HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

43rd PARLIAMENT, 2nd SESSION

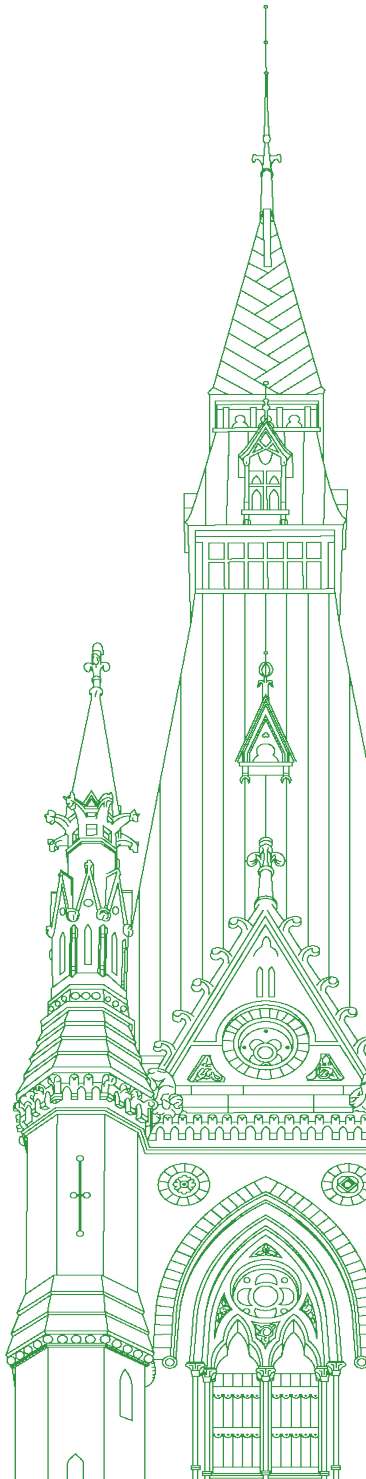
Standing Committee on Government Operations and Estimates

EVIDENCE

NUMBER 013

PUBLIC PART ONLY - PARTIE PUBLIQUE SEULEMENT

Wednesday, December 9, 2020



Chair: Mr. Robert Kitchen

Standing Committee on Government Operations and Estimates

Wednesday, December 9, 2020

● (1535)

[*English*]

The Chair (Mr. Robert Kitchen (Souris—Moose Mountain, CPC)): I'll call the meeting to order.

Welcome to meeting number 13 of the House of Commons Standing Committee on Government Operations and Estimates. The committee meeting today will be from 3:34 your time, until 5:34 your time. We will hear witnesses as part of the committee's study of the Nuctech security equipment contract, and then discuss committee business in camera at the end of the meeting.

To ensure an orderly meeting, I would like to outline a few rules to follow.

Interpretation in this video conference will work very much like in a regular committee meeting. You have the choice at the bottom of your screen to use either floor, English or French, for those who are here virtually. We would ask that you choose the language you are going to speak in when you do so.

Before speaking, please wait until I recognize you by name. When you are ready to speak, you can click on the microphone icon to activate your mike. When you are not speaking, we ask that your mike be muted.

To raise a point of order during the meeting, committee members should ensure their microphone is unmuted and say “point of order” to get the chair's attention.

In order to ensure social distancing in the committee room, if you need to speak privately with the clerk or analyst during the meeting, please email them through the committee email address. For those people who are participating in the committee room, please note that masks are required unless seated and when physical distancing is not possible.

I understand we have some opening statements from our witnesses today. I appreciate that. They will be provided five minutes.

Right now, I will invite the Council of Canadian Innovators to make their opening statement.

Mr. Benjamin Bergen (Executive Director, Council of Canadian Innovators): Mr. Chair, honourable members, thank you for the opportunity to present today.

I'm Benjamin Bergen, executive director of the Council of Canadian Innovators, or CCI, a national business association that represents more than 130 of Canada's fastest-growing technology companies. Last year alone, our members employed more than 40,000 Canadians and generated more than $6.5 billion for the domestic economy.

I'm joined today by Neil Desai, a senior executive with one of CCI's member companies, Magnet Forensics. Neil is an expert in cybersecurity and public procurement policy and will have much to contribute to today's discussion. For my part, I'll focus my comments on the role that procurement can play in supporting the growth of Canada's homegrown companies.

As your 2018 report on modernizing procurement stated, the Government of Canada is the biggest customer of goods and services in the country, and the procurement system has the opportunity to be a much larger driver of economic prosperity. In the global innovation race, having the Canadian government as a purchaser of goods and services is considered a major validator for domestic companies. It helps them to accelerate future sales with other governments around the world, which in turn enhances Canada’s innovation export potential.

We are all abundantly aware of the issues the federal government has faced with procurement in recent years, especially when it comes to buying technology systems. The Phoenix pay system, the Government of Canada website renewal project, and now the X-ray machines for Canadian embassies, have each become matters of national interest, and for all the wrong reasons. The end result is billions of dollars paid to foreign technology firms that have failed to deliver on what they promised.

Canada's current approach to procurement lacks a strategic economic development lens, which has a direct impact on the economic opportunities for domestic innovators who wish to help their governments defend physical and digital borders. This all has a negative impact on both our prosperity, and more importantly, national sovereignty.

I'd now like to turn it over to Neil Desai for his opening comments.

Mr. Neil Desai (Vice-President, Corporate Affairs, Magnet Forensics, and Senior Fellow, Munk School of Global Affairs and Public Policy, Council of Canadian Innovators): Thanks very much, Ben.

Thanks to members of the committee.

Magnet is a Waterloo-based cybersecurity company that provides digital investigation software solutions that are used by over 4,000 police, national security and other public and private entities with investigative authorities in 94 countries.

We're proudly Canadian and thankful to call a dozen federal organizations our customers, but I should point out that Canada accounts for about 5% of our business.

The challenge we see with federal procurement in the security sector is the lack of a strategic lens. First and foremost, the government continues to buy modern tech, largely software, the same way it purchases office supplies, through lengthy RFI and RFP processes that are focused on what is believed to be the lowest price of a static product, versus the best value delivered through a solution that will evolve to develop benefit over a long time horizon.

Modern software is highly iterative technology. It can solve key problems, but it can also create grave ones if it's not developed and purchased with foresight and a focus on value. Leading global governments in procuring security solutions acknowledge this, and allow their front-line experts to work with their innovators much earlier in the development cycle. They also keep a close eye on the potential for such solutions to be exported.

This isn't to say that these governments don't buy foreign technology, but they assess the risk and consider the prosperity opportunity. They use national security and small business exemptions in their trade agreements. They also use non-tariff barriers such as security clearances and government expectations, to ensure that the solutions they procure are trustworthy and deliver economic spillovers. They also shorten procurement to align with imperative development cycles, allowing pivots and off-ramps to avoid massive failures.

The concern I'm expressing here today is less from a business-operator perspective and more from a proud Canadian vantage point.

Cybersecurity is the nexus of prosperity preservation and creation with geopolitical conflict and criminal activity. If we, as a country, don't update our playbook soon, we risk being left behind.

I'd be happy to animate the themes I've covered with some tangible approaches to a Canadian-made technology procurement strategy.

Thanks very much.

● (1540)

The Chair: Thank you.

Now we'll hear from Mr. Buric for K'(Prime) Technologies.

Please go ahead for five minutes.

Mr. Sime Buric (Vice-President, K'(Prime) Technologies): Thank you, committee members.

My name is Sime Buric, and I am the vice-president of K'(Prime) Technologies.

K'(Prime) Technologies is a Canadian-based company based in Calgary, Alberta. We employ approximately 40 people across the country. Our CEO, Kham Lin, and our CFO, Amanda Lin, started the company 22 years ago. The company was founded as a sales and service provider for the analytical testing and security market. We are a for-profit organization that is not subsidized by government. To be competitive, we need a fair playing field.

I want to start by saying that we share the views of prior witnesses, such as Mr. Burton, Mr. Mulroney, Ms. Carvin and Mr. Leuprecht. We are one of the companies that submitted a response to the tender. A lot of the issues that OGGO is discussing now are issues that we brought up when we challenged the awarding of the standing offer. We followed the only avenue we had to challenge the awarding by submitting a complaint to the Canadian International Trade Tribunal.

One of the concerns that we brought to the CITT was the question of how Nuctech could meet the Canadian regulations when submitting bids. We provided examples of many global news articles and decisions against Nuctech for some questionable practices. We expressed our concern about competing against a state-owned company. VOTI Detection—which I'm glad to see is on this witness panel—another Canadian company that bid on the tender, also expressed concerns about Nuctech. In a newspaper article, VOTI also expressed concerns, knowing how the equipment and the hardware could be significantly cheaper—up to 25%.

Another concern that I brought to the attention of the tribunal was the stretching of the truth when it came to the abilities of the technology to automatically detect weapons and other potential threats. All the X-ray systems run on a similar principle. The systems that were quoted were all of a single-view type, meaning a picture from one angle. The probability of accurately identifying a specific threat—like the difference between a gun, knife or bomb—with a single-view system is low, but the specification was not removed or revised. A single-view system is not meant to replace the use of visual inspection of a package. It is meant to be a complementary technique.

The X-ray systems differentiate threats based on atomic mass. Therefore, a colour is applied to the screen to identify a material, whether it's a metal, liquid or organic material, etc. If the premise is to reduce the amount of visual inspections, a dual-view system or a CT-based system is necessary, but these require a higher investment and are similar to what CATSA uses at the airports.

Unfortunately, these concerns were not investigated further, and our complaint on the matter was disregarded. Based on the decision by CITT, it was recommended that we be charged $575 for the challenge.

I personally have over 14 years of experience in responding to government tenders. This was one of the more difficult tenders to respond to, as there were a lot of unrealistic hypotheticals in terms of the number of units required per global region. When I would respond to any previous tenders, the specifications were clear and concise. The number of units was specific or a price per unit and a standing offer issued over a specific number of years. The locations where the units were to be installed were specific.

These are just a few examples of some of the hurdles presented when responding. As this tender was based on hypotheticals, it made responding to the tender more difficult than it had to be. Companies that are for-profit organizations then have to uplift or pad their pricing to make sure they do not lose money in different regions.

There are a lot of security concerns that have been discussed in previous committee meetings. It has been mentioned a couple times that X-ray equipment would be a low to medium security threat. Yes, electronic modifications can be done after the fact by a service person or by anyone else who has access to the equipment, but we also need to question whether there's a security threat coming in with the system. Who tests whether there's a back door, malware or any other security vulnerability in the system prior to deployment?

We at K'(Prime) Technologies are responsible for the maintenance of X-ray equipment at many airports across the country. In order to provide this service, we are required to have a restricted area identity card, which is an application that is reviewed and approved by Transport Canada, to get access to the equipment. However, in order to service equipment at the embassies, no clearance is necessary.

As a Canadian citizen representing a Canadian company that employs Canadians across the country, I am here to say that we are looking for our government to provide better procurement standards, and for matters of security to be reviewed at a higher level with interdepartmental collaboration. This could hopefully prevent the government from spending taxpayers' dollars on expensive reviews by external companies when there are resources available internally, like the Canadian Centre for Cyber Security.

● (1545)

Canadian companies need to abide by ethical and legal standards to compete for business. We want these standards to apply to all non-Canadian organizations that want to do business in Canada. When it comes to security, reviews of companies need to be done ahead of reviewing tender responses, to exclude companies that do not meet the Canadian standard.

I thank you for your time and welcome any questions.

The Chair: Thank you very much.

Now we'll go to Mr. Olson with VOTI Detection, please.

Mr. Olson, you have five minutes.

Mr. Rory Olson (Chief Executive Officer, VOTI Detection Inc.): Thank you very much, Mr. Chairman and honourable members. Thank you for this opportunity to address the committee on issues that I believe are of critical importance to VOTI Detection and the Canadian business community.

In my remarks I will address three main issues that I believe are relevant to your hearings, and it would be my pleasure afterwards to take any questions you might have.

First, as president and chief executive officer of VOTI Detection, I stress our support for the competitive bid process in public procurement. We welcome the opportunity to offer best-in-class technology to address the needs of our potential clients, while offering tremendous value for money. VOTI Detection believes the procurement opportunity that was managed by Public Services and Procurement Canada for the benefit of Global Affairs Canada followed all the rules in place at that time.

Our request of policy and decision-makers is the consideration of changing some of those rules. The only thing we ask for is the opportunity to participate in the bid process on a level playing field. We believe it is virtually impossible to have a level playing field when companies that are state-sponsored, with a history of predatory pricing practices, are allowed to participate. There should be a vetting of companies to ensure that they have the ability to deliver all the commitments in their bid while respecting the high ethical standards of business governance.

Our belief is that any company that has been disqualified from procurement opportunities for security reasons by our closest allies or known to have engaged in illicit and corrupt practices such as bribery and honey trapping should be excluded from Canadian government bid opportunities. It is our hope that the bid authorities will embrace opportunities to consider the value of benefits other than a low price in the evaluation of submitted bids.

The second issue touches on security considerations related to the acquisition, deployment and ongoing maintenance of X-ray security scanners. While we understand that the security scanners will not be connected to any network, we also understand that the scanners will record and store data that should be kept highly confidential. Although the data will not be vulnerable to a network attack, whenever a technician—a simple technician—is required to perform preventative maintenance, a software update or the servicing of a defective part, there would be ample opportunity for that technician to download the sensitive data that should be protected and send it to wherever that person wishes.

The security value can go beyond the actual technology. Companies and the individual employees who will participate in the fulfillment of the procurement opportunity could, and should, receive security clearances based on reliable and verifiable information.

The third point is to stress the importance for Canadian business to find government support through public procurement, especially during these very difficult economic times. I believe small and medium-sized businesses are the backbone of the Canadian economy and the greatest opportunity to stimulate sustainable growth. There is no support that is more valuable that a government entity can give to a Canadian business than a purchase order. Procurement of Canadian goods supports domestic industry as well as the important downstream supply chain. These businesses employ Canadians, and it is through the fulfillment of purchase orders that businesses can grow, continuing to invest in growth strategies, research and development and the creation of additional jobs for Canadians.

VOTI Detection employs over 80 people across Canada. These are high-paying research and development jobs with fundamentally superior IP in technology to any of the competitors in its class. These are things that should be taken into account and considered when going through any type of procurement process.

In conclusion, it's my hope that this committee will shape policy that will support better outcomes for the Canadian government, their departments and agencies, and for the Canadian people. It is my belief that, when possible, the promotion of a Canada-first or buy-Canadian procurement strategy would generate positive outcomes for all involved.

● (1550)

Again, Mr. Chairman and honourable members, I thank you for the opportunity to address you. I make myself available for any questions you might have.

The Chair: To all the witnesses, thank you for your presentations and for staying as close as you could to the allotted time. It was much appreciated.

We will now go into questions and answers.

Mr. Paul-Hus, you have six minutes.

[*Translation*]

Mr. Pierre Paul-Hus (Charlesbourg—Haute-Saint-Charles, CPC): Thank you, Mr. Chair.

I'll start with Mr. Buric.

Mr. Buric, you said that you've been responding to government tenders for 14 years. There's an issue right now. My Liberal colleagues are a bit defensive when it comes to Nuctech, and they're laughing at us a little. However, in Canada, we have a much more serious procurement issue. I imagine that you saw our meeting with government officials, who didn't seem concerned about procurement security. I want to hear your thoughts on this.

[*English*]

Mr. Sime Buric: In my opinion, when it comes to security, anything when it comes to the embassy has to be taken into the same account as any other high-risk area—for instance, the airports that we work at. Information is travel. People are travel. People go through. All of these, whether the risk is low or not, are still security threats. That has to be taken into account in any type of security response or tender.

All of those have to be applied to the same level when it comes to the procuring of hardware.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

I'll continue along these lines. You said that responding to tenders has never been more complicated and that the process is unclear. The tenders are sometimes tailored toward a provider.

Do you think that these tenders were designed so that Nuctech could respond to them more easily than your company, for example?

[*English*]

Mr. Sime Buric: I can't respond on whether or not it was tailored toward a specific provider. What I can say is that, based on hypothetical numbers and the quantities that were being requested by specific regions, it was not realistic based on how many embassies are in those specific regions. When a contract gets awarded for a specific dollar value, when you have a lot of hypothetical quantities of equipment, it is very difficult to say what that final contract will be. When people say it's awarded at specific million-dollar amounts, it's not realistic. Therefore, you start getting budgets that get blown out of proportion, and costs start to creep up.

● (1555)

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

My next question is for you, Mr. Olson. In your presentation, you spoke about security breaches in Nuctech's equipment. Your colleagues in the government tried to say that there wasn't any issue, because the equipment wasn't directly connected. However, you confirmed that a company technician, while performing maintenance, could take the information recorded on the hard drives and copy it. Is that right?

[*English*]

Mr. Rory Olson: There is the potential for a security breach as a function of the machine being required to be maintained. From that maintenance visit, a maintenance technician could easily download all of the information on the hard drive.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you.

I want to point out to the committee that I have a document from the United States Department of Homeland Security dated November 2020. Paragraph 13 confirms that it's very easy to steal data from Nuctech's devices and that this poses a security issue. Our American colleagues confirm that there's a security issue in this area.

I have some time left, so I'll turn to Mr. Bergen.

Mr. Bergen, we discussed the purchase of foreign technology. You said that Nuctech is another example in a series of failures in our procurement system and that billions of dollars were paid to foreign technology firms that failed to deliver on what they promised.

Can you tell us more about this? When you talk about billions of dollars, how many companies and individuals are involved? Can you elaborate on this?

[*English*]

Mr. Benjamin Bergen: My comments really speak to the fact that when you look at how procurement is done in this country, often you see foreign firms bidding but sometimes not actually delivering on what they're promising. We saw that with the Phoenix pay system. We've seen that with the government's website renewals and we are seeing it now with Nuctech in terms of X-rays.

I think the thread that pulls these pieces together is really more the strategy and the policy that we have with regard to procurement. I read over the comments from the committee on the 18th, and if you look at what Assistant Deputy Minister Ieraci and Assistant Deputy Minister Danagher stated, it's about lowest cost and it doesn't take into account other externalities and factors that are critical when thinking about public policy. You need to take into account national security—obviously it is an important piece—but also the opportunity to create prosperity through an economic driver, which is the government actually being a purchaser of these products.

Neil, would you like to add anything to that?

The Chair: Neil, if you have anything further that you might be able to add, could you put it in writing? That would be greatly appreciated. Thank you.

Due to time constraints, we need to continue.

Mr. Kusmierczyk, you have six minutes.

Mr. Irek Kusmierczyk (Windsor—Tecumseh, Lib.): Thank you very much, Mr. Chair.

This government takes cybersecurity very seriously and in budget 2018 committed $500 million over five years for a national cybersecurity strategy. A big pillar of that cybersecurity strategy is to help build up domestic research and innovation capacity. This means making investments to help Canadian tech companies, innovation companies, grow and scale.

You can look, for example, at the $10 million that was given last year to the Rogers Cybersecure Catalyst program in Brampton. This was a partnership with Ryerson University. You can look at the $41 million in investment through FedDev, again in quantum projects, cybersecurity projects related to quantum at Waterloo. This was through Quantum Valley. There was $49 million of FedDev funding that was leveraged to create a cybersecurity centre in Vancouver. My point is that this government is making significant investments in tech companies and in innovation locally.

I wanted to ask Mr. Bergen whether we're on the correct path in terms of making these significant investments in domestic Canadian cybersecurity tech companies to help us address some of the threats we're facing.

● (1600)

Mr. Benjamin Bergen: I think we're confusing two pieces here. Obviously funding research and development and cybersecurity is a positive step and the government should continue to do that. However, it is somewhat absurd when we don't have that same government actually go and buy that domestic technology to defend its borders. That really is the articulation of the challenge we're seeing with new technology right now. We could potentially have Canadian companies that have received things like SR and ED or IRAP or other funding, but then are not the actual company that's being purchased from.

Although it is all well and good for us to spend money on research and development, if we're not actually commercializing and building that capacity through companies in this country, it's a bit of a wash.

Mr. Irek Kusmierczyk: I appreciate that and I understand also the role of procurement in helping these companies once they're scaling and growing to be able to scale further.

As you are probably aware, the Government of Canada has a program called the industrial and technological benefits policy, through which, for large defence procurement contracts, for example, the government can stipulate that, as part of the conditions of the contract, the company that's awarded the contract has to provide economic activity in Canada up to the value of the contract itself. Among the 14 key industrial capabilities that we're targeting are cybersecurity and cyber-resilience, for example.

Is this government's industrial and technological benefits policy program one of those pillars of procurement that you would support and that you think plays an important role in helping Canadian companies locally?

Mr. Benjamin Bergen: Neil, would you like to answer that question?

Mr. Neil Desai: I'll jump in here and just say that these are all really great initiatives, and cyber is a real problem, but we also need to have a scaled understanding of the challenge and then work from there.

I'm going to one industry report. McAfee, a global player in cyber, has done independent research on this. They see cybercrime as growing from a $600-billion global problem two years ago to a $1-trillion problem this year, and they expect it to accelerate because of COVID and the number of vulnerable populations online.

Just on differentiating between economic development, things like the programs you mentioned in the previous question, and ITBs and procurement, I don't think we should consider procurement as a handout. I don't think anyone I heard during the opening statements was looking for favouritism.

What they are looking for is a level playing field, and I'll just say from a purely economic development perspective, a purchase order of $1 million is much greater in terms of its knock-on effects to the economy than $1 million of economic development programming. It validates the technology and its usability in the field, and frankly, we have to be cognizant that Canada is a very well-respected country globally. We make up about 2% of GDP and roughly the same amount of cybersecurity consumption, so the opportunity of domestic procurement—and the Government of Canada is one of the largest purchasers of cybersecurity tools in this country, along with the banking sector and other sectors—is not only to solve the narrow problem within government. It's to give an incredible launch pad to cybersecurity companies.

Frankly, we shouldn't look at size of company as the only measure of capability. We should get deep into the capabilities they have. Large system integrators, big companies—and I won't name them here—often have the balance sheet and lobbyists to withstand long RFI and RFP processes that are multiple years when they, in fact, don't have the technological capability.

Maybe we need to get a a lot clearer on what we're trying to achieve in procurement and create smaller bite-sized procurement processes we can get through, and then validate technology and start responding to problems the way technology is built and not the way procurement is built.

● (1605)

Mr. Irek Kusmierczyk: I appreciate that, Mr. Desai.

Just to go on record, I worked for a regional innovation centre, much like Communitech, for eight years. I'm a big believer in Canadian tech. I know we have world-class talent and companies here, and I agree with you wholeheartedly. The point I was trying to make was that this government has been there for Canadian companies, whether it's through making investments in companies directly as they grow in scale or by having robust procurement policies like the industrial technological benefits program, which is, as you're saying, providing support through the Canadian procurement process. I'm a big believer in Canadian tech. It is world class.

The Chair: Thank you, Mr. Kusmierczyk, I appreciate that.

Ms. Vignola, you have six minutes.

[*Translation*]

Mrs. Julie Vignola (Beauport—Limoilou, BQ): Thank you, Mr. Chair.

Should the bidders' calculations include a calculation that reflects the subsidies received by the company to submit a bid?

We know that Nuctech is highly subsidized and that, as a result, the company can submit low bids. Should there be an additional provision that includes the subsidies that enable companies to lower their costs?

The issue is a matter of popular opinion. Mr. Olson, you can go first.

[*English*]

Mr. Rory Olson: I think it would be extremely difficult to calculate what the degree of subsidy is relative to a given contract. A company like Nuctech is fully sponsored by the Chinese government, and as such, the financial commitment that the Chinese government has made is endless. There is nothing finite about it, so anything they do.... We have been in bids against Nuctech around the world, and in these reverse auctions, they will just continue to go lower and lower and lower. There is absolutely no floor. How do you quantify what the value of the subsidy is and then offset that and add it back to their price?

It would be extremely difficult, in my opinion.

[*Translation*]

Mrs. Julie Vignola: Thank you for your straightforward answer. I greatly appreciate it.

A number of foreign companies, especially Chinese companies, have representatives in Canada who are Canadian citizens. I'll focus on the Chinese companies.

As you know, in 2017, the intelligence law was enforced. This law required every Chinese citizen to provide information to the government.

In your opinion, if a Canadian citizen is hired by Nuctech, are they also subject to China's 2017 law?

[*English*]

Mr. Rory Olson: Is that a question for me?

[*Translation*]

Mrs. Julie Vignola: If you can answer it, yes, Mr. Olson. If not, perhaps Mr. Buric could answer it.

[*English*]

Mr. Rory Olson: Go to Mr. Buric by all means. I'm not qualified to answer.

Mr. Sime Buric: I'm not an expert in government policy, especially foreign government policy, so I can't comment on that.

[*Translation*]

Mrs. Julie Vignola: Mr. Bergen, can you answer my question?

[*English*]

Mr. Benjamin Bergen: I'm not able to comment on it, but it is an interesting question for sure.

[*Translation*]

Mrs. Julie Vignola: Thank you.

[*English*]

Mr. Neil Desai: Maybe I could provide some...not to the specific, but to the general question being asked.

As a Canadian company trying to sell in 94 different countries, as you move up market in security, significant questions come from foreign governments, such as how many nationals you employ, or if you have a separate board of directors for that country where the majority of members of that board of directors are nationals of that country.

As you, again, move further up the security spectrum in terms of risk, then it becomes “Is the development for this product done in country? Can it be validated in country? Would there be opposition to that if the deal size got to a certain level?” Among astute countries in the cybersecurity and broader security space, there's usually a risk opportunity matrix in the policy, where they have expectations of the vendors that increase as the risk increases.

● (1610)

[*Translation*]

Mrs. Julie Vignola: Mr. Olson, do you have anything to add?

[*English*]

Mr. Rory Olson: I'd like to add that small companies like ours spend many millions of dollars a year developing their research and development. To be sure, a minuscule amount comes back to us through SR and ED and other potential subsidies, but not nearly what we put out. To look at the fact that a Chinese company, or any other company, can just hire a couple of people here and all of a sudden that makes them on par with a Canadian company deploying and spending millions, employing hundreds of Canadians, creating and participating in the economic ecosystem and supply chain, I don't see how that equation could ever work out.

[*Translation*]

Mrs. Julie Vignola: Thank you.

Mr. Desai, in your opinion, should the government automatically implement security provisions when purchasing equipment with electronic components?

I'm talking about high-security provisions.

[*English*]

Mr. Neil Desai: I think it really depends on the type of technology being procured and where the security risk assessment is done. I think other witnesses have talked about leading agencies within the government context that have those technical skills to review the nature of a procurement and what the security risk is and then what mitigation should be put in within the procurement program.

I feel as though we're focused in very narrow lanes when it comes to procurement. It's buying at the lowest cost and then security is a separate consideration after the fact. Economic development is another consideration for another group of people at ISED. I think we need to be able to walk and chew gum in our public policy. We need to start looking at them as competing priorities but ones we want to reconcile. We're never going to get it perfect but we need to consider them through the procurement and also start looking at them as highly iterative. The actual technologies are built in an iterative way but the procurements are not. They are long—

The Chair: Thank you, Mr. Desai. I apologize for interrupting you.

Mr. Green, you have six minutes.

Mr. Matthew Green (Hamilton Centre, NDP): Thank you.

The first question I have is for VOTI. I understand that you provide technologies through your partners, through X-rays and security solutions. I believe you have a contract with CBSA, and I'm just wondering if you'd care to expand on the services you provide CBSA.

Mr. Rory Olson: We've supplied CBSA, in response to a tender, with X-ray machines, smaller tunnel-size 60-40 machines and one-metre-by-one-metre tunnel-size machines. We have provided them with quite advanced technology per their request. We worked very much hand in hand with them, and we continue to. I believe the fruits of that labour will have bestowed great benefits for CBSA in terms of their detection capability.

● (1615)

Mr. Matthew Green: That's a good opportunity for a good sales pitch there. Obviously you were successful in that bid. In your opinion, based on the discussions that we're having here, if Nuctech had also bid on that similar technology, do you believe that, based on CBSA's procurement, you would have been underbid and potentially would have lost that contract as well?

Mr. Rory Olson: Yes.

Mr. Matthew Green: Can you comment on the differences between the two? Was it the RFP or the RFQ that pre-qualified you in a different way? Are there any distinctions between the two bidding processes that you might be able to highlight for this committee?

Mr. Rory Olson: I don't even know if Nuctech bid on that.

Mr. Matthew Green: That's fair.

The question I had for K'(Prime) when I was floating around there in the beginning was about the millimetre wave technology, which I saw on their website, that they offer to their partners. Is that specifically for X-rays or is that also transistors and other big stuff?

Mr. Sime Buric: Millimetre wave technology is a complementary technique. It's meant for body screening. It allows for screening of anything through clothing material. It doesn't penetrate your skin, so it's not meant for packages. This technology we are bidding on right now is a human screening technology.

Mr. Matthew Green: This is tangential, only for my own personal information because I'm interested in the conversations about Huawei. What application does it have to 5G?

Mr. Sime Buric: Currently, it's not connected to 5G in any way in terms of how the technology is being used.

Mr. Matthew Green: Okay. Maybe I misread some of my research notes. I'll have to get a better sense on that because I imagine at some point in time we'll be talking about 5G once again.

This is for K'(Prime) as well. Given that you were unsuccessful in your bid, you filed your complaint with the CITT. Into which specific aspects of the federal government procurement processes for security screening equipment did you want the tribunal to conduct an inquiry?

Mr. Sime Buric: We put our concerns on three different areas. In one area we spoke about the technology itself and how the technology that they were trying to apply outreached its capabilities in terms of the likelihood of differentiating between different types of threats, whether a gun or knife.

Another one we had was the concern of Nuctech being a subsidized state-owned company, with all the questionable practices. We provided a lot of newspaper articles from around the world in terms of some of the allegations. Basically, we brought to attention the information that they found to be true in terms of bribery, but the information was deemed not sufficient to go further.

The last one we brought up was about wanting to know the logistics of how to move equipment around the world. We stated that we use companies like FedEx or UPS, known suppliers of transporting goods, but they started knocking down points on how this was supposed to be done. Our response was that we work with our partners. That wasn't sufficient, so we challenged that response as well.

Mr. Matthew Green: Am I to take and infer from that you are not satisfied with the review completed by the tribunal, or do you agree with its statements and reasons for its determination?

Mr. Sime Buric: We are not in agreement, but we are accepting the outcome currently.

Mr. Matthew Green: That is extremely diplomatic of you. I do certainly appreciate that.

Is there anything else you want to add right now with K'(Prime)?

Mr. Sime Buric: Not at this time, thank you very much.

Mr. Matthew Green: Out of curiosity, what's the relationship with L3Harris?

Mr. Sime Buric: We have a relationship with L3Harris, but it's no longer with L3Harris—it's with Leidos—where we are their service arm for the airports. We provide the servicing of the X-ray equipment for multiple airports across the country.

Mr. Matthew Green: Thank you very much.

The Chair: Thank you, Mr. Green. I appreciate that.

We have now finished our first round. We will go into our second round. We'll start with Mr. McCauley for five minutes.

Mr. Kelly McCauley (Edmonton West, CPC): Thanks, Mr. Chair.

Witnesses, thank you very much.

Mr. Olson and Mr. Buric, I'm sure you watched previous OGGO meetings regarding Nuctech. We know Nuctech is not going to get the contract now. I'm sure we'll go through the paperwork and their standing offer will be revoked.

Have you been approached yet for a rebid on this equipment or on this contract?

● (1620)

Mr. Rory Olson: No, VOTI Detection has not been approached for any rebid or given any information about a rebid.

Mr. Kelly McCauley: That's very strange.

I have a question for Mr. Olson and Mr. Buric. We've heard a lot about the problems of dealing with state-owned enterprises and the unfair subsidies they've received. Have you run up against this issue in other private sector bids or bidding for other government, provincial, Crown corporation or federal government contracts?

Mr. Rory Olson: Mr. Buric, you can go first.

Mr. Sime Buric: Depending on the region, if it's in the U.S. we've seen it on some private ones. Obviously price is usually the winning factor on a lot of these because everybody wants the lowest bid.

Mr. Rory Olson: In the other bid opportunities where we have seen Nuctech in other countries outside of North America, while they were given an initial status as being a bona fide bidder, they were subsequently removed as such.

Mr. Kelly McCauley: I want to get back to the security issue of this. When we had Global Affairs and PSPC, basically they all just shrugged their shoulders and said that it wasn't a security issue, and they didn't know it or see it as such, but very clearly it was.

We paid Deloitte a quarter of a million dollars of taxpayers' money for basically a four-page double-spaced report saying, don't buy security equipment or reconsider buying security equipment from the Chinese government.

How should we be proceeding with our technology and our security procurement? Should it all run through a tick-off of the CSE, CSIS or other security departments within the government? Obviously, just leaving it up to the departments is not going to work.

Mr. Rory Olson: Listen, I'm not sure what the correct process is. I'm not a security expert and I'm certainly not an expert in the internal workings of government and best practices, but there are certain things that are so obvious that—

Mr. Kelly McCauley: It didn't need to take a quarter of a million dollars to state the obvious.

Mr. Rory Olson: It certainly didn't need to take a quarter of a million dollars to tell you something, frankly speaking, that should have been quite obvious to everybody, and it was. The attempt to make it obvious to everybody was certainly something that was attempted.

Mr. Kelly McCauley: Mr. Buric and Mr. Desai, one of my Liberal colleagues, Mr. Kusmierczyk, was talking about the ITBs and how great they are, etc. We laughed when we heard that, about a year ago for the Irving ITB obligations, they invested in a french fry factory in Alberta.

At what level should your association be involved in the government to perhaps advise or assist them on how we should be doing these ITBs so that the benefit is not being just pushed away as some throwaway investment, so that it's actually delivering real value to Canadians?

Mr. Neil Desai: I think a proper study on the number of ITBs that have actually been deployed for the specific-purpose or general-purpose technology that's being offset with a foreign piece of technology would be good. I think it's sometimes burdensome to force companies to try to find something in Canada that will work. Making sure that it's generally in the line of security would actually help the economic development piece.

However, an ITB, again, is really trying to create a local economic stimulus. I will go back to pointing out that, in some cases, when a Canadian company can fulfill a procurement and is being kept out for arbitrary reasons, or for unfair business practices from foreign players, I think we have to solve the narrow problem before we try to look at these big structural issues.

I'm blending into your previous question because it's a really important question. The separation between the subject matter expert in security and the procurement process is so wide, there is such a separation. I understand why. You want to make sure you have a fair, transparent process to make sure government money is being spent well. However, the reality of technology is that you need subject matter experts to review things like security, things like the governance of technology and how updates will be delivered. The only way to solve for that is to bring the subject matter expert closer to the procurement process.

I think the procurement officers do their best with what they're given, but there's such a time lapse and separation between those independent procurement officers and the actual technical problems to be solved. We have to figure out ways to get that transparency, but with those subject matter experts in the process to review the tech.

● (1625)

The Chair: Thank you, Mr. Desai.

Now we will go to Mr. Drouin for five minutes.

Mr. Francis Drouin (Glengarry—Prescott—Russell, Lib.): Thank you, Mr. Chair. I want to take the time to thank all of the witnesses who are before us at this committee.

My first questions will go out to K'(Prime) Technologies, and to VOTI Detection if it applies.

I wasn't sure from your testimony whether or not you—and I know this was brought to CITT—were on the standing offer. I would like a yes or no as to whether or not you were on the standing offer.

Maybe we could start with Mr. Buric.

Mr. Sime Buric: We were not on the standing offer. We were not in that final group.

Mr. Francis Drouin: Okay.

What about Mr. Olson?

Mr. Rory Olson: I do not know the answer. I'm sorry.

Mr. Francis Drouin: Okay.

It would probably be normal if government hadn't reached out to those who were not on the standing offer, because there are normally three or four vendors that would be on a standing offer. Then, obviously, Nuctech has been flagged as a security issue.

Then, K'(Prime) Technologies, it would be normal that you probably wouldn't have been contacted yet unless there are major changes to the technical requirements of the particular standing offer. I know you have experience in procurement, so obviously, you would understand that. Is that right?

Mr. Sime Buric: That is correct.

Mr. Francis Drouin: Again, I'm not defending the Nuctech decision. Nobody on this committee is defending that. Have you reached out to Global Affairs or perhaps to PSPC or to whoever your contacts are in the Government of Canada to say, “Hey, we have a solution and we tried to present this solution prior to”?

Mr. Sime Buric: We have not at this time. We wanted to see where this went first.

Mr. Francis Drouin: Okay. Perhaps as a Canadian I would suggest, regarding Canadian devices, that you reach out and let them know you have a potential solution.

I'm not going to talk to the CITT ruling, because it's out of our hands. That's an independent body, and they make their own decisions.

To the Council of Canadian Innovators, you talked about leveraging procurement and what that means in this country. We often find ourselves stuck between—and this dates back 15 or 20 years or to probably before I was born—our international obligations on trade and our will to support our local businesses. Time and time again, I have had my fair share of work with IT companies that have said their first sales were to the U.S. government as opposed to a Canadian government. I find it insulting but it does happen. This is not something that is new in 2020. It's something that has been there for a very long time.

How do we fix procurement? This is something that our committee has studied in previous Parliaments. We have noticed the barriers to entry. Long procurements create a natural barrier to those companies, so what is your advice for how we can leverage that particular procurement to give that edge to Canadian companies?

Mr. Benjamin Bergen: Neil, you laid out a couple of solutions in some of your comments earlier. I'm not sure if you want to articulate them again and maybe add on to them.

Mr. Neil Desai: In the security space specifically, which is what I will talk about, because that's what I know best, I think we have to emulate and also create our own things that meet our own values and systems.

I will say that security clearance is one big piece. I will say that in other leading security technology countries there is a proactive focus on understanding the marketplace and ecosystem of technology companies, and not just understanding their technology but also understanding their technology road map, how it could be applied to public sector challenges and how that could be influenced. These things are done in a very structured way, not just as one-offs with people going out and talking to companies. It's very structured.

In the United States, there are a number of different programs, things like DARPA, the space program. In-Q-Tel is one that's offered by the intelligence community, the 21 intelligence agencies. They are less interested in procurement of a widget and more interested in a company's broad capability, its technical wherewithal and, frankly, the security and reliability of the board of directors, the executives, the key engineers and the key business people in the company.

I think these are really simple steps that we can be taking to avoid some of the challenges we're talking about here.

I will be clear about one thing. I'm not suggesting that the Government of Canada doesn't need to buy foreign technology, but if you put a strategic lens on top of the capabilities required—where there is Canadian capability versus where there isn't or where you take a longer-term value lens—a lot of these companies will win the procurements and then pad them with afterwork. That's their goal. If we look and project a bit forward and not at a static moment in time, we will get better value over the long run.

I will stop it there, Chair.

● (1630)

The Chair: Thank you, Mr. Drouin.

Mr. Francis Drouin: That's where it ends.

The Chair: Now we'll go to Ms. Vignola for two and a half minutes.

[*Translation*]

Mrs. Julie Vignola: Thank you.

I'll start with Mr. Bergen.

Innovating in Canada is expensive. Not only does it require a great deal of creativity, but also a significant amount of money. I understand that it can be very frustrating to see a company's investments overlooked to some extent.

My question is the following.

To encourage our investors, what procurement methods should the government use to keep these investments in Canada?

[*English*]

Mr. Benjamin Bergen: I may have missed a bit of what you were saying. Would you mind reiterating the question?

[*Translation*]

Mrs. Julie Vignola: Given the importance of investing in innovation—in terms of time, money, creativity and human resources—it's also critical to keep the investments in Canada.

How can the Canadian government change its procurement system to boost the return on investments made by Canadians on Canadian soil?

Could the government review the criteria, for example?

[*English*]

Mr. Benjamin Bergen: Thank you.

I think Neil might be able to illuminate some of the policy ideas behind helping to keep procurement opportunities for Canadian firms. It's a bit similar to what he mentioned in his previous comments.

Mr. Neil Desai: Thanks Ben.

I'll nuance it. I don't believe it has to favour. I think we have to be very analytical in the outcomes we want. We want to see a successful business sector for the productivity of our country. Some of the facts we have to get on the record here is that Canada spends some of the highest amounts on investments in R and D from the public sector but has some of the lowest productivity outcomes in the OECD. That's our starting point. Continuing to do that and expecting better results is, by definition, insanity.

The second piece I'll say is that when we look at the economic development work we're doing—another member asked a question about some specific examples, but there are many different ones—we also have to be cognizant that the best form of financing for any company, regardless of what they make, is a purchase order. Take it to any bank, and they'll give you much better financing terms than a government grant, a government tax credit or a zero-interest loan. I think we have to acknowledge that in our analytical constructs here.

What I would say is that, if we assess the success of the programs out there in economic development for technology-intensive businesses, let's consider how we get people in government—who are frankly, as a sector, one of the largest buyers of technology in this country—to actually try Canadian tools and technologies.

Let's also be realistic. Through grants and subsidies we are giving companies money—start-ups, scaling companies, large technology companies—through SR and ED credits. Should we not try to take something back?

The Chair: Mr. Desai, I apologize. It always seems to be you I am cutting off. I apologize for that. Two and a half minutes goes by very quickly.

Mr. Green, you have two and a half minutes.

Mr. Matthew Green: I'm learning a lot, so I really appreciate the feedback here. I'll be an expert—maybe a Ph.D.—by the time we have had five meetings on this stuff, on national security and procurement.

I want Mr. Desai to be able to finish his statement, because he talked about the disconnect between our investments and the OECD average relative to output. I think that's an important point. I would love for you to have the opportunity to expand on it a little.

● (1635)

Mr. Neil Desai: Thanks very much, Mr. Green.

The last thing I was saying is that, in these economic development programs that give grants or low-interest loans, the government should start taking the technology being built by Canadians and try to find out whether there are users in the government context. Many of our programs—even of our strategic procurement programs—are very ideological. They're either pure demand—the government has a problem it wants to solve, and that's innovative solutions Canada—or pure supply, the build in Canada program, which is when technology companies in Canada have a technology they want someone in the government to test.

The reality is that we need to play in the middle of those two, where Canadian technology vendors have something that's of value and that could potentially solve a government problem. If we get that middle ground right, I'm telling you, there will be major exports to be had and better economic growth for this country.

Mr. Matthew Green: When we look at the state capitalism of China, we've heard it characterized in many different ways throughout this committee. I'm going to suggest that it's a state capitalist country, yet we also have our own subsidies and our own preferred ways in which we provide supports here locally to business. If people had it all ways, if we were able to both maintain local production and local consumption within our supply chain in this regard and still export internationally, where do we find that balance to reconcile?

I think I heard some folks speak earlier about how this is only 5% of their business here locally.

Mr. Neil Desai: That was our business, and I'll tell you, we're not looking for any handouts here. However, I'll give you one example of the challenges that the Government of Canada faces in our software realm: investigating the extremely fast-growing issue of child sexual exploitation online, a massive, growing global issue. The same problem is happening in the U.K., the U.S. and around the world.

They all use their small and medium-sized enterprise exemptions in trade agreements. They all use their national security exemptions to work with their local innovators on solutions that solve problems such as that, or pure cybercrime investigations. That's what we're up against in a globally competitive world.

Again, I'm not suggesting that every piece of technology is going to have a Canadian vendor to solve the problem, but when there is a Canadian vendor that has technical chops and has an export potential and they get the door slammed shut on them, I just want to point out that with technology it's a winner-takes-all game a lot of times in procurement, so when you're locked out, you're locked out now for years and that launch pad is lost.

Therefore, we have to be very careful when there are Canadian players in the space and there are also security considerations.

Mr. Matthew Green: Those were very thoughtful responses. Thank you.

The Chair: Thank you, Mr. Desai and Mr. Green.

We'll now go to Mr. Lloyd, for five minutes.

Mr. Dane Lloyd (Sturgeon River—Parkland, CPC): Thank you, Mr. Chair.

This question is going to be focused on Mr. Desai.

The very fact that a company such as Nuctech could get this far in the process without anyone flagging it for security reasons is absolutely shocking, and I think it just demonstrates how our government—and maybe it has been going on for a long time—is taking our national security so for granted.

I read that the European Medicines Agency was hacked recently. They got information about the Pfizer vaccine. FireEye, the top private cybersecurity firm in the United States, was hacked. Even the cybersecurity companies are getting hacked.

I am being reassured by this government over and over again that they have a plan and that they're ready to protect our vaccine supply chains and protect our data with cybersecurity, but I'm just not convinced when I'm seeing all these countries around the world, countries similar to Canada, getting hacked and top firms such as FireEye getting hacked.

I want to get your comment. Does our government have an adequate strategy to enhance and protect our cybersecurity, and if not, why not?

Mr. Neil Desai: On the specific Nuctech stuff, I'll defer to my colleagues, but on the cybersecurity piece, the one thing I'll say, and I'll be very general here, is that, in human history, as long as people have things of value, there are unscrupulous people looking to try to get them. Digital is no different. The major nuance there is that people can act from afar and anonymize their behaviours.

The one thing I struggle with in the rhetoric around cybersecurity, both at the public and private level, is this commentary that "I am wholly secure." Then when instances such as the ones you've outlined happen, we go into PR reaction modes of, "Well, these are all the things I did." We need to be a bit more nuanced in our communications, level with people and say this is a major risk to the security of Canadians, to the prosperity of Canadians, and frankly, to our sovereignty when we talk about things such as elections, because there is no wholly secure system in the analog world, and I can tell you, I guarantee you, there isn't in the digital context.

I've often called for more of a public-private approach to Canadian cybersecurity. I'll also say that we're learning through the pandemic that things that are "essential" don't always sit in the purview of the Government of Canada, let alone the public sector. I know this committee is thinking about government operations and cybersecurity, or security generally, but we have to be cognizant that a lot of the essential systems in our society are outside the realm of the federal government and we need better public-private exchange on these subjects.

● (1640)

Mr. Dane Lloyd: Thank you.

I echo that as well. It's a very good point that there's never going to be a situation where the government spends enough or the government has done enough to ensure that we will be wholly safe from cybersecurity threats. It's a war and it's a forever war that we're going to have to keep fighting. We're going to have to keep adapting. We're going to have to keep investing in new technologies, because what we're seeing out of countries like China with quantum computing is that the threats are evolving, and we need to evolve.

For too long Canada has taken for granted that we're not going to be targeted by these state actors or criminal organizations, but it's becoming an increasingly competitive and hostile world. Don't you think it's time for the government to put forward a real strategy to ensure that we can evolve and adapt, a strategy that would lead to an application like Nuctech's being dismissed out of hand because it's common sense? We're all acknowledging on this committee that a company like that should have never been considered for this kind of contract.

Mr. Neil Desai: To me, when someone says "strategy" in a public sector context, what I believe is that it has to be horizontal in government, not vertical. What I see being called "strategy" is that they've secured this specific thing. You know, this X-ray machine meets the needs of the security of this embassy. I think we have to be a little more holistic. I don't mean that just in a Canadian context. We have to look at multilateralism and evolve it as well.

We have the Five Eyes, which I would say is one of the most effective forms of multilateralism that Canada is a part of, discussing critical issues of cybercrime, infrastructure, integrity and such. We are putting it at risk currently.

I think better conversations with our allies where we have capabilities, not just in Canada but within our tight, close allies where we have co-accreditation of technologies and of governance of those technologies, these are some actual solutions we can be looking at. Not everything is going to be able to be built under the watchful eye of the Government of Canada. We have to take a risk management approach here, not a risk avoidance approach, because we're just going to be let down at the end of the day if we have a risk avoidance approach.

Mr. Dane Lloyd: Thank you.

The Chair: Thank you, Mr. Desai.

Thank you, Mr. Lloyd.

Now we'll go to Mr. Jowhari for five minutes.

Mr. Majid Jowhari (Richmond Hill, Lib.): Thank you, Mr. Chair.

Thank you to all the witnesses. It's been quite informative.

I'll start with Mr. Bergen.

Mr. Bergen, in the closing part of your opening remarks, you talked about a strategic versus economic lens, or at least a balance of a strategic and economic lens. Also, you indicated or you predicated that the current process for procurement is more like the lowest price of a static product. You said the technology is evolving, and it's evolving quickly, and our current procurement process is not aligned with it. Mr. Desai has talked about various activities or various indicators of the fact that we're not using a strategic lens, and the last comment on a horizontal way of thinking rather than vertical is an example of that.

My question to both Mr. Bergen and Mr. Desai is this: What specific changes do we need to make to the procurement process to make it more agile as well as more horizontal?

Mr. Bergen, would you like to start?

● (1645)

Mr. Benjamin Bergen: I think I'll pass it over to Neil, given that he's already articulated some of these pieces and is so eloquent on this stuff.

Mr. Neil Desai: Thanks. I appreciate the question.

I'll get into the nitty-gritty. When we develop a piece of software, it is not static, as I mentioned. It's a 1.0. We have a road map that's very tight and, I would say, within a six-month window. There's still a road map even beyond that for up to two years. That's constantly evolving based on our users' feedback and the things we're learning about the cyber-threat landscape, etc.

In a procurement process, what we see is a waterfall list, a long laundry list of capabilities that are required on the day the RFP goes live. That list usually takes almost a year, if there's an RFI, through to the RFP. Really, most of the time when we see these RFPs, they're dated by the time they get posted, or they are actually asking for things that don't exist in the market or aren't functionally capable.

Oftentimes when we show them to users of such products in the government, they don't even know where they came from or why anyone would want those capabilities. The things they want are very specific. They have to navigate that through procurement services, where they actually list in a waterfall way what they want today, in a long laundry list, but they also know that it's going to evolve over time. Sometimes, frankly, they have to do what they know is wrong and say that they're picking things that will lead them to where they want to get to in six months.

I think there are a couple of really tangible things we can be doing. One is shortening the time, the length from information gathering through to procurement. Then, concurrently, we can be reducing the dollar amounts so that the risk isn't as high, and acknowledging how software is built—highly iterative, versioned—including opportunities to pitch road maps of technologies within the procurement process to the end-users and the technologists, not to the procurement people to be translated into jargon, but in the language that the end-users use them.

Also, then, there's understanding the landscape in a constant way. We have a procurement system that's highly responsive and not actually proactive in getting to the marketplace and understanding, first, what's out there, and second, what's possible within road maps and structures.

The last piece I'll say is that in the security phase, I think we need to do more assessment of companies and getting security clearance to the companies that have capabilities and can have capabilities in the future, so that they can work with government more hand in glove.

Mr. Majid Jowhari: Thank you.

That was the “one, two, three, four” that I was looking for. Hopefully, it will make it into our report as a recommendation.

I'm going quickly to Mr. Buric and Mr. Olson.

You guys have talked about the acquisition, installation and maintenance. In the case you talked about, the fact was that you've already installed products at CBSA.

When it comes to the maintenance, there's been a lot of concern about the possibility of data being downloaded. Is that specific only to the maintenance for Nuctech or is it a risk that's available or that you're exposed to for all products that contain data during maintenance, in that if it's not properly overseen or validated, the data may get lost?

Probably Mr. Olson can talk about that first.

Mr. Rory Olson: Sure.

The Chair: Mr. Olson, if you could respond fairly quickly, I would greatly appreciate that.

Thank you.

Mr. Rory Olson: Thank you.

It's a big question, and I'm not sure a short answer can do it.

The Chair: If you feel that it would be better to give a written response, then that would be fine as well.

Mr. Rory Olson: Fine. If someone will send me the question, I'm more than happy to put it in writing.

The Chair: Okay. Thank you very much.

That ends our second round.

In looking at the clock, we basically have 10 minutes left to do this. What we will do is that we will go to one question per party in order for the witnesses to finish at the time frames they were looking for.

We'll go to Mr. Paul-Hus for one question please.

[*Translation*]

Mr. Pierre Paul-Hus: Thank you, Mr. Chair.

Given the recent experience with Nuctech, the issue with CanSino Biotech and the situation with Huawei, we recommend that national security review all contracts with Chinese companies.

I want to hear your thoughts on this, Mr. Olson.

● (1650)

[*English*]

Mr. Rory Olson: Could you please repeat the question?

[*Translation*]

Mr. Pierre Paul-Hus: Given the recent experience with Nuctech and the issues with CanSino Biotech and Huawei, the Conservative Party members are asking that national security review all contracts with Chinese companies. I want to hear your thoughts on this.

[*English*]

Mr. Rory Olson: I'm not in a position to determine who should be investigated and for what. That's not something I'm confident to comment on.

The Chair: Thank you, Mr. Olson.

Thank you, Mr. Paul-Hus.

We'll go to Mr. Weiler for one question.

Mr. Patrick Weiler (West Vancouver—Sunshine Coast—Sea to Sky Country, Lib.): Thank you, Mr. Chair. I'll try to make this one question count.

I'd also like to first thank the witnesses for joining us for a very interesting discussion today.

My question is for Mr. Desai.

You mentioned some of the programs that the U.S. has for procurement, and you mentioned DARPA specifically. There is a local biotech company called AbCellera that won a competition that DARPA had where companies could compete to show how they could respond to the threat of a pandemic in developing a therapy.

It just so happens that, once the pandemic hit this year, there was a significant amount of investment from the Canadian government into AbCellera to develop a treatment for COVID, which eventually they did, and it was approved by PHAC, and we've now procured 26,000 doses of the therapy.

This is an interesting example, and I was wondering if you could speak to what lessons you think we can learn from the response to the pandemic with respect to the medical sector and how this can translate to support of the tech sector, particularly to navigate the valley of death?

Mr. Neil Desai: Thanks for that really thoughtful question.

I'm not in the bio space, but I think the lessons I draw from experience dealing with similar organizations like DARPA in the U.S., on more of the law enforcement or national security side of technology versus the medical security side, is that we have to start being able to walk and chew gum. We need to understand that solving real problems that are societal problems is the best form of economic development. If we don't marry those two, we will lose some of our best companies.

I will say that, if we work with some of those types of agencies similar to DARPA in other jurisdictions, they become attempts to draw us away from Canada. If we don't mirror this.... This is not just saying we should be nice Canadians and support our companies. This is a matter of future prosperity and maintaining our standard of living in this country. This is how, in highly secure industries, development is being done, both in the public and private sector.

The Chair: Thank you, Mr. Weiler and Mr. Desai.

I have Ms. Vignola for one question.

[*Translation*]

Mrs. Julie Vignola: I'll be brief. We asked many questions. We sometimes received an answer, and we sometimes didn't. It depends on your area of expertise. Are there any questions that we haven't asked and that you would like to address?

The question is for Mr. Buric.

[*English*]

Mr. Sime Buric: One of the questions I believe should be asked is “Should the hardware or any type of equipment be examined before going out into the field, as is done by some other Canadian entities?” CATSA, some of the transportation safety authorities and CBSA do examinations of hardware before it is deployed. That is definitely something that I believe the cybersecurity field should take into consideration for any future bids.

● (1655)

The Chair: Thank you, Mr. Buric.

Now we'll go to Mr. Green for one question.

Mr. Matthew Green: In the spirit of giving, I'm going to give my time over to Mr. McCauley. Put that in the record books.

The Chair: Mr. McCauley, you have one question.

Mr. Kelly McCauley: We have socialized time here.

To any of the witnesses, we've seen the issue with Nuctech and this part of the Canadian industry around scanners. Are there other examples you could perhaps share with us where we have a state-sponsored industry, unfairly subsidized, horning in on Canadian industry, besides the scanner ones that we've been talking about?

Mr. Neil Desai: I'll go quickly.

You might also want to take a look at Russian technologies. It's a little less clear in the cybersecurity space, the lines between the public and private sector in that country, but there's definite risk. We're seeing some of our allies starting to analyze and create risk matrices for where they will allow Russian-made technologies into their cybersecurity supply chains.

Mr. Kelly McCauley: Thank you.

The Chair: Thank you very much.

Mr. MacKinnon, I may not have been clear. If you have one question.... I'm not seeing him.

Mr. Drouin, do you want to ask a question in Mr. MacKinnon's stead?

Mr. Francis Drouin: Are we planning to finish at 5 o'clock?

The Chair: Yes.

Mr. Francis Drouin: Perfect.

The Chair: I put in a one-question rule and all of a sudden you guys are being so efficient. I'm finding that just tremendous. I'll have to do that more often.

Mr. Francis Drouin: I'll jump back to my question for the Canadian council of innovation. My question revolves around the U.S. example they portrayed.

Mr. Desai, I think you were talking about that and all the different programs that are involved in the U.S. Do you know if that represents a similar market share for those smaller SMEs that get to participate in those potential procurements? Is it similar to Canada or is there a very big difference?

Mr. Neil Desai: I would say those are just a small sampling of the programs. I will say, however, that the non-tariff considerations that favour American SMEs are prevalent in the core of their procurement, besides those economic development programs that use procurement. This is core to their procurement system. We see it in everyday procurements: Please list your U.S. board of directors, and please list how many U.S. veterans you employ. Points are awarded for those types of things.

Eyes wide open, this is happening in other places and these are places that have the same trade agreements that we're party to.

Mr. Francis Drouin: This is something we had actually looked at. With women entrepreneurship and the link to government procurement, the U.S. have used some of those examples and set-asides.

Thank you very much.

The Chair: Thank you, Mr. Drouin.

I'd like to thank all the witnesses for their presentations and for answering questions. It's greatly appreciated.

Committee members, we will be moving in camera. We will suspend the meeting, after which the technical staff will end this meeting in Zoom. You will have to go out and then come back in. Information with the password and the link was sent to you by the clerk.

Again, thank you very much, witnesses.

[*Proceedings continue in camera*]