Subject: RE: Media request for comment from The Guardian and The Narwhal regarding TC Energy recording that references company's communications with CSIS

Date: June 26, 2024 at 12:55:29 PM PDT

Hi Matt,

Foreign interference poses a whole-of-society threat, targeting not just the federal government but a wide range of national security partners, and individual Canadians. We know that the issue of foreign interference requires a whole-of-government and whole-of-society response, and we are committed to equipping partners to stand up to malicious actors who threaten Canada's economic and national security. This is why we speak to and work with a wide range of partners and stakeholders, including different levels of government, civil society and industry. Through various engagements over the past years, we have heard frustrations from a wide range of partners regarding the information sharing and other limitations of the outdated *CSIS Act*.

In November 2023, the Government of Canada launched public consultations on possible amendments to the *Canadian Security Intelligence Service Act* (the CSIS Act) that would better equip CSIS to carry out its mandate to investigate, advise the Government of Canada, and take measures to reduce threats to the security of Canada and all Canadians. The consultations included an online survey available to the public, as well as direct and pro-active engagement with provincial and territorial governments; Indigenous governments; academia; legal, privacy and transparency experts; the private sector; community and religious representative organizations; and other civil society stakeholder and partner groups.

This extensive consultation process was a valued experience for CSIS, and provided an opportunity to reach out to and learn from a wide-range of members of Canadian society and Canadian organisations. There was widespread agreement that it would be sensible for CSIS' mandate to include sharing information beyond the Government of Canada, and that this would help mitigate a broad range of threats and build awareness and resilience for those at risk. For more information please see the What We Heard and Learned Report: CSIS Act Consultations.

An Act respecting countering foreign interference protects people in Canada and further strengthens Canada's counter-foreign interference toolkit, by adopting legislative amendments to enhance the government's ability to detect, disrupt, combat foreign interference and protect people in Canada against the threats posed by foreign interference.

Amendments to the CSIS Act, enable the disclosure of information, subject to privacy protections, to individuals and organizations outside the Government of Canada, to help them build resiliency to threats to the security of Canada. Increased resiliency will enable Canadian society at large to mitigate the impact of foreign interference before it undermines our institutions, economy, rights and sovereignty.

Authorizing the timely disclosure of information by CSIS to relevant stakeholders is an important addition to the Government of Canada's toolkit to protect Canada, the Canadian public and our democratic institutions against threats to national security.

The discussions alluded to in your questions occurred in the context of strategic-level engagements with the Business Council of Canada (BCC) for which the CEO of TC Energy is the co-chair of the BCC's National Security Working Group. CSIS will continue to engage with the BCC and many other partners and stakeholders on issues of national security.

CSIS is increasing its collaboration with industry and academia through a number initiatives to mitigate the threat of FI and protect Canada's economic security. This includes table top exercises, and a <u>security summit</u> held in October 2023 by Five Eyes (FVEY) principals in Palo Alto, California, alongside private sector and academic partners involved in emerging technology research and development from across FVEY countries.

This historic engagement represents just one of many steps CSIS has undertaken to generate public awareness of economic espionage threats posed by foreign states, particularly the PRC, that seeks to illicitly acquire the competitive advantages held by FVEYs countries in critical and emerging technologies that include AI, quantum computing and biotechnology.

These efforts aim to protect Canada's research ecosystem and economic prosperity from foreign interference, espionage, and unwanted knowledge transfer that could pose a threat to Canada and against Canada's national security interests.

The Director of CSIS in his 2018 remarks at the <u>Economic Club of Canada</u> mentioned that "the business community needs to be fully aware of the security threats to which it is exposed [...] Hostile states typically target companies or universities that are active in emerging technology – the kind of potentially revolutionary discoveries that can bring massive profits. Many of these advanced technologies are dual-use in nature in that they could advance a country's economic, security or military interests [...] It's important that you see yourself as being a part of national security and that you see your colleagues at CSIS as part of the solution. When you get back to your office, start this dialogue with your VPs, your board and with your employees. And remember that together, we can better safeguard Canada's businesses, we can bolster our economic strength, and we can better protect our country and its people."

CSIS works with its partners across the private sector to ensure they are aware of the threat environment and that they have the tools and information they need to protect their interests. Everyone has a role when it comes to protecting our national security.

Thanks,

Eric Balsam Media Relations, CSIS Relations avec les médias, SCRS @csiscanada / @scrscanada