a couple of weeks, we will have 200 pastors coming together from all of our communities to begin conversations to talk about how we resolve issues. It would be impossible to do that remotely.

There is also another aspect of this. What kind of message does this send to the American people when Members of Congress can just stay at home and push a button or call in or video conference while our other essential workers are still showing up? My wife is a trauma one nurse specialist practitioner. She has to show up every day.

Would you address that as well?

Mr. GINGRICH. I am deeply concerned by the level of panic that the American news media has created. I don't see it here in Europe. I don't see it anywhere else around the world. And I think that it is almost entirely media driven.

Yes, this is a problem, but we have dealt with a lot of other health problems before and I think that we can deal with this one.

And I think, as a populist, as somebody whose father served 27 years in the Army, came out with no money, look, I find the idea of the political class being too precious to take the risk of getting together, I find that goes against everything in the American system. And I find it deeply offensive to think that the politicians think that they are more valuable than a truck driver or a worker at In-N-Out in Los Angeles.

Mr. WALKER. Thank you. Right on time, five minutes. Thank you, Mr. Speaker. It is a pleasure to see you today.

I yield back.

The CHAIRPERSON. At this point I would like to recognize the other gentleman from North Carolina, Mr. Butterfield, for his questions.

Mr. BUTTERFIELD. Thank you very much, Madam Chair.

And it is good to see all of my colleagues today. I hope and pray that all of you are well.

Let me also thank our witnesses for your testimony.

I have been listening very carefully, Madam Chair, to the various witnesses today, and I was really struck when Mr. Gingrich suggested that we are acting in a sense of panic that the news media has created. And I want to respectfully dispute that premise.

I suggest today that Democrats are engaged in what I would like to call strategic planning. That is to protect this institution if rates of infection continue to increase.

Protecting the Members if assembling on the floor is infectious, that is our goal. It is not to create any panic. It is simply to protect the Members if assembling on the House floor becomes infectious.

I will note that there was a press conference last week in front of the Capitol and one of our beloved Members from Virginia contracted the coronavirus while right here on the Capitol Grounds.

And so we are just trying to be proactive and to look forward and to do some strategic planning.

I was in a meeting the other day, a virtual meeting, with two of the leading epidemiologists in the world, and what those two gentlemen told us was that COVID is winning—COVID is winning.

If States don't require extraordinary measures, the infection rates could reach as much as 50 percent by the end of the year.

I hope my colleagues are not surprised by that. I hope you agree with that assessment. But if the rates of infection continue on the same course that we are seeing now, it could rise to 50 percent this year.

And so as my colleague, Susan Davis, said a moment ago, this is a national emergency and it could be a matter of life and death.

Let me just turn my first question to the clerk.

And thank you, Ms. Johnson, for your incredible work in all that you do for all of us in the House.

At any given time under normal circumstances, Ms. Johnson, how many people are on the floor? And that would be Members and Members' staff and the support personnel, including the Capitol Police and the sergeant at arms and the personnel from your office. Collectively, how many people under normal conditions are on the floor?

Ms. JOHNSON. Approximately 20 persons, and that is clerk staff, as well as staff of the parliamentary and Speaker's leadership

staff as well, both Democrat and Republican. But with the Clerk's Office, we have the bill clerk, the reading clerk——

Mr. BUTTERFIELD. But put it all together, including the Members, including the Capitol Police, in the aggregate, how many people, 500 perhaps?

Ms. JOHNSON. Oh, if we include everyone on the floor at one time, it is well over 500. It is probably more like 550.

Mr. BUTTERFIELD. And so while I think it is wonderful to have 500 people on the floor so that we can talk with each other and plan our votes in the middle of a motion to recommit and all of that, I think we have to look at extraordinary circumstances.

We do not need 500 people on the floor at one time. We don't need 50 people on the floor at one time. And so thank you for that.

It occurs to me that one of the most straightforward ways to vote remotely might be to do it by video conference in which the Member would simply tell a vote clerk how they wish to vote.

I know our friends over in the other body, they vote by a roll call, but it is an in-person roll call. And I am thinking perhaps about an electronic teleconference roll call.

Would that be practical?

Ms. JOHNSON. It would be technically feasible. We would just have to make certain that it is reliable. But it certainly would be practical.

Mr. BUTTERFIELD. And finally, in a remote voting scenario, do you think it would be beneficial to have votes to be public the moment the votes are cast?

And as we all know, the public does not know how we vote instantaneously. The Members know because we can look up at the board, but the public does not know for a few minutes until your office is able to post it on the internet.

But do you have a system in mind whereby the public would immediately know how a Member of Congress voted on legislation?

Ms. JOHNSON. I think that involves variables. I don't have a system in mind, but we could probably have such a system. But, no, I don't have one in mind.

Mr. BUTTERFIELD. But that would be beneficial, I take it, if the public could instantly know how a Member voted?

Ms. JOHNSON. Transparency is always beneficial, I agree.

Mr. BUTTERFIELD. Thank you, Ms. Johnson.

Thank you, Madam Chairman.

The CHAIRPERSON. Thank you very much.

I would now like to turn to the gentleman from Georgia, Mr. Loudermilk, for his questions.

Mr. LOUDERMILK. Thank you, Madam Chair. Appreciate it.

I apologize for my voice. Believe it or not, there are other sicknesses other than COVID out there. And I came down with the good old common cold this week and I totally lost my voice yesterday.

The CHAIRPERSON. I am sorry.

Mr. LOUDERMILK. But it is coming back. It isn't COVID because of a flight I took on Air Force One a few days ago. I was tested.

And so I know that that kind of plays into, I think, what Speaker Gingrich was talking about, it is almost like today if anybody gets

a cold, they are all of a sudden just scared to death that they have COVID. And so we have to keep things in perspective.

I think the question that we should be asking here today, and several of our witnesses have alluded to this, the question isn't whether or not this could technically be done, it is whether we should be doing this.

And I think one key indicator to whether we should be doing this or not is the amount of time that we have talked about security on here today. That ought to be the first indicator, that ought to raise a red flag.

I spent 30 years in the technology sector and one of the things I can tell you, there is an old adage that basically said, the question isn't if you are going to be hacked, but it is when.

And I know that we can build systems that will be secure enough to do this, but also those systems are only as good as you maintain them continually. And it would create an inordinate amount of work to continue to maintain these, because as some of our esteemed panelists have said today, they have talked about how high profile this would be, what a target we would be, the risk that we would have.

And obviously we would be one of the highest profile targets, not only to cyber criminals, but to foreign entities as well. And the amount of effort that we would spend in just continuing to stay ahead of the bad guys, I don't know that it would be worth implementing a system like this.

I think we really should be talking about ways to hold ourselves accountable to do the jobs we are supposed to be doing. I can't remember, I am sure Speaker Gingrich can tell us, when was the last time that the House and the Senate actually passed appropriations by our own deadline?

I mean, I think we should spend time on how we hold ourselves to do our jobs, not trying to make it easier for us not to do our jobs.

But I think it is important to have the conversation. But the most secure way to vote is to walk on the floor with your card.

And I give credit to the system that we have right now. It does take longer. It isn't as efficient, because we can't go on the floor and vote on four votes at one time. It takes half a day or a quarter of a day to vote on one bill because the machines are closed. But yet we have got it down to where we can do that.

So anyhow, I think the real question ought to be, is this something we should be considering, not if it could be done?

Speaker Gingrich, good to see you, again. And it took me a moment when you said you are in Rome, I had to figure out, were you talking about Rome, Georgia, or Rome, Italy? So I think I figured that out.

But you did a lot to reform House processes. I have read several books on it. When you became Speaker it was like reforming the entire House because of the level of corruption that existed at several levels—and including at the time the House Administration Committee.

And one of the things that has been spoken about is that you got rid of proxy voting. Why did you get rid of that in the committee level and what were the problems it created?

Mr. GINGRICH. Well, let me say first, just for a second, that in terms of what Clerk Johnson is dealing with, we actually brought in a firm to audit the House. And after about 9 months they came back and briefed us and said, "It is impossible. Since 1789 the House has never kept records accurate enough to be audited." But they said, "If you will give us a contract, a year from now we will be able to audit the House." And that was one of the breakthrough moments that led to a much more modern House.

And the corruption wasn't particularly partisan. It was just people had gotten sloppy over a very, very long period.

I would say, and I draw a distinction here, as I said earlier, I have no doubt with the experts you have heard from today that you can get to a safe and secure method for remote voting.

The proxy voting issue is a different issue and one which does concern me, and that is it centralizes power and actually lowers the interest of other Members in participating because they are just going to lose the vote. And the chairman of the committee or the Speaker of the House or whoever is just going to beat them with the names of people who aren't even there, have no idea how it has been voted.

And so for us that was a very frustrating part of being in the minority and that is why we changed it when we took over. We actually took away from our brand-new chairmen the power that their predecessors had and would not let our new chairmen use the proxies to dominate their committees.

Mr. LOUDERMILK. Thank you, Mr. Speaker.

I mean, there are times that it would be beneficial when I have three committee hearings going on at the same time or markups and I have to run from one to the other, but that is just part of what I signed up to do.

So thank you. I see I am out of time. And I yield back.

The CHAIRPERSON. Thank you.

Mr. Raskin has been able to join us from the Rules Committee. We thank you.

The gentleman from Maryland is recognized for his five minutes.

Mr. RASKIN. Madam Chair, thank you very much. And thanks for calling this extremely important meeting at a time when the country is in an intensifying crisis with the coronavirus. We have 3.3 million cases. We lead the world in case count. We lead the world in death count. We have tens of millions of people thrown out of work because of this nightmare. And several of our States would be in the top five countries in the world in terms of increases in the coronavirus if they were treated as a country.

And we know that there are hospitals being maxed out and overrun in Florida, in Texas, in Arizona, and throughout a lot of the southern part of our country.

I would not agree with the proposition that using remote voting or proxy voting in the context of a national public health crisis reduces deliberation. I would think that people can engage in robotic, cultish, party-line voting even when they are standing on the floor of the House. And I have seen many, many people do that.

And I think people, at the same time, could call in a proxy vote or vote remotely, having listened carefully to the speeches on TV and having consulted with their colleagues.

So I just think that that argument has very little force to it. There might be other things we can do to promote meaningful dialogue and discussion. But I understand the same kinds of arguments were made when the House of Representatives first moved to use electronic voting in the first place, that somehow this would sterilize the process and cut down on interpersonal communication and so on.

So I am more concerned about the arguments that I have heard from several people today, phrased rhetorically: What kind of message does it send to Americans on the front lines, like nurses and doctors and first responders who go to work, if there are Members of the House who can't make it and they vote from home?

Does it say something, as Mr. Gingrich said—and I am sorry I never had the chance to serve in Congress with Congressman Gingrich because he is an interesting guy—but does it say something about the preciousness of the political class?

Well, I don't think so. If anyone wants to really prove his manhood in this process or prove your courage or your tenacity, go spend a day in a hospital with the nurses and the doctors and the frontline providers. And if you can't do that or you don't want to do that, listen to them, because they are all telling us the same thing: Stay home. Because the hospitals are being overrun and the pandemic is out of control. And we have people like the President who are not wearing masks and we have people who are undermining the public health advice of our doctors and our scientists and Dr. Fauci. Stay home if you can stay home because this virus is still out of control.

Now, the House of Representatives, as I think I heard the Clerk testify, when we are operating and there is a vote going on, can have anywhere between 400, 500, 550 people together on the floor.

My friends, conferences across the country have been canceled during this period because they have 500 people coming together at hotels. And that is how the virus has spread in a number of cases, one infamously in Boston at a conference where it just spread like wildfire.

We basically think we are a regular meeting conference in that sense when you look at it from an epidemiological perspective.

So nobody wants to be in this position, and this is not the occasion to discuss the incompetence of the national government's response to this crisis. Nobody wants to be in this situation, but we do have a responsibility to maintain continuity of government and the continuity of Congress and to make sure that we are acting consistent with public health protocols in a safe and in a secure way.

And so I very much favor the idea of moving forward.

You know, Madam Chair, if you would permit me one more thought. There were people saying, well, this isn't fair to our constituents, when we were talking about proxy voting.

Proxy voting has allowed lots of Members who were sick, and we have had a number of Members, both Republicans and Democrats, suffer from the coronavirus. We have enabled people to participate. We have enabled them to participate if they have immunocompromised or vulnerable family members, or other people who couldn't go because of travel logistics and couldn't make it

to Washington. Their constituents had a voice. And I know because the Republicans are suing about this.

A lot of Republicans didn't participate. I think in the last vote, there were nine or ten Republicans who didn't participate. What does it say to their constituents that they would prefer to make some kind of vain moral gesture by not voting and not having their own constituents represented than to participate in a system which allows everyone to be heard?

I yield back. Thank you.

The CHAIRPERSON. The gentleman yields back.

I would now like to turn to the gentlelady from Ohio, Ms. Fudge, for her five minutes of questioning.

Is Marcia still with us? Perhaps not.

Then we will go to Mr. Aguilar.

Mr. AGUILAR. Thank you, Madam Chair.

And appreciate the panel and the panelists for being here.

Just off of what Mr. Raskin mentioned, too, one of the other roles I play is chief deputy whip of our caucus. And I have a number of conversations with colleagues about it, just like you, Madam Chair.

And no colleague is in the same position. Some colleagues live with someone who has autoimmune issues. Some live with in-laws or spend time with family members who have compromised systems. We all have to make decisions based on our own personal health and circumstances.

This isn't anything that has to do with how the press is portraying it. This has to do about public health. This has to do about the real risks that exist by Members getting on planes and coming from all points in the country.

We don't all live in Washington, D.C. I know maybe in another time that was more prevalent. That has been weaponized by politics in the past.

And so many of us, and I among them, I have been to every vote that we have made here in the pandemic. I will board a plane and come five hours each way doing that and having a commute that is over 8 hours each way. And there is no problem with that, that is what I signed up for, as my colleague from Georgia mentioned.

But let's not minimize the fact that every Member is going to make the decisions that is best for them.

And I would like to just bring it back briefly to the topic of the hearing isn't about our hopes and fears, isn't about the press. It is about exploring the feasibility and security of the technology that is at hand.

And so I would like to ask Mr. Green, is there a technology in existence in the commercial market space that could be useful to the House in creating a secure infrastructure to implement remote voting?

Mr. GREEN. I don't want to self-promote too much, but of course my own company produces something like that that is used widely for secure access, and that is just—that is a piece of an overall solution. That is not a complete solution.

So we focus on the network, and there are other tech companies that focus on secure network connectivity as well. On top of that, you can layer very standard types of technologies, whether that is

browser-based applications. A voting application could be as simple as a web server and a browser running on a mobile device.

So it doesn't have to be a complex thing given that the other protections that we have talked about and the other panelists have talked about today are in place, notably some live verification that a correct vote was received. That is really the key to the entire thing.

So I think we can solve the network problem. We can solve the application problem. The other processes that go around it, that is the more complicated part.

Mr. AGUILAR. If you were responsible for a secure voting system, what would concern you most? What would keep you up at night about devising a system that can work?

Mr. GREEN. As I indicated at the end of my testimony, I would be most concerned about the availability, the fact that you may have Members with poor internet connections or no internet connections or unreliable internet connections. You may have adversaries that specifically target those Members. If they know what the vote is going to be and you can prevent those specific Members from voting, you may potentially be able to throw the vote in a direction or another.

So, again, backup systems are really critical, and there are different ways to engineer those that I think involve humans rather than necessarily involving technology that can end up making things safe.

Mr. AGUILAR. I appreciate it.

Professor Rubin, different legislatures in statehouses across the country and across the world have taken different approaches on this, as you highlighted. Some require legislators' emails and signed and scanned ballots. Others have created apps.

When you think of the possibility of the House having a vote-remote system, is there a particular system or framework that comes to mind that is something you would counsel us to consider?

Mr. RUBIN. I think that if we had to recommend a particular system, the first step would be to gather the experts together and brainstorm that. And I think Dr. Wagner presented some very compelling ideas. For example, the recorded—pre-recorded video of the vote, as well as what has been discussed, such as a web server and an app.

I think the key underlying all of these is the ability to look in real-time and decide if there has been a problem and identify it right away.

And I think as to the availability question, for example, the first thing you could do if you are voting on a phone and there has been a denial of service attack, perhaps switch from your Wi-Fi to your cellular provider and see if that works.

If that doesn't work, then the next step would be to alert somebody and to have a mechanism in place in advance that would make it easy to alert someone, saying, "I am trying to vote and my vote has not been successful," and then have a procedure for getting that vote in some other way.

Mr. AGUILAR. I appreciate it.

Thank you, Madam Chair. I yield back.

The CHAIRPERSON. Thank you.

So I would like to recognize myself for a few questions.

Mr. Crowell, Members of the House are all over the board in terms of their familiarity with technology. Are there secure methods to remote voting that you think would be more user-friendly than others?

Mr. CROWELL. Well, certainly. And, in fact, I would agree with what Avi Rubin said, that a purpose-made application running on a browser or running in an operating system would be the most complete approach and would make it easier for the Members to vote no matter what device they were using to vote on, because these are commonly available on all of the devices.

Purpose-built because you want the voting to be very, very easy, a “yes” or a “yea” or a “nay” button for the vote itself, clear identification of what the matter is in front of you so that there is no ambiguity about what you are voting on, and the ability to record all of these things not only in real-time, but for posterity since these become public records.

The CHAIRPERSON. Right.

Mr. CROWELL. All of that has to be done securely and it can be in a purpose-built system as opposed to trying to patch together various apps that were never intended to support voting.

The CHAIRPERSON. Mr. Green, I wonder if you have thoughts on how votes that were cast remotely could be integrated with the votes cast in the Chamber from a technological standpoint given that the system we have is air gapped with one-way data flow?

Mr. GREEN. Yeah, I think integrating those systems would be ideal so that you don’t have a 100 percent remote or a 100 percent in-person type of voting operation.

Ultimately, it seems like you are going to need somebody to sit there and push the right button or somehow feed those systems in, probably that somebody sitting on site in the House Chamber or at least in the building there.

And, again, as long as the Member voting remotely can see that and see the result of that, that can be done fairly safely.

The CHAIRPERSON. Dr. Rivest, in your testimony you mentioned that the most an adversary would be able to do in a particular system would be to delete or duplicate votes. Can you explain what sort of measures could be taken to protect against deletion or duplication of votes?

Mr. RIVEST. Thanks. Great question.

I think some innovation in the procedural aspects of voting in the House might help a lot. One thing that occurs to me here, hearing the discussion, would be to be able to file a default vote ahead of time so that you can say, “Should my internet go down, should I be unable to communicate, this is how I would intend to vote on this bill,” but then after hearing the debate, as Speaker Gingrich suggests, you change your mind or you have other influences that cause you to rethink the vote, you could file, either remotely or in-person, a new vote that would override the default.

So something like that could be one way of mitigating the risk of having unavailability, which is a risk that is pretty unique to remote voting compared to in-person voting.

The CHAIRPERSON. Right.

Dr. Rubin, it is important that we authenticate—we have all talked about that—that the vote being cast is being cast by the Member herself.

Do you think we should consider, if we move to this, any kind of tech system, a biometric authentication as part of a multifactor authentication system? And if so, would that be an iris scan?

Mr. RUBIN. So biometrics are very powerful and if designed correctly they can provide a useful factor. I am a big fan of multifactor authentication, so I think that if there were a way to integrate an iris scan such as what you get when you unlock an iPhone today—well, that is face recognition, it is not an iris scan—but something, some biometric to that effect, if you could initialize the system in advance with what a person's face is like and then integrate that into the authentication at the time, that that would be beneficial.

But I also think that we can achieve authentication without that. So it is just one of the tools in the arsenal that we have that can help us when we design a system.

The CHAIRPERSON. Dr. Wagner, would technology that uses a lot of bandwidth make denial of service attacks more likely? Would it be better to utilize technology with low bandwidth and more fault tolerance?

Mr. WAGNER. Thank you.

I don't think that should be your primary consideration. What I would recommend is the primary way to mitigate denial of service concerns is to have a fallback method. We don't have effective technological ways to absolutely prevent denial of service attacks. So the primary defense is to have some other alternate channel that can be used in the event of a problem.

The CHAIRPERSON. Let me ask you this. Should we be concerned about man-in-the-middle attacks? And if so, what would be the best way to secure a system against that type of attack?

Mr. WAGNER. Certainly. Man-in-the-middle attacks could arise if casting votes over the internet or over a telephony system where attacks are possible. And there are industry standard defenses that would be effective at preventing man-in-the-middle attacks. For instance, many of us have referenced end-to-end encryption, which is an effective defense.

So I think using industry standard mechanisms would be a reasonable way to defend against those attacks.

The CHAIRPERSON. Thank you.

I see my time is expired, so I want to thank all of the witnesses for this enormously valuable testimony.

I would note that House Resolution 965 requires this committee "to study the feasibility of using technology to conduct remote voting in the House."

So that is what we are about. We have different views on whether we should or shouldn't. But our task is to examine the technology and to be able to certify to the House if we are able to determine that an operable and secure technology exists to conduct remote voting in the House.

The testimony received today is enormously helpful in helping us to complete the task that has been assigned to us. And I would like to note for the witnesses that the Members may have additional questions for you. And if we do, we would ask that you respond to

those questions in writing and the hearing record will be open for those responses.

You know, this is an important question for all of us. Nothing is perfect. And I was listening to Members. I have missed votes, not because of a denial of service attack, but because United Airlines took off late and I didn't make it in time to go to the House floor.

I agree, Mr. Gingrich, there is really nothing to substitute for Members going on a codel together and getting to know each other, but that is not happening now because we are following the advice of the attending physician.

And I love being on the floor when the mix of Members, everybody is running around and talking to each other and getting letters signed, but that is not happening either because the attending physician is saying we have to go in groups of 20 and then leave.

The votes are taking a very long time because of the need for social distancing. So in this pandemic our situation has changed.

We look forward to the time when the conflagration of this pandemic has abated. I envy you there in Rome where you are not actually with the kind of wildfire that is eating through America with this—not just America, but my own State of California, where thousands and thousands of positives are logging in every day. It is really a very serious matter.

Mr. GINGRICH. If I might, Madam Chairperson, I just want to say, I think for the purpose you were assigned, to ascertain whether or not it is technically doable, this was a superb hearing. It makes me proud to, once again, be briefly part of House Administration. I think you had terrific guests, and I think they all did a very fine job of outlining the technical possibilities. So thank you for allowing me to be part of that.

The CHAIRPERSON. Well, thank you for that. From a former Speaker, that is great praise indeed and we appreciate it.

With that, I want to thank all the Members for their participation. I ask unanimous consent to put into the record a letter received from Demand Progress and keep the record open for other material that Members may wish to add to the record.

[The information follows:]

HEARING
COMMITTEE ON HOUSE ADMINISTRATION
“EXPLORING THE FEASIBILITY AND SECURITY OF TECHNOLOGY TO CONDUCT REMOTE
VOTING IN THE HOUSE”
JULY 17, 2020
MAJORITY QUESTIONS FOR THE RECORD
FOR
THE HONORABLE CHERYL L. JOHNSON
CLERK OF THE U. S. HOUSE OF REPRESENTATIVES

1. From your perspective, what specific elements or capabilities would important in a potential remote voting system?

Preserving and protecting the integrity of the legislative process must be the primary goal of any potential remote voting system considered for the House. The key to preserving the integrity of the process and the data is security at all layers of the system. As some of the panel experts pointed out, the foundation of any secure system is confidentiality, integrity and availability. These principles would have to apply to the devices Members use, the networks they communicate over, and the systems that process the data.

Secure devices are required to ensure that the interface to the system cannot be tampered with and Members can be reliably authenticated to maintain the confidentiality of their actions. The devices and networks must be secured to preserve the integrity of Member voting actions and the feedback they receive, and the recording of votes in the remote system. Availability is crucial to ensure that Members can access the devices, networks and systems when a roll is called and reliably review their votes. Fortunately, as also noted by some panelists, commercial solutions that meet many of these requirements are available.

Of the core principles, maintaining availability of the system while a roll call is in progress, especially preserving availability of the network, is the most sensitive and difficult of these requirements. As shared by some of the panelists with technical expertise, the very nature of each Member's vote as public data makes it feasible to design a system with audit trails that enable real-time checks and remediation capabilities. The Member, Member's staff, and the public will know how the vote was cast and any discrepancy can be addressed by following carefully designed rules and processes.

In addition, we believe that any potential remote voting system must be seamlessly integrated with the existing Electronic Voting System (EVS) currently in use by the House. If the House elects to enable remote voting we anticipate that remote voting

will be conducted in conjunction with the on-the-Floor voting, which means the current EVS must run synchronously with a remote voting system. Furthermore, functionality of a remote voting client (what a Member would use remotely) should mirror that of the vote station on the House Floor.

We understand that placing a mission critical system such as the one discussed here into a modern wide area networked environment, an environment with implied presence of threat, is a complex and challenging undertaking with clear risks. However, there are models for such systems and a body of knowledge for operating such sensitive and critical systems. The Clerk's Office remains ready to further examine and if called upon to develop and support remote voting capabilities for the House.

2. Did you learn any specific lessons from the implementation of the proxy voting procedures established by H. Res. 965 that could be applied to potential voting procedure changes in the future?

The implementation of proxy voting procedures pursuant to H. Res. 965 provided numerous lessons that could lead to more efficiency, greater transparency, and a smoother transition for any possible future changes in voting procedures. First and foremost, the Office of the Clerk was grateful to receive thorough guidance from the Rules Committee regarding this process at the outset. Additionally, the Office of the Clerk and its subject matter experts, particularly in Legislative Operations and Legislative Computer Systems, were appreciative of the opportunity to provide feedback and offer suggestions prior to the implementation of proxy voting procedures in the House, with the concurrence of the Office of the Parliamentarian. For future endeavors, we suggest two possible improvements that would assist both Clerk and other staff:

1. The guidelines surrounding voting procedures may be creating inefficiencies in their stated requirements and could therefore be a modicum less restrictive. For example, Clerk staff report that the majority of rejected proxy letters were rejected due to the incorrect citation of the relevant clause in H. Res. 965. In the future, the citation of the correct resolution number as sufficient for accepting a letter would drastically cut down on the number of rejected letters, improving efficiency for Clerk and other staff, while maintaining the integrity of the process.
2. Future implementation of changes to voting procedures can be both adherent to the Rules and precedents of the House and also allow for changes if issues arise or clarification is needed. For instance, the current voting guidelines do not spell out a procedure for Members who have designated a proxy that is no

longer available because the Member they have selected has themselves named another Member as their proxy. (Member A names Member B as his proxy but, subsequently, Member B names Member C as her proxy, and thus is unable to serve as proxy for Member A.) This creates a duplicative workflow. Under the existing rules, the Member in this situation (Member A) must either (i) revoke the inactive proxy via letter and then resubmit a new proxy designation letter or, (ii) submit a proxy alteration letter. This is an area where clarification is often needed and inefficiency arises. For future voting changes, the ability to modify those changes to accommodate such need for clarification would be a way to limit inefficiency and ensure a smoother transition from one process to another.

The Office of the Clerk remains committed to the integrity of the legislative process and to carrying out the directives of the House in any future changes to the voting processes.

3. What lessons were learned from the implementation of the current electronic voting system in the House Chamber that could be applied to potential voting procedure changes in the future?

Since its first introduction in 1973 the EVS has undergone multiple transformations. The EVS server evolved from a large mainframe computing machine that filled entire rooms in the 1970's to high performance compact servers that fill up only a fraction of a rack space today. The vote displays based on placards with light bulbs as indicators have been replaced with real-time high-resolution LED displays. Similarly, the voting system software has undergone evolutionary changes over the years to accommodate procedural changes instituted by the House, as well as incremental improvements to enhance security and stability of the system. Today the EVS continues to serve its purpose in the House, accurately recording votes and securely disseminating vote results to multiple end points, including the Clerk's website, the Government Publishing Office, the Library of Congress, and the public.

The Clerk's Office stands ready to support any changes to the legislative process. Technology decisions must be executed carefully and always with institutional needs as the primary driver.

4. In general, do Members of Congress ever accidentally press the wrong button on voting machines or otherwise mistakenly vote the wrong way?
 - a. If so, do they have an opportunity to change their vote?

Currently, the EVS allows members to change their vote following a prescribed rule set by the House. For a fifteen-minute-vote, a Member may change their vote selection any number of times during the first ten minutes of the vote on any vote station. Any changes to a vote during the final five minutes of a fifteen-minute-vote must be executed by going to the well and making the change manually with the assistance of a Tally Clerk. For a five-minute-vote and a two-minute-vote, a Member may change their vote any number of times on a vote station before the vote is closed.

HEARING
COMMITTEE ON HOUSE ADMINISTRATION
“EXPLORING THE FEASIBILITY AND SECURITY OF TECHNOLOGY TO CONDUCT REMOTE
VOTING IN THE HOUSE”
JULY 17, 2020
MAJORITY QUESTIONS FOR THE RECORD
FOR
MR. JON GREEN
VP AND CHIEF SECURITY TECHNOLOGIST
ARUBA NETWORKS

1. Assuming VPN provides protection for wireless internet connections, what are best practices with respect to securing cellular connections?

Answer: Cellular connections are often thought of as “secure” because of native encryption technologies used in 4G and 5G networks. Two major weaknesses are still present: interception and man-in-the-middle attacks of the signal (e.g. the Harris Stingray), and interception/monitoring of network traffic inside the cellular core network or elsewhere beyond the mobile carrier’s network. For this reason, some form of end-to-end encryption should be used over cellular networks. A VPN is one way to achieve end-to-end encryption, and has the advantage of making all network traffic inside the VPN tunnel invisible to the cellular carrier. Another method of achieving end-to-end encryption is Transport Layer Security (TLS), commonly integrated into applications such as web browsers and email clients. Although TLS provides confidentiality for the majority of data it carries, a small amount of information (the server name) is sent in plaintext and can thus be tracked by the cellular carrier or other upstream service providers.

The cellular carrier may be able to interact with the baseband processor on mobile devices and may be able to push firmware updates. For this reason, trust in the cellular carrier is important. In the NSA Commercial Solutions for Classified architecture, mobile devices may not connect directly to a non-US cellular network. Instead, they require a “retransmission device” – the mobile device connects to the retransmission device over Wi-Fi, and the retransmission device connects to the cellular network. Whether or not such an architecture is deemed necessary depends on the sensitivity of the data being transmitted.

2. Please explain the differences between router-based VPN and some wireless access points.

Answer: Many different types of devices can serve as VPN endpoints. The most common VPN endpoint is an end-user device such as a laptop, tablet, or smartphone. In that type of VPN deployment, some form of secure tunnel extends from the end-user device back to a central enterprise-controlled device like a VPN concentrator or router. One of the downsides of this type of VPN is that the user often needs to interact with the VPN software, to start it and establish a connection.

VPN can also be built into routers – both enterprise-grade routers designed for business use and consumer routers designed for residential use. When a router implements VPN technology, a secure tunnel can be formed between the router and an enterprise datacenter. All network traffic passing through the router (e.g. from one or more end-user devices) can be sent through the VPN tunnel, or routers can apply rules so that only certain types of network traffic are sent through the tunnel. One advantage of this approach is that the VPN technology is transparent to the user – nothing needs to be configured, enabled, or managed on the end-user device. Additionally, router-based VPN can support multiple types of end-user devices, including those that may not have the capability to use VPN themselves (e.g. printers, phones, video conferencing systems).

Some types of wireless access points (e.g. the Aruba Instant family, or the Aruba Remote Access Point family) can also support VPN technology, in a way that is similar to router-based VPN. With these wireless APs, any device that connects to them over Wi-Fi can have network traffic sent over a VPN tunnel, either in total or selectively based on configured rules. One reason this solution is popular over router-based VPN is that existing routers remain in place and existing networks continue to operate – the wireless AP is added *behind* the router; it is thus less disruptive to deploy. A second reason this solution is popular, speaking from an Aruba point of view, is that it becomes possible to send native encrypted Wi-Fi network frames across a VPN tunnel and only decrypt and process them back into routable network traffic inside an enterprise datacenter. The effect is that from the perspective of the enterprise network, Wi-Fi users at a remote site appear to be directly connected to the enterprise network rather than connected to a remote site. This has significant security benefits and also network/device management benefits since enterprise IT personnel have link-layer visibility of the connected devices. This style of deployment is

often done in such a way that an enterprise Wi-Fi network deployed inside enterprise buildings and facilities also appears inside small branch offices and remote locations such as homes. An end user may take a mobile device, such as a laptop, to any location where this Wi-Fi network appears and access the network in exactly the same way; any differences between an on-premise Wi-Fi network and a remote Wi-Fi network are handled by the equipment and not visible to the end user.

HEARING
COMMITTEE ON HOUSE ADMINISTRATION
“EXPLORING THE FEASIBILITY AND SECURITY OF TECHNOLOGY TO CONDUCT REMOTE
VOTING IN THE HOUSE”
JULY 17, 2020
MAJORITY QUESTIONS FOR THE RECORD
FOR
DR. RONALD L. RIVEST
INSTITUTE PROFESSOR
MIT COMPUTER SCIENCE & ARTIFICIAL INTELLIGENCE LAB

1. We know that certain forms of multifactor authentication are more secure than others. For instance, when dealing with a sophisticated state actor, utilizing a text message verification may not be sufficient.

- a. What characteristics should the House be looking for in a multifactor authentication system?

Answer: You should be looking for a system that is hard to spoof and having experimental evidence for “hard to spoof” would be good.

- b. Are there any multifactor authentication methods you recommend avoiding?

Answer: Those that are easy to spoof or too hard to use.

- c. Are certain multifactor authentication methods more user friendly than others?

Answer: Yes, this is an empirical question.

- d. Which multifactor authentication methods are most secure?

Answer: Typically, multi-factor authentication systems are based on (a) something you know (b) something you possess, and (c) something you are. For example, PIN, phone, biometrics. You should try to have a multifactor system that uses two or even all three of these types.

2. Are there any recent trends in cryptography that the House should consider if it implements a remote voting system?

Answer: The most important property is verifiability: the voter should be able to verify that the vote cast and recorded is the vote intended. As noted in my testimony, a public bulletin board can effect this. The voter should be given ample time and means to perform such verification (e.g. by examining the public bulletin board), and to correct any errors.

HEARING
 COMMITTEE ON HOUSE ADMINISTRATION
 "EXPLORING THE FEASIBILITY AND SECURITY OF TECHNOLOGY TO CONDUCT REMOTE
 VOTING IN THE HOUSE"
 JULY 17, 2020
 MAJORITY QUESTIONS FOR THE RECORD
 FOR
 DR. AVIEL RUBIN
 PROFESSOR AND TECHNICAL DIRECTOR OF THE JHU INFORMATION SECURITY INSTITUTE
 DEPARTMENT OF COMPUTER SCIENCE
 JOHNS HOPKINS UNIVERSITY

1. In your testimony you mentioned that any remote voting system should be auditable. How do you recommend the House make its system auditable?

I would recommend that the House make its system auditable by putting processes in place where every vote has an independent check that it was cast and recorded correctly. There are several ways to do this, and these can be implemented concurrently. For example, a staffer, or several staffers for the House Member casting a vote should be able to register a mobile device that will receive a push notification whenever the Member casts a vote. The notification will include the matter voted on and the way the Member voted. Furthermore, the vote should be displayed on a publicly viewable virtual board, as I described in my testimony, and a staffer should be assigned to verify that the vote on the board is correct. It would also be possible to have house administration staff review votes as they come in. In general, I assume that for most Members on most issues, it is well known how they stand. The House staff could assign someone to sanity check the votes as they come in, and to raise a flag if a vote appears to be out of character with the Member's expected vote. These instances can be followed up with direct contact of the Member by phone or some other way to double check that their vote is in fact as recorded by the system.

- a. Is the fact that members can check to ensure that their vote is counted as cast enough, or should the House be looking at other ways to ensure the system is auditable, such as a paper trail?

I think the fact the Members can check to ensure their vote is counted as cast as I describe above should be sufficient, and I do not think a paper trail is necessary nor appropriate in this context.

2. Are certain devices easier or more difficult to harden than others? Explain.

Yes, certain devices are more difficult to harden than others. What determines the difficulty of hardening a device is the amount of software present. For example, a smartphone with a general-purpose operating system and dozens of apps on it is much more difficult to harden than a dedicated special purpose device that can only be used for one thing. Smartphones are an attractive type of solution to remote House voting and other problems, because they are ubiquitous, and every Member and staffer can be expected to

already have one. However, if a special-purpose device were deployed and given to each Member, that would be a much more secure solution.

3. Please describe criteria for usability and security that you think the House should consider when assessing potential remote voting platforms.

I believe that the criteria for security are as follows:

- Each Member's vote is independently audited and verified, in the way I describe in my answer to question #1 above
- There is a backup mechanism for each Member to use to vote in the case that the network they normally use is down. In the worst case, there must be a way for a Member to alert the House administration that they are unable to vote if their network is down.
- There is a publicly viewable virtual board that displays the votes as they are cast and recorded that the Members' staff can use to verify that votes are correct

As far as usability, it is important that the Member be presented an interface that is intuitive and which does not contribute to any confusion on the part of the Member as to how they are voting. It would be a good idea to include a confirmation, such as "Are you sure you meant to vote X?" pop-up before a final vote is submitted.

In both cases, I suggest engaging with security and usability experts before a solution is adopted, to help ensure that the security and usability criteria are met by the system.

HEARING
COMMITTEE ON HOUSE ADMINISTRATION
“EXPLORING THE FEASIBILITY AND SECURITY OF TECHNOLOGY TO CONDUCT REMOTE
VOTING IN THE HOUSE”
JULY 17, 2020
MAJORITY QUESTIONS FOR THE RECORD
FOR
DAVID WAGNER, PH.D
UNIVERSITY OF CALIFORNIA, BERKELEY

1. Are there different levels of vulnerability between systems that utilize a wireless internet connection versus ones that utilize a hard-wired internet connection?
2. Are there certain types of cybersecurity threats that may not be common now, but that you anticipate becoming more common in the medium and long term?

July 16, 2020

Hon. Zoe Lofgren, Chair
Committee on House Administration
U.S. House of Representatives

Hon. Rodney Davis, Ranking Member
Committee on House Administration
U.S. House of Representatives

Re: Hearing Entitled “Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House”

Dear Chair Lofgren, Ranking Member Davis, and members of the Committee on House Administration:

We write to commend the Committee on House Administration for its well-timed hearing entitled *Exploring the Feasibility and Security of Technology to Conduct Remote Voting in the House* and to share our recommendations on the topic. We write on behalf of Demand Progress, a progressive non-profit focused on building a modern democracy, and the Lincoln Network, a conservative non-profit with a mission to bridge the gap between innovation and policy. We have spent a great deal of time and effort understanding and making recommendations to strengthen the legislative branch.

To understand how the legislative branch functions, it is important to understand the modern House of Representatives, forged by Speaker Newt Gingrich. When Republicans seized the House majority in 1995, Gingrich oversaw the work that accelerated the House’s transformation from the analog age into the digital. This included the reorganization of operational information technology under the newly created Office of the Chief Administrative Officer, the creation and adoption of the House Information Systems Program Plan by the newly created Computer and Information Services Working Group, and the subsequent CyberCongress project.¹ Fulfilling his long standing posture against corruption, he also shook up ossified practices like ice-delivery and member car washes, which reeked of decadence.²

Despite helping advance positive reforms, Gingrich’s approach to governance greatly undermined Congress as an institution. It resulted in the gross centralization of power in the Speakership, the evisceration of its committee and personal offices, and the undermining of its support offices and agencies. The House post-Gingrich is less deliberative, more polarized, and has significantly less capacity to fulfill its constitutional responsibilities of legislation, oversight, and constituent services.

¹ “CyberCongress Accomplishments During the 104th Congress,” presentation of the Computer and Information Services Working Group to the Committee on House Oversight (February, 1997), https://web.archive.org/web/20010105040400/http://www.house.gov:80/cha/publications/cybercongress/body_cybercongress.html.

² We do not wish to make too fine a point here, as he was the first Speaker ever to be reprimanded by the House for ethical misconduct. “House Reprimands, Penalizes Speaker,” John Yang, *Washington Post* (January 22, 1997), <https://www.washingtonpost.com/wp-srv/politics/govt/leadership/stories/012297.htm>.

A few data points as illustration. The third bullet point in Speaker Gingrich's *Contract with America* pledged to "cut the number of House committees, and cut committee staff by one-third."³ He kept his pledge, and went further.⁴ During his first Congress as Speaker, House committee staff decreased by 33%, from 1,947 staff in 1994 to 1,306 staff in 1996. Personal office staff decreased by 10%, from 7,284 to 6,532. In that same time period, GAO staff decreased by 20%, from 4,572 to 3,677, and CRS staff decreased by 13%, from 835 to 729. The Office of Technology Assessment was defunded, and significant efforts were made to undermine other legislative support agencies. He also undermined the Democratic Study Group and other caucuses, which were a forum for member collaboration.⁵ The House of Representatives has not recovered, and power has shifted to the executive branch and lobbyists — and to the Speaker's office.

The fifth plank of the *Contract With America* was a ban on the casting of proxy votes in committee. The Congressional Research Service has a useful summary of how proxy voting worked in Committees prior to the 104th Congress.⁶

In the 103rd Congress (1993-1994), the last Congress in which proxy voting was permitted, 18 of the House's 22 standing committees authorized proxy voting in their rules. If a committee permitted proxy voting, House rules required that a member's proxy authorization:

- be in writing,
- assert that the member was absent on official business or was otherwise unable to be present at the committee meeting,
- designate the person who was to execute the proxy,
- be limited to a specific measure or matter and any amendments or motions pertaining thereto, and
- be signed by the member assigning his or her vote and contain the date and time of day it was signed.

Members generally indicated in their proxy authorization how they wished to vote on a specific question. Blanket (or "general") proxies were permitted only for procedural motions such as motions to recess or adjourn. Several committees' rules dictated the wording of a proxy authorization or provided a boilerplate form for the purpose.

³ "Contract With America," <http://media.mcclatchydc.com/static/pdf/1994-contract-with-america.pdf>.

⁴ "Science, Technology, and Democracy: Building a Modern Congressional Technology Assessment Office," Zach Graves and Daniel Schuman (January 2020), pp. 13-17, https://ash.harvard.edu/files/ash/files/293408_hvd_ash_science_tech_and_democracy_report.pdf.

⁵ See, e.g., "The Man Who Broke Politics," McKay Coppins, *The Atlantic* (October 17, 2018), <https://www.theatlantic.com/magazine/archive/2018/11/newt-gingrich-says-youre-welcome/570832/>; "When Liberals Were Organized," Julian E. Zelizer, *The American Prospect* (January 22, 2015), <https://prospect.org/power/liberals-organized/>.

⁶ "The Prior Practice of Proxy Voting in House Committee," Christopher Davis, Congressional Research Service (May 1, 2020), <https://www.everycrsreport.com/reports/IN11372.html>.

The proxy voting rules adopted by the House of Representatives in response to the emergency triggered by the COVID-19 pandemic, by contrast to the rules that existed prior to the 104th Congress, remove any discretion on the part of the person authorized to cast the vote, put in place transparency requirements, and contemplate the instantiation of *remote deliberations*, whereby a member fully and contemporaneously participates in legislative debate and has the ability to make motions and vote in real time on pending matters.

The COVID-19 pandemic necessitates the ability of members to deliberate remotely. We articulated principles for remote deliberation back in March,⁷ and they include deeming members present when they are present via electronic means and permitting the counting of votes cast by members present via electronic means. Demand Progress published a comprehensive memorandum analyzing remote deliberations on March 24,⁸ which started with the premise: "We would rather have a House of Representatives that can deliberate remotely than a House of Representatives unable to deliberate at all."⁹

This remains the crucial choice. And unlike in the era of Speaker Gingrich, where a 24-hour news channel was considered modern and the Internet was still described in terms of an information superhighway, technology has sufficiently advanced where members serving on a committee or engaged in "floor" debate can remotely engage in debate and cast votes as if they were present in person. Members can be seen and heard, they can introduce amendments and make motions, they can be advised by staff, and they can participate in the legislative process. In addition, they have the ability to collaborate with one another regardless of whether they are in Washington, D.C., as they can communicate by phone, text, email, video-conference, and so on. This level of deep engagement with one another and in the legislative process should be the goal of any legislature.

We have seen some instances where professional commentators are holding out unreasonable standards for online legislative deliberations that go beyond what is the current practice for in-person deliberations. For example:

- There are instances where members have trouble making themselves heard during deliberations when they begin speaking. This happens when they communicate over the internet, but this happens in person, too, when they forget to turn on the mic.
- There are instances where members may miss a proceeding because their internet connection breaks. This happens in person, too, when a member misses a flight or their car

⁷ "Continuity of Legislatures," Daniel Schuman, Demand Progress (March 17, 2020), https://s3.amazonaws.com/demandprogress/reports/Memo_for_Legislatures_on_their_Continuity_in_Emergencies_2020-03-17.pdf.

⁸ "Summary and Analysis: House Rules Committee Democrats Report on Remote Voting," Daniel Schuman, Demand Progress (March 24, 2020), https://s3.amazonaws.com/demandprogress/reports/Summary_and_Analysis_House_Rules_Committee_Democrats_Report_on_Remote_Voting.pdf.

⁹ More resources on remote deliberations can be found at <https://www.continuityofcongress.org/>.

breaks down. Few members have a perfect voting record.

- There may be instances where members cast the wrong vote when communicating electronically. This happens in person as well, where members push the wrong button on the floor or say the wrong thing (and sometimes hand their voting card to another member). We have error correction mechanisms for this, and the nature of public votes means such errors can be identified and corrected.

There are electronic equivalents to in-person actions that fulfill the same purposes. A member wishing to be recognized can electronically raise a hand in the same way the member could rise from a sedentary position. All that is necessary to make this work is a good will, significant groundwork to get the technology functioning properly, and a desire to keep the House operating. We applaud the questions raised by Ranking Member Davis on May 14th is exactly the kind of smart technical questions that should be asked and addressed,¹⁰ and we agree that a crawl-walk-run approach is a smart way to conceptualize the shift in House operations.¹¹

We have significant concerns that recent events have further centralized power in the hands of leadership over committees and the rank-and-file. This concern does not arise from proxy voting, but a combination of the fact that in-person voting is so unsafe that it can take hours to conduct a single vote and that the nature of an emergency is that power flows to the center. Proxy voting may be a factor, but a comparatively minor one.¹²

A move to instantiate regulate order through fully remote deliberations may help ease the pressure to reduce time spent with members on the floor. That, in turn, may reduce the pressure to constrain floor activities, which, in turn, may empower committee deliberations. We also recognize that the extraordinarily power now held by leadership is the natural result of the changes wrought in the House of Representatives by Speaker Gingrich. Addressing that issue is beyond the scope of a hearing on remote voting technology.¹³

We thank you for your kind consideration.

Sincerely yours,

Daniel Schuman
Policy Director, Demand Progress

Zach Graves
Head of Policy, Lincoln Network

¹⁰ "Letter from the Hon. Rodney Davis to the Hon. James McGovern," (May 14, 2020) https://s3.amazonaws.com/demandprogress/documents/2020-05-14_CHA_RM_Davis_Concerns_With_H.Res_965.pdf.

¹¹ Ibid.

¹² "Initial Thoughts on the House's Remote Deliberation Resolution," Daniel Schuman, First Branch Forecast (May 13, 2020), <https://firstbranchforecast.com/2020/05/13/initial-thoughts-on-the-houses-remote-deliberation-resolution/>.

¹³ But we would welcome a conversation on that topic. A starting point is our bipartisan letter "Strengthening the Legislative Branch by Increasing its 302(b) Allocation," (June 22, 2020), https://s3.amazonaws.com/demandprogress/letters/Strengthening_the_Legislative_Branch_by_Increasing_its_302b_Allocation_2020-06-22.pdf.

The CHAIRPERSON. And with that, we are ready to adjourn, and I will take my gavel and virtually tap it.
We are adjourned. Thank you very much.
[Whereupon, at 2:56 p.m., the committee was adjourned.]