On June 23rd, 2020, the Standing Committee on Procedure and House Affairs adopted the following motion:

> *It was agreed, — That in camera transcripts of the meetings held on May 28 and June 2, 2020, be shared, by the clerk of the committee, with the Chief Information Officer of the House of Commons administration and any other officials deemed appropriate; and, that the CIO provide to the committee recommended redactions to the in camera transcripts regarding national security no later than July 3, 2020.*

On July 7, 2020, the committee agreed to the redactions suggested by the Chief Information Officer of the House of Commons, adopting the following motion:

> *It was agreed, — That the specified sections of the transcripts of in camera proceedings for the committee's May 28 and June 2, 2020 meetings be rendered public committee evidence, provided that agreed upon redactions are made.*

The redacted committee evidence from portions of the June 2nd in camera meeting appears below.

****

Standing Committee on Procedure and House Affairs

Comité permanent de la procédure et des affaires de la Chambre

UNEDITED, TRANSLATED EVIDENCE NUMBER 19,
TÉMOIGNAGES DU COMITÉ NUMÉRO 19, TRADUIT, NON ÉDITÉ

PARTIE À HUIS CLOS SEULEMENT - IN CAMERA PART ONLY

Tuesday, June 2, 2020 - Le mardi 2 juin 2020

* * *

🕛 (1230)

[Traduction]

The Chair: Thank you very much.

I think as long as we do this a few more times, we can probably get our time down once everyone's familiar with the proceeding.

Next up for the second panel, we have Mr. Jones joining us from the Canadian Centre for Cybersecurity. Welcome, Mr. Jones.

We still have our officials from the House administration team—Mr. Patrice, Mr. Robert, Mr. Gagnon, Mr. Aubé and Mr. Dufresne. Thank you for joining us for the second panel. I'm sure there are going to be a lot of interesting questions on this panel.

Technically I would say it's not even another panel really. It's just a continuation, but we had to move to go in camera. Originally what we had decided is that we would carry on with the five-minute rounds, but I think I will put it out to you if you want to start back up at the top of round one for this panel again. I guess I keep saying panel even though we've just added another member. It's just a three-hour long meeting with one panel really.

Would you like to start out at the top of the five-minute round, or at the top of the six-minute round?

Ms. Rachel Blaney: Madam Chair, I would like to start at six-minute round. I certainly don't want to have just two and a half.

The Chair: That's what I thought. Okay.

I don't think I have a clear list since we're starting this way of who would like to start, but for the Conservatives who would like to start with questioning?

Mr. Tochor, please go ahead, for six minutes.

Mr. Corey Tochor: Thank you, Mr. Jones, for being here today.

On the technology side of things and the security side, what can we work into the system to catch mistakes, or catch errors, or fraud? From your point of view, what could be done?

Mr. Scott Jones (Head, Canadian Centre for Cyber Security, Communications Security Establishment): I'm sorry, I'm not sure I quite understood the question in terms of fraud. Do you mean in terms of somebody impersonating?

Mr. Corey Tochor: There are dozens of ways that this could be crutted. What would be your fix if there was be it fraud, be it questionable foreign actors that are affecting our democracy, be it even partisans, either organized parties or just partisans in the general public that would want to interfere with a member's right to cast a vote one way or the other.

🕛 (1235)

Mr. Scott Jones: Understood. Thank you.

That's one of the areas we've been working with Mr. Aubé and his team on is to make sure we understand all the different threat environments, and then you design security to counter that with a layered defensive posture. On a longstanding partnership with the House of Commons both from the design, as they design the solutions we're working with them hand in hand on the security pieces, but also that we are really trying to layer in a full layer of defences out to the perimeter all the way back into the application as well.

Really what we do is we look for the threats, and then we look to make sure that we have counters to all of those different threats that were identified.

Mr. Corey Tochor: But what could happen after the threat was successful then?

Mr. Scott Jones: **
****
****
****
****
******************************.

Mr. Corey Tochor: **

Mr. Scott Jones: **
****
****
****
****
****
****
****************************.

Mr. Corey Tochor: Then to take this line one step further, maybe not on the technical side of it but a reality of it is if we have pressures on a vote—say there was a very tight vote and there were pressures afterward on members to change their vote either through accusing that there was a technical issue, that they voted the wrong way, you would find holes in this policy or problems with our democracy where we would have undue pressure on individuals to recast their votes in a different way with the guise that it was a mistake or that a foreign actor had infiltrated our system.

There have been cases around the world of different issues on technology with virtual either Parliament or voting. Are you aware of any attacks on our so-far limited use of virtual Parliament?

Mr. Scott Jones: I haven't seen any information on attacks on virtual Parliament, any information on that. Certainly one of the key things for us is we have been working from the start to design security in and certainly on things like voting, I can't speak to the procedural controls that the House uses to ensure one member one vote, but from a technology perspective, certainly encryption means that you can set this up so that you know that when a vote is issued it is that member who is issuing that vote.

It is the same concept we use when, for example, we are signing digital documents. Right now ** signing the document because of the way we've set things up.

It's a similar concept around voting as well.

Mr. Corey Tochor: Similar to any time you want to protect something, if you build a tall fence, you'll have the criminals just wanting to use a taller ladder so I still don't have the confidence. We're talking of an over 150-year tradition of how we cast votes in Canada, and I don't have the confidence that a technology solution will replace this in time.

There's a general concern about what we're discussing, but on the technology side of things, where is the easiest hole for a bad actor to crawl in?

🕐 (1240)

Mr. Scott Jones: If we were talking outside of the current environment we have, certainly just lax perimeter security, lax patching etc. is what most actors are using~~.~~

*** *** *** *** *** **.

*** *** *** *** **.

You continue to layer on defences to provide enough mitigations that you feel comfortable with the residual risk.

Mr. Corey Tochor: A quick question on the biometrics—

The Chair: There is no more time, unfortunately. Sorry, Mr. Tochor.

Next up we have Mr. Turnbull.

Mr. Ryan Turnbull (Whitby, Lib.): Thank you, Madam Chair.

Thanks to all our witnesses for being here. In particular I want to say thank you to Mr. Aubé and Mr. Jones.

I know that it seems from the Chair's remarks today that we've overcome quite a lot already in pursuing a hybrid in virtual proceedings. I am very reassured by that and all the great work you have done to make that happen, I really want to acknowledge.

I have three lines of questioning. One is, Mr. Aubé, you talked about how the Zoom platform ***. I really found that reassuring.

What I wanted to ask Mr. Jones about, if possible, is just how secure ******************* ****************? I apologize, I'm not a technical expert and I use some of these terms a bit loosely, so please feel free to correct me if I've misused any terms.

*** ** ***.

Can you speak to the data protocols and data around that platform?

Mr. Scott Jones: Absolutely. I'm sure Mr. Aubé can probably go into further detail on things, but certainly when we look at, for example, a data centre, the general IT security posture, we're talking about three things, the physical security pieces, which are more in the realm of the House of Commons and Mr. Aubé to talk about, but really we're talking about, in terms of IT security and House of Commons, it's a long-standing partnership. We have been working on security together. The perimeter has been very strong and strengthened in response to the evolving cybersecurity area, but also just everything down to even the management of the devices that every person is given, I know with those controls the House of Commons would rank up among the top organizations in terms of IT security that we deal with, including the private sector.

Mr. Ryan Turnbull: Thank you.

I imagine, Mr. Aubé, you might want to jump in here too.

You're doing regular risk assessments and a risk-management plan. You're looking at all the potential threats, and then, as Mr. Jones said, you're looking at a layered approach. To me, these are measures that ensure there's a very, very small likelihood of any threat actually penetrating our security system. Can you speak to that a little more, that layered approach? What are the layers specifically?

Mr. Stéphan Aubé (Chief Information Officer, Digital Services and Real Property, House of Commons): Thank you, Madam Chair.

Thank you for the question, Mr. Turnbull.

As Mr. Jones said, security for us at the House of Commons starts at the end point, it starts with the users, so we take great pride in how we secure these end points. We try to reinforce for all members how they certainly need to participate in such meanings. We enforce that they use House-managed devices, meaning that with these House-managed devices we have the controls and encryption for the transfer of data between these machines and our infrastructure.

Then we also have a monitoring strategy. ***
****
****
****
****
****
****
****
***.

🕐 (1245)

Mr. Ryan Turnbull: Thank you for that response.

How many breaches have there been since we started this virtual Parliament?

Mr. Stéphan Aubé: In the context of these virtual sittings there have been none, sir.

Mr. Ryan Turnbull: Zero. Okay. Thank you.

The threat has been out there the whole time, but we've had zero penetrations of our system currently.

Mr. Stéphan Aubé: Not that we're aware of, and we certainly do a lot of monitoring every day.

Mr. Ryan Turnbull: Thank you for that work, because that reassures me and I'm sure reassures everybody here.

One other thing. I know the U.K. developed a MemberHub to do online remote voting and it has multi-factor identification. I wonder, Mr. Jones or Mr. Aubé—whomever is most appropriate, I'll leave it to you—how do we verify, from end to end, specific persons who might be voting in the future?

Mr. Stéphan Aubé: I can talk to that.

We're certainly aware of what the U.K. has been doing as part of our relationship as international partners. We looked to that, but, sir, our strategy is, we have 10 points to actually secure this infrastructure.

We're focusing on the first part, which is the notification. We need to ensure that everyone gets notified and that they're secure notifications, that means between the House and the members. That's the first step, sir.

The second part, sir, is identification of the members. We're going to restrict access to these events to only members and only members ****************, sir, and ************, other identification measures to actually ensure at 100% or near 100% that it is that person participating in the meeting, sir.

We're also going to be looking at the transport mechanism of all information between these end points, so we are securing, as Mr. Jones talked about, through encryption between the end devices that are participating, right up to our data centre.

We're also looking at the recording of the results and the archiving of the results to ensure that no one has the ability to modify or change these results, sir.

We're also looking at the casting approach, because it's not only about casting your vote, it's also confirming it's that person who has voted, so we need to look at ways, through different channels— for example, the U.K. was sending a confirmation of the vote when the members casted their votes, through an encrypted messaging approach. That's how it's been done. These are approaches we are considering right now and assessing with our peers CSEC.

We're looking also at the publication of the results—

The Chair: That's all the time we have unfortunately, Mr. Aubé.

Mr. Ryan Turnbull: Thank you, Mr. Aubé.

The Chair: Thank you.

Next up is Madame Normandin.

[Translation]

Ms. Christine Normandin: Thank you, Madam Chair.

Once again, thank you for being here.

Like my fellow member Mr. Turnbull, I’m not very tech savvy, so I hope you’ll correct me if I say something that doesn’t make sense.

My first question has to do with face recognition. A bit like we just did with the committee. How much of a threat do deepfake programs pose? Is it something we should take into account, or is it a bit far-fetched to think it could happen?

Mr. Stéphan Aubé: Given the architecture work that's been done thus far, it's almost impossible for something like that to happen. I always say almost, because there's always a certain degree of risk in anything we do. Nevertheless, as far as the architecture we're putting in place goes, we want to be 100% sure that we're able to identify the person participating in the meeting and the person who, if a vote were taken further to such a request, would be the right person voting as well.

Ms. Christine Normandin: Great.

I just want to be sure I understand. For example, if there's a vote, the person voting will be authenticated at many specific points in time. That's part of the underlying security you would build in. When the member joins, then, when they vote and, afterwards, a third time, to make sure it's the right person.

Mr. Stéphan Aubé: Yes, I would say it starts even before that, meaning, ************ ***. Those would be elements used to validate the person's identity.

🕐 (1250)

Ms. Christine Normandin: Wonderful.

As we all know, when votes are called suddenly, a person might be in the washroom because they don't want to vote on a particular issue. If a member were to indicate that there was a technical difficulty and they weren't able to vote. If there was indeed a problem with the Internet connection or if a member said they weren't able to exercise their right to vote, could the IT people validate that information to confirm whether it was true, for instance?

Mr. Stéphan Aubé: When I was speaking to Mr. Turnbull earlier, I was looking at the list of things we were talking about, but something I didn't mention before is the whole system audit component.

We were talking about possible transactions and the sending of messages between us and the member. All of those things leave a footprint that is used to validate the person's identity to make sure it is them and that they were able to participate.

If something were to happen, we would know about it. For instance, since you asked us a question earlier [*Inaudible—Editor*], do we know how many people are disconnected during the event? It's that kind of footprint that we are keeping right now in an effort to work with the people after the meeting to improve the system. At the same time, it will help us validate that the results are indeed the right ones.

Ms. Christine Normandin: All right.

In that regard, it’s possible to see what types of problems may have occurred. Is it the member, themselves, who chose to disconnect because they didn’t want to vote, or did a technical difficulty really occur? There will indeed be a way to know.

Mr. Stéphan Aubé: Yes, that’s our intention.

As an option, the first validation step could be determining whether the member received the voting notification. What device did they receive it on? Their tablet or their cell phone? On top of that, did the member read it to complete the second step?

Next, did the member exercise their right to vote and what was the result? All of those things will happen securely in order to ensure they aren’t altered. We won’t be able to really validate what happened.

Ms. Christine Normandin: Thank you.

As for choosing the voting platform and sharing that information with the parties—who will have a say—do you already know what protocol you’ll be following to explain to members what the platform will be, to discuss the recommendations with them and to find out whether or not they are comfortable? Is there something already in place?

Mr. Stéphan Aubé: In terms of how we’re going about things now, we are working towards having a flexible infrastructure that can meet the needs of the different parties. That’s a first result.

The second thing is that we are trying to use tools we already have. Our approach is to use available tools to create the platform.

However, from the user interface standpoint, we make sure it’s user-friendly. Those are things we could work on with a group of members to make sure we have the required feedback to make it as user-friendly as possible.

Our first goal is to make sure we can do it securely so we can, then, work with you to ensure the user interface meets your needs. We want it to be as uncomplicated as possible.

Ms. Christine Normandin: Wonderful.

I have one last question about possible incidents in the future. Is there already a protocol in place outlining how you will report such incidents? Who will you report them to? One of the House services or the parties directly? Who will be notified?

Mr. Stéphan Aubé: As far as voting goes, the protocol hasn’t been defined yet because we haven’t received the formal request. If we had the formal request, there would be a protocol.

I’ll give you the example of when a security incident occurs inside the House. If our team discovers a security incident within the House, *************************************

****
****
****
****
***.

If an incident occurs outside the House, ***
****
****
****
****
****
****
***************.

🕛 (1255)

[Traduction]

The Chair: Thank you, Mr. Aubé.

Next we have Ms. Blaney, please.

Ms. Rachel Blaney: Thank you.

So far this has been very informative, and I think it's always important to recognize the tremendous work of all the folks who have been working on the many levels of adjusting to COVID-19. I would like to take that opportunity to thank all of you right now.

First, Mr. Aubé, you started to list 10 steps that you're taking. I think I got six. I'm just wondering, is that information that you're able to table with the committee, those six steps?

Mr. Stéphan Aubé: Yes, we can.

Ms. Rachel Blaney: Thank you. That would be extremely helpful.

I guess my question...one of the biggest concerns as we move forward is, first of all, that we don't replace the important work that should be done in Ottawa, but we are in this circumstance so we have to do it differently. I think most of us understand that.

I'm just wondering if we could hear a little bit more about what models of virtual voting have been looked at and if there is any particular security issues that we should be aware of.

Mr. Stéphan Aubé: I can answer the first part, Madam Blaney.

There are different scales of voting systems. I just want to focus. We're not talking about electoral voting systems. We're really talking about board-type meetings or meetings that are linked to a particular organization. What you'll find is a large scale of voting system which, as an example, this tool could be used as nominal voting, by which we call the name of a member and the member states his votes, okay, so that would be as simple as possible.

Then there would be an added ability, for example, for people to vote with a system in the chamber, just as someone mentioned the point... I don't know if people know, but 12 years ago when we did the last upgrade of the audio system we had built in the functionality to have voting in the chamber. Cabling and infrastructure in the Centre Block was already there. At the consulate we were planning at one point to actually have the ability to have [*Inaudible*], so these are built-in systems, dedicated systems for voting that exist out there.

Then the third side is, usually if you look at the audio systems in the committee rooms, most of the suppliers such as Bosch or Televic offer voting capabilities built into them.

Then the last years it's really because of the evolution of technology. We're now seeing more and more voting that is based on mobile infrastructure, leveraging the cost of the mobility to vote.

This is, you might say, the spectrum of voting systems that you'll see. What we're talking about here from a more complex approach is a complete mobile voting approach. If someone not present in the meeting would have the ability to vote, I'm calling a mobile infrastructure. These are the steps that we're looking at, the 10 steps that we're looking at in the concept of these systems.

Having said that, if you're focusing more on a normal video participation voting system, it would be a lot simpler. It's basically leveraging what you have right now and looking at the procedures to make this happen.

We're looking at the different scenarios of voting, ****************************** *****************************, which is leveraging a mobile environment that is a little bit more flexible but more complex and the need to have these daily discussions with our security partners.

Ms. Rachel Blaney: Thank you so much for that.

I think, from my perspective, video voting does alleviate some of the concerns that members have around identification, if we can actually see the person by video saying yes. I'm just thinking of earlier in this meeting where it was like, can you look at your staff member and verify that as who that person is. I think that's important.

So I'm wondering a couple of things. The first one is, do you feel that video voting is a place we should consider starting? The other aspect is, as we go down this path what would be the cost associated? I would assume that if we're using this technology that we already have, we've made that investment. As we take that next step that you're talking about, what would be costs and how would we be able to understand that?

Mr. Stéphan Aubé: I'll just start with the cost option. We believe the approach that we're taking is that we're leveraging our existing investments in mobility, in our IT infrastructure and our own resources *************** to actually build any solution that you like. We believe that for any solution that you will ask we do this with minimal investments required by the House because you already have the mobile infrastructure to do that, we already have the team in place that actually supports you ********************** also. So these resources are not an additional cost to you at this stage. The systems that we're planning to use already exist at the House of Commons. That's our approach.

As an example, for the messaging element we're hoping to leverage existing tools that we have,**************************. This is a secure mobile application that would be leveraged in our portfolio in applications to notify the members. That wouldn't be an additional cost because this already exists at the House of Commons.

So these are the types of tools that we're planning to put together to make this happen, at a minimal cost. This has been a criterion since the beginning of this pandemic. We want to leverage what we have before we expend any new funding on anything less.

🕐 (1300)

Ms. Rachel Blaney: Thank you for that. I know that we have biometrics on our MPs' computers, tablets and phones. I'm just wondering, is there anything else we should be looking at in terms of addressing the issue of security?

Mr. Stéphan Aubé: In the context of voting, we're currently having this discussion **** ****. I wouldn't say that we're eliminating biometrics or including biometrics. We're not there at this stage. We just want to make sure that it is secure and it can meet all the requirements. If it is a requirement, we'll recommend this to this committee, Madame Blaney.

The Chair: Thank you, Mr. Aubé.

Next, for the Conservatives, who do we have? Is it Mr. Genuis?

Mr. Doherty, please go ahead.

Mr. Todd Doherty: Thanks, Madam Chair.

This is for Mr. Jones and Mr. Aubé regarding the Zoom platform itself.

Are there any concerns regarding the privacy and the security of the Zoom platform itself? Have we entered into a formal agreement with Zoom?

Mr. Stéphan Aubé: I will start answering that question, Madam Chair.

Thank you for the question. The agreement that we have right now with Zoom is we did an initial purchase order for three months of licensing, sir. That's the extent of agreements that we have. As I mentioned in public, our monthly cost for operating Zoom in camera or in public is the same; so it's still at $3,000 a month right now, sir. That's the extent of agreements that we have. We are considering—

Mr. Todd Doherty: It's very reasonable.

Mr. Stéphan Aubé: It is, sir, it is. That is one of the factors of why we looked at that solution, because we wanted to minimize costs for allowing this to happen.

For any other collaboration on the Hill, sir, we're promoting other approaches such as Microsoft teams because again we also have the licensing agreements to do that.

Mr. Todd Doherty: In normal circumstances, we know that there are foreign actors who are always trying to hack into our systems on a daily basis. I think you answered Mr. Turnbull's question regarding any potential hacking to this point that you're aware of; you said, none. But very publicly and as recently as in March there are states that have launched inquiries into Zoom's privacy and security practices. Do we have any concerns regarding that, specifically with the data-sharing policies. To your knowledge, is Zoom offering end-to-end encryption?

Mr. Stéphan Aubé: The public meetings are done on Zoom infrastructure. I want to clarify that. I believe you weren't at the last meeting when I presented that.

From our perspective, from a risk assessment perspective, very limited information is shared on these public meetings for the participants into these Zoom meetings. It's the House infrastructure used to authenticate these users. We're not asking people to create an account with Zoom, we're leveraging the accounts on the House side, so very little information is shared with Zoom.

**.

As far as information exchanged from the House with Zoom, it is only metadata. For example, a token that says that this person is authenticated with the House and will be allowed to participate. We also share meeting dates and times because of the licensing agreement, but that's pretty much the extent of what is shared with Zoom to address the sensitivity issues of these meetings.

🕐 (1305)

Mr. Todd Doherty: How would be get beyond members sharing their passwords with the Whip's office for voting?

Mr. Stéphan Aubé: There are different ways we're going to look at a person's authentication in the context of voting. As I said, one thing we would want to enforce if we go there is that this would be a **********************. That's one additional thing we're going to be looking at, ********************************* to that member.

In addition to that, I'm hoping members would not breach the policy of the House by sharing their personal passwords to their personal accounts to other parties. That's the second thing.

The third thing we are also considering is biometrics in the voting process to ensure it is that person who pressed the button. We would maybe have the ability to even capture an image of the person and validate against existing photos we have, public photos we have of the members. I'm not saying we're going to go there, but we're looking at different mechanisms to ensure it is the person who is supposed to be voting. If there's an risk, ********************************* ** **************************.

Mr. Todd Doherty: Any concerns regarding our public meetings being Zoom bombed at all?

The Chair: That's all the time we have, unless you can give a 10-second answer.

Mr. Stéphan Aubé: I feel at 99.9% that this will not happen to us unless someone does it [*inaudible*]. There's more risk using other tools than the one now with the way it has been configured.

The Chair: Thank you.

Mr. Gerretsen.

Mr. Mark Gerretsen: Thank you, Madam Chair.

Mr. Aubé, I have a quick question. There has been a lot of discussion about face recognition and looking at images of people. With the growing concern over deep fake, does it not become more and more possible the images portrayed could be altered to make it look like somebody but it's not them.

What is your preferred method for authentication, is it biometrics or something more reliable, authentic or harder to alter?

Mr. Stéphan Aubé: My quick answer, Mr. Gerretsen, is multi-factor authentication, so not one thing to prevent that from happening. I would first want to seek your vote and leverage your credentials by making sure it's your account and machine, but I would also maybe possibly look at sending you a confirmation that you just voted by using a different one or two more mechanisms. I would like to send you an email to make sure you did get that, and also possibly send an encrypted message with a different tool to make sure you did receive it.

These multi-factors are addressing it, versus focusing on one approach to doing it.

Mr. Mark Gerretsen: You also mentioned that using *********************** could perhaps avoid and prevent the Whip's office from voting on people's behalf. Are you not worried about a Whip's office having 60 computers or 70 computers there and voting for everybody?

Mr. Stéphan Aubé: I would hope that we're not doing that, sir.

Mr. Mark Gerretsen: I think the integrity of every member would prevent that from happening.

I'll share the rest of my time with Mr. Turnbull, Madam Chair.

The Chair: Please go ahead, Mr. Turnbull.

Mr. Ryan Turnbull: Thanks, Mr. Gerretsen.

The speaker said in his opening remarks that the technical team had developed a conceptual solution and I understood that this solution would use existing tools, including security measures that may already be utilized in the day-to-day functioning of the House.

Could you describe that in a bit more detail, that conceptual solution, and maybe just clearly indicate how easy it might be to implement that?

🕐 (1310)

Mr. Stéphan Aubé: Okay, Mr. Turnbull, and Chair, thank you for the question.

So conceptually, Mr. Turnbull, the way we see this happening is at first you would leverage the voting notification system that we have at the House and an encrypted message would be sent to multiple members' devices saying that there is a vote going on. ***.

That's the first process. You would launch this in the same way that you're launching right now with the bells but it would also send it electronically, notifying the members that there is a vote, and through that notification, in that message, what we're considering is including the motion. So you'd see what you'd be voting on, in the language of your choice, and also these tools would be accessible, okay, and once you've seen that, sir, what we would do is, if you wanted to vote or participate, we'd send you to a secure portal ************************, and there you would be authenticated and you'd go through the process of voting in the manner of your choice, sir.

Once you've voted, yea, nay or abstain, you would also get a confirmation, sir, a multi-factor encrypted approach [*Inaudible*] remember I talked about...validating your identity at different stages of the process. That would be another step by which we'd authenticate that yes, okay, I did send this because I did receive this on all my devices and depending on the device I'm using, I can confirm that I did make a vote or I did not make a vote, and then there would be a process if I did not make a vote to call in and say, “Hey, someone is actually using my devices.” I want to bring that in as an example, sir.

Then we'd be leveraging our existing publication of results process, tools that we have. We'd also allow voting grouping and we'll also have...as I said, identity capabilities to track at all times what's happening and monitor what is done, and all of this, sir, while leveraging encryption so that we can ensure that the transport of any messaging, either while you're voting or while you're receiving the notification, is encrypted ********************. That's the approach essentially that we're looking at and we're having a discussion on, through these different steps.

One last bit of information, because I didn't get a chance to raise it, it's very important that we validate the supply chain. That's one consideration that needs to be taken. If we're bringing new tools, we need to know what's behind the new tools to ensure that we can track all changes and track how it's been done so that we can validate the security of it also.

The Chair: Thank you, Mr. Aubé.

Next, from the Conservatives, all right, thank you, Mr. Genuis.

Mr. Garnett Genuis: Thank you very much, Madam Chair.

Can you speak a little bit, to clarify the kind of relationship between the technology platform and the House, because the technology is developed and operated by Zoom but you're saying that they're minimally involved because **. We're all seeing Zoom at the top of our window as we're having this conversation and there have been concerns in the past, for instance, about technology developed in China where it comes out later that there are back doors within the technology.

Help me understand why you don't seem to be as concerned about that in this case. Is there an issue with potential back doors that are sharing information through a channel that you're not seeing?

Mr. Stéphan Aubé: ******, I might just start with this and you can build on it if you want to.

Given the fact that ******************, we have the ability ***********************
****
****
***.

The concept of back door is what you're talking about, the ability for the software to start acting on its own **
***, to ensure that doesn't happen. ***
**********.

Mr. Garnett Genuis: If [Inaudible] has a quick follow-up question first, you mentioned if there was **. That seems to apply that there's a threshold ****************************. Is that correct?

Mr. Stéphan Aubé: What I would say is, I wouldn't frame it that way, sir. ************** *** *** **.

🕐 (1315)

Mr. Garnett Genuis: Okay, look, I'm not trying to put words in your mouth. I'm just trying to take the words you said and understand what they mean. You're saying—

Mr. Stéphan Aubé: I'm saying as an example, sir, if I might just correct what I said******** *** **.

Mr. Garnett Genuis: It just seems like it would be a pretty low-level operation if they were **********************************. It's far more likely there'd be somebody ******** **.

__*** ** ** ** ***********************. Is that correct? It seems to be based on what you're saying.

Mr. Stéphan Aubé: I wouldn't say that, Mr. Genuis, because there are many controls that we have ********* of *********.

*** *** **************************************.

The second thing, sir, we also don't record these meetings, so none of that content is being recorded to be used at a later date. *** *** **.

Mr. Garnett Genuis: Okay, if that's true, that's great. I just wanted to understand. You're saying now that if *** ** ***********************. Is that correct?

Mr. Stéphan Aubé: Absolutely, sir.

Mr. Garnett Genuis: Okay. That seems just different than what you said at the beginning, but if that's the case, then that's great. I'm glad it's been clarified.

Mr. Stéphan Aubé: We were focusing, sir, ** ********.

Mr. Garnett Genuis: ******************.

Mr. Stéphan Aubé: ** ************.

Mr. Garnett Genuis: ** ***?

Mr. Stéphan Aubé: ************************************.

The Chair: That's all the time we have. Thank you. I allowed for that exchange to occur and I'm glad we got an answer to that.

Ms. Petitpas Taylor, please.

Hon. Ginette Petitpas Taylor: Thank you so much.

Just a few quick questions.

For Monsieur Aubé, I'm wondering, do you feel that with the security measures that have been put in place that we can securely practise hybrid sittings in remote voting?

Mr. Stéphan Aubé: I feel that we can practice all remote participation in the sittings, ***** ** *******************.

Hon. Ginette Petitpas Taylor: Thank you so much.

I believe I understood you to say earlier that the services are being hosted within the House infrastructure. I believe that's what I understood.

Mr. Stéphan Aubé: That is the case, for in camera meetings.

Hon. Ginette Petitpas Taylor: Great. What security controls have been put in place?

Mr. Stéphan Aubé: As I said earlier, for the in camera meetings, more specifically, the first focus ** ** **

[redacted].

We also have the [redacted].

🕐 (1320)

Hon. Ginette Petitpas Taylor: I have one quick question before I turn it over to Mr. Turnbull as well.

What would be your response time for patch development if someone did infiltrate the system?

Can you give a quick response?

Mr. Stéphan Aubé: Madam Petipas Taylor, I'm trying to scope the question because it's a hard question. It depends on the infiltration.

Small things that we find on a day-to-day basis we basically address within the hour; for example, if a member's account was penetrated, and we've seen that. [redacted]. This is done 24-7 hours a day. [redacted].

That's what I'm saying; it depends on the scale. Easy things like that are done instantaneously. If there was something larger where they would have to penetrate the centre it's hard to estimate the time. Having said that, we certainly have measures to shut things down in order that nothing

is leaking in our information. **
********************.

Hon. Ginette Petitpas Taylor: Thank you so much.

Mr. Turnbull.

Mr. Ryan Turnbull: I have a quick question.

In terms of interference related to electronic voting it sounds like with all the security measures in place that would be highly unlikely.

In the case where there was some form of interference would we know, Mr. Aubé, based on all the monitoring that's going on and you have described, that there's been some interference?

Mr. Stéphan Aubé: We're certainly putting in place all the tools to know, Mr. Turnbull. That's my premise.

We are doing our due diligence working with Mr. Jones' team to ensure that we would know. If it did happen we could provide means for the members to continue participating.

Mr. Ryan Turnbull: So we could just recall the vote then?

Mr. Stéphan Aubé: Yes.

The Chair: Thank you.

That's all the time we have.

The Chair: Madam Normandin.

[Translation]

Ms Christine Normandin: Thank you.

My first question is about using Zoom as a voting platform until a system is implemented or as a Plan B in the event of a technical loophole or an incident affecting the other platform, where we would have to fall back on Zoom as a Plan B.

What would be the main drawbacks of using Zoom as a voting platform for the taking of a recorded division where the person is identified and says yea or nay and, then, it's the next person's turn? Time-wise, it would take longer than the15 minutes we have in the House. Have you identified any drawbacks?

Mr. Stéphan Aubé: As things stand, the members would have to decide to go ahead with that method to start, but I'll ask André Gagnon to answer that question. We don't see any technical issues with doing it, except in terms of taking the time necessary for the vote. We haven’t done the testing yet to assess how long the process would take. It is something we’ll be examining, though, so the process is as efficient as possible.

🕐 (1325)

Ms. Christine Normandin: I see that Mr. Gagnon’s mic is on. Would you like to add to Mr. Aubé’s comments?

Mr. André Gagnon: I feel obligated to answer because of Stéphan.

I would add that the two methods we are referring to each have their pros and cons. The upside of the voting method the chair was referring to, in other words, voting while the bells are ringing, is that members could basically vote from their platforms and, using elements in front of them, vote on each of the motions on which a question is put. That means it’s possible to vote during the half-hour bell and even to vote on different questions.

As you know, on numerous occasions, a number of votes are taken successively, one after the other. That is one option, then, to make it easier for members to vote on various motions. It would also be over a longer period of time. When it came time to take the vote, if there were any technical issues, which don’t always last 30 minutes, it would increase the likelihood of voting, unlike voting by facial recognition, which has been mentioned, because it happens at a specific moment in time. If all 338 members of Parliament are online, it makes things more difficult.

Ms. Christine Normandin: Thank you.

[Traduction]

The Chair: Thank you.

Ms. Blaney, please.

Ms. Rachel Blaney: Thank you.

Mr. Aubé, I'll come back to you. You mentioned, I believe, in one of your answers that you're looking to set-up a task force to look at some of these processes with members. I'm wondering how that is and if every recognized party would be included in that task force.

Mr. Stéphan Aubé: I'm sorry, I didn't quite hear the start of the question.

Ms. Rachel Blaney: I think you mentioned in one of your responses that there would be a task force of members to look at some of these processes, and I'm just wondering if all recognized parties would be included in that.

Mr. Stéphan Aubé: If I said that, I want to correct it. What I meant is that if we were asked to consult with the parties we would be open to that, for the interface perspective.

If ever we engage with members on any system we build for them, our usual process is to engage all parties. If we were asked to do that, that's what we would do.

Ms. Rachel Blaney: Thank you so much.

One of the things we had a lot of discussion about today is how we assess risk and how we adjust to any risk that may arise, especially as we look at having a more virtual Parliament potentially in the future.

How do you report back to the parties about what risks may arise and how do you evaluate them and get that information out to the members?

Mr. Stéphan Aubé: As it relates to risk, as a first step our goal is to assess and document these risks. **. Once documented, they would certainly be shared with the Speaker's office as a first point, and I would leave it to the Speaker to decide how to share it with the political parties.

That would be the approach we would use. We would go through the Clerk, and then the Clerk through the Speaker's office. However, if there are risks, we would certainly make sure the Speaker is made aware so they can be shared.

Ms. Rachel Blaney: Thank you.

Those are all the questions I have.

The Chair: Thank you so much, Ms. Blaney.

Thank you to all the witnesses.

That ends our rounds of questioning for this meeting. We're going to stay in camera while the witnesses leave, so we can discuss some committee business. Thank you once again to the whole team. We really appreciate all the time you give this committee.