

**FOLLOW-UP TO THE HOUSE OF COMMONS STANDING COMMITTEE ON
GOVERNMENT OPERATIONS AND ESTIMATES
Minister of Digital Government
March 12, 2020**

**1. The Health of the Government of Canada's Application Inventory (OCIO)
(CPC) Mr. Ziad Aboultaif (Edmonton Manning):**

In today's age we have smartphones with weather apps built into them. The private sector has already built these applications and tested them. So why is the government is wasting taxpayers money on things that already exist then boasting about it as an accomplishment?

Hon. Joyce Murray (Minister of Digital Government): Thank you very much for that question. So open data is a movement by which data that is collected by government is available to the private sector and citizens in order to be able to create businesses, help grow the economy or be able to solve problems out in society. The example that you provided is an app by Environment and Climate Change Canada. I mentioned that because we are a leader in the open data and open government movement by which we make data available so it can be used productively by the public and businesses to serve Canadians.

Mr. Ziad Aboultaif (Edmonton Manning): We try to solve a problem here, Minister, **We have to stop competing with the private sector in one way or another. We have resources available to us we can allocate them to be used somewhere else. What we're doing here is we're getting the same old fashion way, which is basically continuing doing what we shouldn't be doing and what you stated in your speech. I would really like you to regard that, basically putting resources where they need to and not just in cases like this.**

The Chair: It will have to be forwarded response, Madam Minister.

(BQ) Ms. Julie Vignola (Beauport—Limoilou): According to your mandate letter, you are tasked with identifying at-risk IT systems and platforms. How is that work coming along? When can we see the report on the exercise?

Mr. Francis Bilodeau (A/Chief Information Officer of Canada): That's what we talked about regarding core and at-risk services in response to an earlier question. As we mentioned, we are now conducting an application health review. This involves large systems that are at risk. We have just set up a deputy minister committee and started working on the planning process with the minister. I hesitate to provide a definite date, since we're in the planning stage.

Mme Julie Vignola (Beauport—Limoilou): That's fine. Mr. Bilodeau, you said earlier that you had an application health file. Would that file be readily available for consultation and analysis?

Mr. Francis Bilodeau (TBS): We would be able to provide that information. There is an application that departments use to give us information on the health of their applications.

Mme Julie Vignola (Beauport—Limoilou): Would it be possible to transfer it?

Response

TBS regularly monitors and tracks the health and evolution of the overall Government of Canada's IT business software and applications portfolio. As of December 31, 2019, this inventory lists 7,363 business and software applications currently in use across the Government of Canada (GC). TBS regularly surveys 59 departments to identify, monitor and assess the health and value of these applications.

The health of an application is determined based on a department's self-assessment of the application's business value, technical condition, funding condition and criticality. The health assessment is used to identify the urgency of action required to maintain application health. This information is used to provide evidence for enterprise decision making, including future investment decisions.

Of the 7,363 applications in the portfolio, 1,115 applications support mission critical services. Mission critical services are defined as those services or activities that if disrupted would cause high or very high risk to health, safety, security, economic well-being or continuity of government operations.

Currently, 36% of the GC application portfolio is considered "healthy." Eight percent of the applications have been identified as "requiring immediate attention," indicating a higher risk to the GC and should be taken as a priority call to action. Forty-six percent of the portfolio requires attention and 11% were not assessed by departments. Applications identified as "requiring attention" represent an increased risk to the operation of the GC and will require varying levels of investments to address. Reasons for required attention include aging infrastructure, legacy software platforms, inflexible systems architecture, insufficient operational funding, or unidentified business continuity planning.

2. Provide information on supporting digital government services in the context of social distancing and the COVID-19 response (OCIO/SSC)

(NDP) Mr. Matthew Green (Hamilton Centre): In your opening statement you referenced the challenges of our constituency staff and connecting Canadians to the critical services of government and we see here reference in a fall 2017 report of the Auditor General on the CRAs call centres found that the call centre agents answered only one-third of the calls to the call centre largely due to call volume. In my riding of Hamilton Centre we will serve hundreds of people a week on filing very simple tax forms to be able to get them back their returns, and yet with this COVID epidemic our very real concern is that as we get into social distancing we won't be able to maybe provide the same quality of face to face service that we have in the past. **What efforts are you taking to ensure Canadians can access CRA services through call centres and online?**

The Chair: Minister, I'm very sorry but I'm going to have to say in the essence of time that's a great question, but if you can provide the answer to this committee through the clerk in written form we'll make sure we distribute that and share that with the rest of the committee

Response

SSC is responsible for providing reliable, secure IT infrastructure and telecommunications across the Government of Canada. In times of emergency, SSC's services are critical to providing continuous services to Canadians. Given the threats posed by COVID-19, SSC is taking action to support the critical services of other departments in addition to general preparedness activities. In order to ensure collaboration across government, SSC is working closely with the Government of Canada lead—Public Safety under the Federal Emergency Response Plan (FERP) — and other federal partners.

SSC is responsible for providing IT services (Email/Workplace Technology, Data Centers, Telecommunications, Cyber and IT Security) to Government of Canada organizations, who in return deliver hundreds of critical services directly to Canadians. Due to this responsibility, SSC has an important role to play during emergencies, in support of our partners' mission critical programs and to ensure their critical services are operational during emergency events. In addition, several of SSC's customer departments are First Responders or lead agencies who have primary roles to play during emergency events and therefore it is imperative that SSC continues to support them.

The following is a list of actions that SSC is undertaking to support critical Government of Canada services:

- An SSC Emergency Operations Team has been activated and is coordinating the Department's Pandemic Emergency Response Plan.
- SSC provides departments with Secure Remote Access (SRA) services so that their public servants can access networks and systems remotely.

- Work is currently underway to increase remote access and network capabilities to support remote access for a large portion of the public service.
- SSC is developing a series of best practices for management and employees to improve the experience of Government of Canada employees connecting remotely.
- The Department is working with the federal Chief Information Officer (CIO) community to prioritize essential network traffic.
- SSC is ensuring additional resources are mobilized to help ensure federal public servants have the tools they need to work from home. This includes:
 - The deployment of long term evolution devices, including tablets, for some type of users (executives, communications teams, etc.) requiring email access and various internet tools.
 - The deployment of alternative options for conferencing:
 - Microsoft Teams as a collaboration and instant messaging solution
 - BlackBerry Messenger Enterprise (BBME) for secure messaging up to Protected B level
 - Increased conferencing capacities through the addition of 20,000 licenses from Cisco
- SSC is continuing to collaborate with vendors to:
 - seek alternative communications options
 - increase capacity to meet growing needs
 - expedite procurement process and equipment delivery
- SSC is prioritizing requests for essential services, especially ones that have links to the current situation.
- SSC is working closely with the federal CIO community and is implementing measures to reschedule non-essential IT infrastructure changes that could impact service delivery to Canadians.
- SSC is ensuring that essential services and tools continue to be provided for front line staff at other government departments during this time.

The following is a list of actions that TBS is undertaking to support critical Government of Canada services:

Critical Services: TBS is working closely with SSC and Government departments and agencies to ensure the availability of reliable, secure IT infrastructure and telecommunications across the Government of Canada to support the delivery of critical services.

- This includes working with departmental partners to ensure Business Continuity Plans are in place, appropriately tested, and adapted to the current situation.
- TBS is also working with Public Safety Canada and departments and agencies, to finalize a comprehensive list of Government of Canada critical services and ensure that mission critical applications and systems are mapped to this list, to ensure that critical services and government operations are appropriately supported.

Remote Work: The federal government is also taking action to ensure that the employees who support critical services are able to continue to work remotely. The Government of Canada currently has sufficient capacity to ensure employees supporting critical activities can work remotely and work is continuing to increase capacity as telework is increased. In the interim, departments have been asked to take action to limit non-critical network usage and reducing non-critical activities.

- In addition, to support employees working remotely, cloud-based collaboration solutions (Office365) are being deployed. This will allow employees will be able to access the workspace using their personal devices without requiring Virtual Private Network (VPN), reducing demand on existing network systems.