Dear Minister,

Congratulations and welcome to your new role as Minister of National Defence. As Minister, your portfolio includes the Communications Security Establishment Canada (CSE) - an important member of Canada's security and defence ecosystem, and a contributor to Canada's defence investments. This letter provides a brief introduction to CSE's mandate, and your responsibilities in relation to our authorities. As Chief (Deputy Minister) for CSE, I look forward to working with you and discussing how our expertise and capabilities will support you in advancing the priorities and commitments of the Government of Canada.

Who we are and what we do

CSE is the national authority for foreign intelligence - we collect signals intelligence, or SIGINT, to provide timely and relevant intelligence to you, your Cabinet colleagues, and leads across other departments, on emerging priorities, strategic issues, and crises. CSE's foreign intelligence collection capabilities are guided by Cabinet-approved Government of Canada's Intelligence Priorities. Accordingly, CSE supplies foreign intelligence on key priorities including Arctic sovereignty, Russia's invasion of Ukraine, Border Security, Economic Security and Trade, the People's Republic of China, Indo-Pacific regional stability, terrorism and violent extremism, and hostile state activity (for example, foreign interference, intellectual property theft, cyber threat activity). Additionally, we have a long history of working together with the Canadian Armed Forces (CAF) as CSE supports Canadian military missions abroad, providing information to enable military objectives and keep personnel safe.

CSE also has a mandate to conduct cyber operations to advance Canadian interests, including countering some of the toughest national defence and security challenges we face, including economic security. As Minister, you oversee the foreign cyber operations authorities that enable Canada to take direct action to disrupt, degrade, or influence an adversary's networks. As these tools are a significant element of military and state power needed to deter and defeat external threats to Canada, you discharge these duties in close consultation with the Minister of Foreign Affairs, and the Intelligence Commissioner (IC). CSE often conducts foreign cyber operations in coordination with our Five Eyes partners to achieve common goals. We also conduct joint cyber operations with the CAF and law enforcement partners to support their mission objectives.

CSE includes the Canadian Centre for Cyber Security (Cyber Centre) - Canada's world-renowned lead agency in cyber defence and cyber security. Using our network of sensors placed across federal institutions, we defend Government of Canada systems against malicious attacks aimed at federal systems, databases and websites. When cyber incidents happen, the Cyber Centre provides fast support recognizing that actioning the right steps quickly can significantly reduce the harm and economic impact and speed up the recovery process. Through these activities, the Cyber Centre gains knowledge of the trends and threat landscape, which it then uses to provide actionable advice and guidance to Canadian businesses and governments, and to help inform Canadians on how to take steps to protect themselves and their networks. Having our intelligence, cyber security, cyber operations, enterprise technology and all mission support functions under the same roof allows the Cyber Centre to work together with other CSE teams to achieve unique outcomes that benefit Canadians, such as CSE's ongoing campaign against cybercrime.

As the resiliency of critical infrastructure in Canada is key to national security, the Cyber Centre's mandate also includes systems of importance to Canada – as such we are focused on increasing trusted relationships with critical infrastructure partners across all sectors. The recently launched National Cyber Security Strategy demonstrates the Government of Canada's shift towards a whole-of-society partnership and, as a first step, announces the establishment of the Canadian Cyber Defence Collective which will serve as a national multi-stakeholder engagement body to advance Canada's cyber resilience through direct public-private partnership on national-level cyber security challenges, policy priorities, and defence efforts. Given cyber threats are increasingly directed at critical infrastructure networks and technology used to run vital sectors, the Cyber Centre is well positioned to support further activities to raise the collective cyber resiliency of Canada – this could include cyber security legislation such as the former Bill C-26: *An Act Respecting Cyber Security*, which was introduced but not passed in the last parliamentary session, and would have required operators in the federally regulated energy, finance, telecommunications, and transport sectors to report cyber incidents to CSE's Cyber Centre - a best practice already enacted by likeminded partners.

Cryptography is a fundamental part of cyber security. For nearly 80 years, CSE has been Canada's national cryptologic agency, making and breaking codes. As the national authority for Communications Security (COMSEC) in Canada, CSE contributes to the security and protection (encryption) of the Government of Canada's most classified information and data, ensuring that departments and agencies, as well as private industry partners who work with the government, are deploying equipment that is approved for use and effective in keeping Canada's information secure. For instance, when you hold a virtual meeting with Cabinet colleagues at the SECRET or TOP SECRET level, the technology and standards enabling that secure communication were developed, tested, and deployed by CSE. Through its own research and partnership with Five Eye partners, CSE plays a key role in ensuring that Canada is prepared to respond to new technologies, such as the emergence of quantum computers with the capacity to break modern encryption. Opportunities exist for Canada to increase its own sovereignty, increase resiliency across the North Atlantic Treaty Organization and the Five Eyes, and contribute to our own industrial base through investments in Canada's cryptologic industry.

CSE is unique in that we have combined our foreign intelligence, cyber security, cyber operations, and communications security authorities under one agency. This is what I like to call Canada's "secret sauce": it distinctively positions CSE to respond to threats in a nimble and decisive manner. What we learn from our intelligence or cyber-threat reporting serves to inform our cyber operations, and vice versa, thereby strengthening the advice that the government provides to Canadians and domestic industry partners and solidifying our collective security posture and safety. Our ability to capitalize on the various aspects of our mandate makes us a key partner in priorities such as economic security and Canada's Border Plan where CSE is working with partners both within Canada and in collaboration with the United States to disrupt and mitigate the threat of fentanyl and organized crime.

Partnership and collaboration are key to our success; they are a big part of what I believe positions CSE and its partners to respond to the dynamic threat environment we face. CSE is a core member of the Five Eyes, an almost 80-year-old partnership between Canada, Australia, New Zealand, the United Kingdom, and the United States. This alliance is a force multiplier for CSE and Canada – providing a forum to share intelligence, technology, collaborate on research and generate insights to hone our understanding of our threats, risks and adversaries and strengthen our collective defences. The Five Eyes also issue joint publications on issues of common concern (e.g. guidelines on the secure development and use of Artificial Intelligence (AI)) which serve to amplify the message around the world. In addition to the Five Eyes, CSE also maintains bilateral and multilateral relationships with like-minded allies as part of our SIGINT and cyber security activities. For example, CSE participates in two multinational intelligence forums to coordinate with like-minded allies on Arctic security. One forum, chaired by CSE, is specific to signals intelligence and concerns both polar regions. The other is an all-source intelligence forum focused exclusively on the Arctic.

CSE strives to be at the forefront of innovation and research. CSE and the Cyber Centre host several events throughout the year to work intensively on problems related to our mission. These workshops are innovation incubators that bring together participants from across Canada and the Five Eyes, academia, industry and the public sector. CSE also has its own researchers focused on foundational research related to cryptography, vulnerability research and data science - our own classified research and our research partnerships ensure we have the expertise to tackle current and emerging challenges. As a data-centric organization, CSE has been on the forefront of the foundational data science that underpins AI, as well as the use of AI and machine learning to help support mission activities. We work closely with other federal, academic and industry partners on AI safety and security. Although CSE has some of the most powerful high-performance computers in the country, we anticipate our compute needs escalating exponentially as we seek to collect more data and leverage emerging technologies. Looking ahead, new measures will be key to strengthening the common and interoperable systems that enable Canada's high security organizations to securely communicate and work together to address threats to Canada's sovereignty and security.

I want to close with the assurance that CSE delivers on its mandate responsibly. CSE's authorities are aligned with government priorities and direction, protect the privacy of Canadians and people in Canada, and are subject to robust controls, oversight and review. CSE is explicitly prohibited in legislation from directing its foreign intelligence, cyber security, or foreign cyber operations activities at Canadians anywhere in the world, or at any person in Canada. Our legislation also requires us to have measures in place to protect the privacy of Canadians whom we may incidentally encounter as we carry out our activities. CSE's activities are subject to independent oversight by the IC and retroactive review by the National Security and Intelligence Review Agency and the National Security and Intelligence Committee of Parliamentarians. CSE is also subject to audits by the Auditor General, reviews by the Office of the Privacy Commissioner, requests for access to documents through the *Access to Information Act* and the *Privacy Act*, and examination, primarily in response to complaints, by the Office of the Commissioner of Official Languages and the Human Rights Commission.

At your convenience, I look forward to the opportunity of welcoming you to CSE's Edward Drake building to learn about the important work that we are doing as a member of the defence portfolio and security and intelligence community. In the meantime, I am pleased to share this QR code that links to a digital binder that provides you and your office with additional documents, in both official languages, on CSE's mandate and activities.

This QR code links to a digital binder (www.cse-cst.gc.ca/key-documents) that includes additional documents on CSE's mandate and overview in both official languages.

At a time when Canada is more threatened by hostile states than at any time since the Cold War, and in an increasingly complex threat landscape of foreign interference, cyber attacks, and a destabilized geopolitical environment – I look forward to working with you, Minister, to protect Canada and Canadians and enhance national resilience.

Yours sincerely,

Caroline Xavier
Chief
Communications Security Establishment Canada