Ron McKinnon, MP
Chair of the Standing Committee on Public Safety and National Security
House of Commons
Ottawa, Ontario
K1A 0A4

Dear Colleague:

As the Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs and on behalf of the Government of Canada, I am pleased to respond to the Seventh Report of the Standing Committee on Public Safety and National Security, titled *Up to the Task: Strengthening Canada's Security Posture in Relation to Russia.*

I would like to commend the Committee for its efforts to examine Canada's security posture in relation to Russia.

The Government agrees-in-principle with both the overall tenor and with a majority of the Committee's recommendations. While the Government does not disagree with any of the recommendations, further study or examination is required in some cases.

Recommendation 1: ***That the Government of Canada continue to impose severe costs on Russia for its aggression against Ukraine; support Ukraine's sovereignty, independence, and territorial integrity; work with allies and partners to uphold the rules-based international order; and accelerate efforts to deter and defend against any conventional and unconventional threats to Canada's national security.***

The Government of Canada agrees with this recommendation.

Canada's future security and prosperity depend on a stable, predictable and collaborative international system built on respect for United Nations Charter principles including sovereignty, human rights, and the rule of law. Canada's support to Ukraine is an investment in a more stable, democratic and accountable world, ensuring Russia's aggression is neither rewarded nor imitated elsewhere.

Canada remains committed to playing a leadership role in the preservation and strengthening of an international rules-based order – sanctions are a key component of this approach.

To support Ukraine's sovereignty, independence and territorial integrity, the Government of Canada's over $1 billion in military aid and donated equipment to Ukraine has included air defence, Leopard II tanks, armoured personnel carriers, artillery, drone cameras, ammunition, and satellite communications equipment. Additionally, as part of Operation UNIFIER, extended and expanded until March 2025, Canada has trained over 36,000 Ukrainian troops, continues to conduct training in Poland and the UK, and has deployed trainers and combat engineers to the region.

To uphold the rules-based international order, Canada has leveraged its global influence, resources and diplomatic networks to maximize support for Ukraine and isolate Putin's regime. Canada has acted across multilateral fora, including the North Atlantic Treaty Organization (NATO), Organization for Security and Cooperation in Europe (OSCE), G7 (including its Multi-Agency Donor Coordination Platform) and G20. Canada was also co-facilitator and co-sponsor of United Nations General Assembly (UNGA) resolutions condemning Russian aggression, including those passed on March 24, April 7, and October 12, 2022, as well as on March 2, 2023.

Canada takes the concerns of new and emerging partners seriously, and is actively building international support for Ukraine. For example, Canada and allies campaigned worldwide ahead of the October 2022 UN General Assembly resolution on the territorial integrity of Ukraine, helping achieve a record 143 'Yes' votes. In other fora, including the June 2022 Commonwealth Heads of Government Meeting in Kigali, Rwanda, Canada has helped address the consequences of the crisis for the most vulnerable by announcing $250 million for global food security, with a focus on Sub-Saharan Africa.

Since Russia's illegal occupation and attempted annexation of Crimea in 2014, Canada has imposed sanctions on more than 2,400 individuals and entities in Russia, Belarus and Ukraine.

Canada will continue to work with its allies and partners to pressure Russia to end its war. Canada stands with Ukraine.

The Communications Security Establishment (CSE) has been tracking cyber threat activity associated with the current crisis. CSE has been sharing valuable cyber threat intelligence with key partners in Ukraine and continues to work with the Canadian Armed Forces in support of Ukraine.

CSE continues to leverage its full spectrum of cyber authorities to defend Canada's national security. This includes cyber security authorities and capabilities, foreign intelligence, and foreign cyber operations to impose costs on aligned actors that target Canadian systems of importance.

Recommendation 2: ***That the Government of Canada work with provincial and territorial partners to create and promote accredited post-secondary cyber defence training programs.***

The Government of Canada agrees to further examine this recommendation.

The Canadian Centre for Cyber Security—part of the CSE—is the single unified federal source of expert advice, guidance, services, and support on cyber security for Canadians. It is responsible for defending Government of Canada networks; providing advice, guidance, and services to systems of importance to the Government of Canada; and offering simple and effective tips that all Canadians can use to help keep themselves safer online.

CSE continues to work with stakeholders, including government and non-government partners, to share information to ensure that they have access to the cyber security experts, expertise, and resources they need to defend against and recover from malicious cyber activity. For example, the Cyber Centre's Learning Hub provides training to improve the cyber security of Canada's government and critical infrastructure organizations. The Cyber Centre also works with academic institutions to build Canada's pool of cyber security talent and has published a list of certifications in the field of cyber security.

Recommendation 3: ***That the Government of Canada, in consultation with relevant stakeholders, build on the* National Cyber Security Strategy *to ensure that—operators and enterprises of all sizes connected to critical infrastructure have the cyber security experts, expertise, and resources they need to defend against and recover from malicious cyber activity; and cyber security standards are met and reported on.***

The Government of Canada agrees with this recommendation.

Public Safety Canada is drafting a new National Cyber Security Strategy in consultation with the federal cyber security community. As part of this process, the Department will continue engaging with provinces, territories and industry stakeholders, including critical infrastructure representatives, to position Canada to be equipped to face the challenges of the digital era.

The new strategy is envisioned to articulate Canada's vision for protecting our national security and economy, deterring cyber threat actors, and promoting norms-based behaviour in cyber space.

For CSE, the development of the new Strategy is an opportunity to look back, take stock, and build on the accomplishments of the Cyber Centre over the past five years, as its creation was a flagship initiative under the previous 2018 Strategy.

As our vital assets and systems are far more interconnected, integrated, and interdependent, Public Safety Canada is also modernizing the National Strategy for Critical Infrastructure, in consultation with the critical infrastructure community. Canada's critical infrastructure is more susceptible to cascading failures across multiple sectors of our economy given the evolving threat landscape, and so efforts are needed to strengthen Canada's critical infrastructure security and resilience.

Recommendation 4: ***That the Government of Canada instruct the Communications Security Establishment to broaden the tools used to educate small- and medium-sized enterprises about the need to adopt cyber security standards.***

The Government agrees with this recommendation.

Cyber security is a shared responsibility; Canadians, the government, the private sector and our international partners all have an important role to play. To ensure that small and medium organizations have access to resources to help bolster their cyber security and overall resiliency, CSE has helped develop and deliver tailored advice and guidance, as well as learning programs through its Cyber Centre (including the Get Cyber Safe program, a national public awareness campaign created to help inform Canadians about cyber security) and broader Government of Canada partnerships. Public Safety Canada has also developed a number of applications and exercises to help critical infrastructure owners and operators across Canada to understand how to improve their cyber resilience and security. Industrial Control Systems are key to the well-functioning of all infrastructures and, if affected by cyber incidents, could jeopardize Canadians ability to function in our increasingly digitalized economy.

The Cyber Centre regularly develops, and updates advice and guidance tailored to small and medium organizations. This includes the baseline cyber security controls for small and medium organizations, top measures to enhance cyber security for small and medium organizations, the Ransomware Playbook and supply chain threats and commercial espionage.

CSE will continue to work with and provide up-to-date advice and guidance to small- and medium-sized enterprises to ensure that they are able to implement necessary and important security controls to ensure the security of their organizations.

Recommendation 5: ***That the Government of Canada establish incentives, including – but not limited to – an accelerated capital cost allowance or other tax measures, for small- and medium-sized enterprises to make the investments necessary to follow the Communications Security Establishment's baseline cyber security controls.***

The Government takes note of this recommendation.

Small- and medium-sized enterprises making capital investments, including those related to cyber security, are already able to benefit from various accelerated capital cost allowance measures and other tax measures introduced by the Government. This includes the Accelerated Investment Incentive introduced in 2018, which allows for an enhanced first-year tax deduction up to three times the normal rate, and the temporary measure introduced in Budget 2021 that allows small businesses to immediately expense up to $1.5 million of eligible new investments. It is also noted that computer software that is not considered systems software is generally eligible for a 100 per cent capital cost allowance rate. Additionally, Budget 2022 introduced a more gradual phase out of the small business deduction, with access being fully phased out when taxable capital reaches $50 million, rather than at $15 million (under the previous rules). This allows more medium-sized businesses to benefit from the reduced rate and increases the amount of income that can be eligible, leading to further tax savings that can be reinvested into a business.

Recommendation 6: ***That the Government of Canada require critical infrastructure operators – from appropriately designated sectors – to prepare for, prevent and report serious cyber incidents, and that it put in place accompanying reporting timelines, technical assistance, and protections for the information that would be reported to the Communications Security Establishment and the lessons-learned that would be shared with industry, and that it then table annual reports to Parliament on these efforts.***

The Government agrees with this recommendation.

In June 2022, the Government introduced Bill C-26, an Act respecting Cyber Security. Under Part Two of this bill, the Critical Cyber Systems Protection Act (CCSPA), designated operators would be required to report cyber security incidents that meet or exceed a threshold to the CSE. Immediately after reporting a cyber security incident, the designated operator would be obliged to inform the appropriate regulator. Upon request, the Cyber Centre would be obliged to provide an incident report to the industry regulator.

In addition, the Cyber Centre already has a well developed working relationships with industry and critical infrastructure operators, many of whom voluntarily report cyber incidents. The CCSPA would allow the Cyber Centre to build on these relationships in a collaborative and more engaged way.

Recommendation 7: ***That the Government of Canada ensure that the cyber roles, responsibilities, and structures that exist across the federal government maximize coherence, coordination, and timely action in relation to cybersecurity, and that it submit annual reports to Parliament on these efforts.***

The Government of Canada agrees with this recommendation.

Bill C-26 would ensure that the cyber roles, responsibilities, and structures that exist across the federal government maximize coherence, coordination, and timely action in relation to cyber security. The CCSPA will ensure a consistent cross-sectoral approach to cyber security in response to the growing interdependency of cyber systems. Moreover, it will authorize regulators who are already responsible for ensuring compliance and enforcement activities under other federal statutes to exercise compliance and enforcement authorities they receive through the Act and sector-specific regulation.

Roles envisioned under the Act:

Minister of Public Safety: The Minister of Public Safety, in his role as the Minister responsible for national and cyber security coordination and policy, would be responsible for the implementation and administration of the Act.

The Minister of Public Safety would submit to the Governor in Council for consideration, in consultation with implicated ministers, Cyber Security Directions that would compel any designated operator to take specific measures necessary to address a known and imminent threat or vulnerability.

The Minister would be responsible for submitting an annual report to Parliament on the administration of the CCSPA.

Public Safety Canada: Public Safety would lead the development of regulations necessary for implementing the Act, in consultation with implicated lead federal departments, the CSE, regulators and Canadians. It is expected that these departments and their Ministers would engage their respective regulators, as required, to provide their expertise and contribute to discussions leading to the development of regulations.

Governor in Council: The Governor in Council would be empowered, by order, to direct any designated operator or class of operators to comply with any measure set out in a Cyber Security Direction for the purpose of protecting a critical cyber system.

Regulations will be made by the Governor in Council on the recommendation of the Minister of Public Safety.

Regulators:
The regulators under the Act would include the Minister of Industry, the Canada Energy Regulator, the Canadian Nuclear Safety Commission, the Minister of Transport, the Office of the Superintendent of Financial Institutions, and the Bank of Canada.

Designated Operators:
The Act would require designated operators to, among other things, establish and implement cyber security programs, mitigate supply-chain and third-party risks, report cyber security incidents and comply with Cyber Security Directions.

Recommendation 8: ***That the Government of Canada emphasize the importance and modernization of cyber security in departmental mandates.***

The Government of Canada agrees with this recommendation.

In 2019, the Treasury Board Policy on Service and Digital was published. The Policy and supporting instruments serve as an integrated set of rules that articulate how Government of Canada organizations manage service delivery, information and data, information technology, and cyber security in the digital era. The Policy advances the delivery of services and the effectiveness of government operations, including modernization of digital services and cyber security, in support of the Government's Digital Ambition and Canada's Digital Government Strategy.

Further, the Directive on Service and Digital outlines the direction for the departmental designated official for cyber security, in collaboration with the departmental Chief Information Officer and Chief Security Officer as appropriate, to ensure that cyber security requirements and appropriate risk-based measures are applied continuously in an identify, protect, detect, respond, and recover approach to protect information systems and services.

Finally, the Treasury Board Secretariat, in collaboration with Shared Services Canada, and in consultation with the Communications Security Establishment and other implicated departments, is developing a comprehensive whole-of-government vision and plan for the cyber security of government operations.

Recommendation 9: ***That the Government of Canada explore options for a Canada–United States cyber defence command structure.***

The Government of Canada agrees that collaboration with the U.S. on cyber defence is important.

The United States is Canada's closest ally and partner, and the Department of National Defence and the Canadian Armed Forces maintain a strong defence and security relationship with the U.S. military. DND/CAF, in partnership with the Communications Security Establishment, continues to work closely with a range of U.S. cyber authorities, including the United States Cyber Command (USCC) to ensure collective defence and security in cyberspace.

DND/CAF is always exploring options to enhance its cyber defence relationship with the U.S. DND/CAF and CSE will continue to work closely with USCC, and other U.S. agencies, to enable and enhance operational cyber defence coordination and collaboration. We will achieve our common goals through shared situational awareness, and by working together on cyber operations as appropriate.

Recommendation 10 : ***That the Government of Canada examine the full extent of Russian disinformation – and other state-backed disinformation – targeting Canada, the actors, methods, messages and platforms involved, and the impact this disinformation is having on the Canadian population and Canada's national security, and that it report its findings to Parliament annually.***

The Government agrees to further examine this recommendation.

In Budget 2022, the Government of Canada committed to providing $13.4 million over five years, starting in 2022–23 to renew and expand the G7 Rapid Response Mechanism, an international forum that addresses foreign threats to democracy, including state-sponsored disinformation. Further, in August, the Government also announced the creation of a dedicated team to monitor and detect Russian influence operations and enable deeper international coordination, including through the G7 Rapid Response Mechanism.

Canada's security and intelligence community remains vigilant against the potential threat of Russian foreign interference against Canadians and Canadian interests in retaliation for our support for Ukraine.

Recommendation 11: ***That the Government of Canada, in collaboration with allies and domestic partners, continue to expose and counter Russian and other state-backed disinformation campaigns targeting Canadians*****.**

The Government agrees with this recommendation.

Canada's role as the secretariat for the G7 Rapid Response mechanism helps monitor and detect Russian state-sponsored disinformation and deepen ties and collaboration.

We have seen Russian narratives and disinformation used to try to justify the invasion of Ukraine, undermine the Ukrainian government and delegitimize Western responses. Canada will continue to condemn the overt and covert use of disinformation not only by the Russian Government and its affiliated media and proxies, but by any foreign state that seeks to threaten global democracy and the safety and security of Canadians.

Recommendation 12 : ***That the Government of Canada work with experts, Internet Service Providers, social media platforms and international partners to counteract online bots that are amplifying state-sponsored disinformation, and that it report the findings and actions to Parliament.***

The Government agrees to further examine this recommendation.

Global Affairs Canada's Rapid Response Mechanism (RRM): Canada and its communications teams coordinate with international partners in governments, academia and civil society to counteract state-sponsored disinformation, including disinformation amplified by bot networks on social media. This is done by promoting factual information through official channels and through diplomatic efforts aimed at rallying international partners to also work with service providers and social media platforms to identify and disrupt networks of automated accounts spreading state-sponsored disinformation. RRM Canada also supports the efforts of think tanks and civil society organizations who conduct open source research to identify these networks, shine light on their covert and malign tactics, and who also work with social media companies to disrupt these networks.

Recommendation 13: ***That the Government of Canada support independent Russian journalists and academics who are working to expose the regime's propaganda and disinformation.***

The Government agrees to further examine this recommendation.

Through Global Affairs Canada, Canada is providing support to advance the safety of journalists, counter restrictions to free and safe civic spaces, promote information integrity, and counter mis/disinformation, globally. While this does not include direct support for individual Russian journalists, it does include support for independent journalists in Eastern Europe, including those in exile, some of whom report in Russian to Russian audiences.

Recommendation 14: ***That the Government of Canada urgently work with its international and domestic partners to combat sanctions evasion, including by taking appropriate steps to ensure all property of sanctioned Russian individuals and entities situated in Canada has been identified and frozen.***

The Government of Canada agrees with this recommendation.

Canada is seized with the importance of addressing sanctions evasion, and improving the impact of our sanctions. In this regard, Canada is keen to work with international allies and domestic partners to find ways to collectively address enforcement challenges.

Canada also regularly cooperates with G7 members, Australia, and New Zealand to improve the effectiveness of sanctions once they are imposed. This includes participation in multilateral fora on sanctions implementation and enforcement, with a particular focus on working with allies and partners to develop solutions to confront tactics of evasion, circumvention, and backfilling. For example, on February 24, 2023, G7 leaders announced the establishment of an Enforcement Coordination Mechanism, aimed at maintaining, fully implementing and expanding the measures imposed, including by preventing and responding to sanctions evasion and circumvention.

As a first step, Canada is actively sharing trade data with allies to compare trade anomalies, and identify circumvention and backfilling patterns. The Government will also continue to look at how best to address below-threshold goods that may be diverted to third parties. This will help to understand and address Russia's evasion tactics, so sanctions can effectively constrict Russia and curtail its ability to engage on the battlefield.

Shortly following Russia's invasion of Ukraine, Australia, Canada, France, Germany, Italy, Japan, the United Kingdom, the United States and the European Commission jointly launched the Russian Elites, Proxies, and Oligarchs (REPO) Task Force, a multilateral effort that has used information sharing and coordination to isolate and exert unprecedented pressure on sanctioned Russian individuals and entities. The REPO Task Force's collective efforts have resulted in the freezing of tens of billions of dollars and in some cases asset seizures. The Task Force is also tackling loopholes that facilitate sanctions evasion. Notably, on March 9, 2023, the REPO Task Force and its members, including Canada, coordinated to publish a global advisory that outlines tactics employed by the Russian Federation, oligarchs and their proxies to evade sanctions in an effort to access funds and support their war efforts. Canada will continue to play an active role in the REPO Task Force to coordinate sanctions implementation and crack down on sanctions evasion.

Canadians and persons in Canada are required to comply with sanctions, and to report instances of possible violations. Under the Special Economic Measures Act (SEMA), every person in Canada and all Canadians outside of Canada must disclose to the Royal Canadian Mounted Police (RCMP) the existence of property in their possession or control that is believed to be owned or controlled by a designated person. Canadian financial institutions continue to play an essential and appreciated role in this regard.

Enforcing sanctions is a whole-of-government effort, and Global Affairs Canada works closely with domestic enforcement agencies to ensure that Canadian sanctions are complied with. The RCMP and the Canada Border Services Agency (CBSA) have authorities to take enforcement actions by investigating potential violations and enforcing willful contraventions. For example, the CBSA regularly stops and detains prohibited shipments at the border, and works with vigilance and often in partnership with international allies to identify instances of possible diversion or evasion. The RCMP plays a critical role in collecting information on assets owned or controlled by designated persons (i.e., individuals or entities). To date, the RCMP reports that a total approximate equivalent of C$122 million of assets in Canada have been effectively frozen, and a total approximate equivalent of C$292 million in financial transactions have been blocked as a result of the prohibitions in the Special Economic Measures (Russia) Regulations.

Budget 2023 announced further measures that will strengthen sanctions compliance and enforcement. Bill C-47 (Budget Implementation Act 2023) proposes targeted changes to the SEMA and the Justice for Victims of Corrupt Foreign Officials Act to support the effectiveness of the seizure, forfeiture and disposal framework introduced in 2022, and related amendments to the Proceeds of Crime (Money Laundering) and Terrorist Financing Act to require the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) to disclose information to the Minister of Foreign Affairs in certain circumstances.

The Government further intends to set up obligations for the financial sector to report sanctions-related information to FINTRAC and will review the mandate of FINTRAC to determine whether it should be expanded to counter sanctions evasion. An update will be provided in the 2023 fall economic and fiscal update.

The Government of Canada will continue to work with our international allies and domestic partners to close any gaps in implementing our sanctions, including to address sanctions evasion, circumvention, and backfilling.

Recommendation 15: ***That the Government of Canada accelerate the modernization of the North American Aerospace Defense Command (NORAD).***

The Government of Canada agrees with this recommendation.

Since the Minister of Defence's June 2022 announcement of Canada's plan to modernize NORAD, National Defence has been working to establish and integrate NORAD modernization projects into the broader Defence program, move out on early priorities in the 20-year plan, and lay the ground for deeper partner and stakeholder engagement on the full suite of initiatives over the coming months and years.

National Defence maintains a publicly accessible web page with up-to-date project timelines for NORAD modernization.

National Defence is taking a phased approach to NORAD modernization. Many projects will reach initial operational capability by the late 2020s, while the most complex projects should by the mid-2030s.

To deliver on this new suite of investments in a timely manner, National Defence is working as quickly as possible to establish new program offices and to strengthen its internal services capacity. This approach is based on lessons learned from Canada's defence policy, *Strong, Secure, Engaged*, and will support timely and effective implementation.

Early progress on capabilities includes:

- Deepening planning and collaboration efforts with the U.S. During President Biden's visit to Canada in March 2023, the Prime Minister and President issued a joint statement reconfirming their commitment to ongoing collaboration to modernize NORAD.
- Refining concepts of operation and siting options with the U.S. on Over-the-Horizon-Radar (OTHR) to optimize radar coverage of the approaches to the continent. During his bilateral meeting with the President in March 2023, the Prime Minister confirmed Canada's intent to move quickly to align our Over the Horizon Radar timelines with the U.S., and to that effect, announced the target initial operational capability date for Arctic OTHR of 2028.
- Ongoing binational work on Cloud-Based Command and Control (CBC2) for NORAD.
- Progress to include additional Air-to-Air Refueling capacity to the Strategic Tanker Transport Capability project (previously approved in December 2020) as part of *Strong, Secure, Engaged*.

Like the new capabilities, infrastructure investments will also be implemented through a phased approach. The timelines will stem from operational requirements and ongoing coordination with northern and Indigenous partners, and will be influenced by the longer construction times and other challenges associated with northern infrastructure.

- National Defence has commenced engagements with territorial, municipal and Indigenous partners on the site development planning process for northern infrastructure upgrades in Inuvik, Yellowknife, Iqaluit, and Goose Bay.

CSE also benefited from investment to improve its abilities to safeguard and advance Canada's national and collective interests in the North. It will collaborate with DND/CAF to protect Canadians against new and emerging aerospace threats to Canada and North America more broadly.

Recommendation 16: ***That the Government of Canada ensure it has both the capacity and the funding in place to realize Canada's defence procurement objectives, that it take all measures necessary to support the reconstitution of the Canadian Armed Forces, and that it report regularly to Parliament on its efforts to meet both these objectives*****.**

The Government of Canada agrees with this recommendation.

The Department of National Defence, in collaboration with Public Service and Procurement Canada and Innovation, Science and Economic Development Canada and central agencies, leads and participates in a number of ongoing initiatives to ensure it has both the capacity and funding in place to realize Canada's defence procurement objectives. National Defence will continue to examine measures to address challenges related to defence procurement. This includes continuing to hire civilians to support procurement activities.

More specifically related to reconstitution, in October 2022, the CAF published The CAF Retention Strategy, which is designed to build awareness, drive principal approaches to support people, and help inform policy development and decision-makers to make more effective decisions impacting CAF members. National Defence also recognizes that accelerating culture change in the CAF could contribute to improved recruitment and retention. In addition, National Defence is undertaking a review of the CAF's recruitment initiatives to help facilitate the revitalization of recruiting and training that is expected to occur over the course of the next five years.

National Defence regularly reports to Parliament on defence issues, including through the estimates process and the annual reporting processes such as the Departmental Results Report. National Defence will continue to update Parliament through these and other mechanisms.

Recommendation 17: ***That the Government of Canada honour its commitments to its NATO Allies and meet the Alliance's 2% defence spending target.***

The Government agrees to further examine this recommendation.

Canada is unwavering in its commitment to NATO, to the defence of Euro-Atlantic security, and to the rules-based international order. Overall, Canada's defence spending and procurement are based on threat analyses and assessments of our needs, as opposed to arbitrary spending targets.

Canada remains committed to maintaining the defence budget increases that were set out in Canada's defence policy, *Strong, Secure, Engaged.* This will increase Canada's total defence budget from $18.9 billion in 2016–17 to $32.7 billion by 2026–27, an increase of more than 70 percent. In addition, we will invest $38.6 billion on an accrual basis over the next 20 years into NORAD modernization. These investments ensure that a secure North America can project power in support of NATO Allies without being held at risk at home from emerging and future threats.

Canada continues its steady and reliable commitment to NATO missions, operations, and activities. This includes the leadership and expansion of the enhanced Forward Presence Battlegroup in Latvia, support to NATO maritime forces through the deployment of up to three surface vessels, and the provision of lethal and non-lethal military assistance to Ukraine. Canada fully supports the renewal of the Defence Investment Pledge at the upcoming Leaders Summit, which will take place in July.

Going forward, we need to position NATO for success, including by balancing ambition with attainable objectives. As the Alliance adapts its deterrence and defence posture to meet the challenges of the future, a renewed Defence Investment Pledge must reflect the contributions of Allies across all three C's: Cash, Capabilities, and Contributions. It must also align with the commitments which leaders made in the 2022 Strategic Concept.

Recommendation 18: ***That the Government of Canada put in place a register of foreign agents or a measure equivalent to the Australian Foreign Influence Transparency Scheme Act.***

The Government agrees to further examine this recommendation.

Some foreign governments, or their proxies, use individuals or entities to attempt to influence, covertly or in a non-transparent manner, Canadian government policies or Canadian public discourse. These activities can be detrimental to the national interest, national security and public trust in democratic processes and institutions. The threat of foreign interference has increased in sophistication, and pervasiveness, affecting Canada and Canadians. For this reason, the Government of Canada launched public and stakeholder consultations on a Foreign Influence Transparency Registry in March 2022. The online consultations on FITR, which lasted 60 days, produced nearly 1000 responses from a wide range of respondents across Canada to guide the creation of FITR. Roundtable and bilateral discussions with stakeholders—including community organizations, Indigenous groups and provincial/territorial stakeholders—have continued beyond this date. The Government of Canada continues to review the tools and authorities at its disposal to ensure that our approach keeps pace with the evolving threat environment and is adapted to the Canadian context.

Recommendation 19: ***That the Government of Canada publish a comprehensive and integrated national security strategy, which takes into account an internal review of Canada's national security capabilities.***

The Government agrees to further examine this recommendation.

Securing an Open Society: Canada's National Security Policy was published in 2004 and was the first statement of its kind by the Government of Canada providing a strategic framework and action plan designed to ensure that Canada is prepared for, and can respond to current and future threats. The Government of Canada recognizes that the national security landscape has evolved since the release of Securing an Open Society, and that today's threats include a myriad of complex, multidimensional issues and challenges. These include, for example, foreign interference, cyber security, space and emerging technologies, violent extremism and terrorism, border security, environmental and health security, and the nexus between organized crime and national security. In light of the changed threat landscape, the Government of Canada also recognizes the need to ensure that the national security toolkit remains flexible and adaptable to ensure it can continue to prevent, mitigate, and respond these issues and challenges.

Recommendation 20: ***That, pursuant to Section 34 of the National Security and Intelligence Committee of Parliamentarians Act, the House of Commons designate the Standing Committee on Public Safety and National Security as the House committee responsible for conducting a comprehensive review of the provisions and operation of the Act.***

The Government takes note of this recommendation.

The review of the *National Security and Intelligence Committee of Parliamentarians Act*, required to take place five years after entry into force, has not yet begun. Both the timing of when the review starts and the committee to which the review is designated are decisions made by Parliament.

Recommendation 21: ***That the Government of Canada present to Parliament an annual assessment of threats to Canada's national security.***

The Government agrees to further examine this recommendation.

The Government of Canada, in continuing efforts to promote transparency, is exploring potential opportunities to provide Canadians an appreciation of Canada's established intelligence priorities. The Government Intelligence Priorities are developed on an annual basis, through discussion and consultation with the ministers representing Canada's security and intelligence community, and provide direction to departments and agencies with a collection mandate.

Beyond the Intelligence Priorities, the departments and agencies representing the Canadian security and intelligence community publish unclassified reports that are readily accessible to Parliament and the public. These include, for example, the Canadian Security Intelligence Service (CSIS) Public Report, the Royal Canadian Mounted Police (RCMP) Federal Policing Annual Report, the Communications Security Establishment's annual report, as well as the annual Departmental Plans and Department Results Report of federal departments and agencies, including Public Safety Canada.

Conclusion

The Government appreciates the insights and recommendations provided by the Committee, and this Report will be a valuable resource as the Government takes action to counter the threats posed by Russia to Canada's national security.

Sincerely,

The Honourable Dominic LeBlanc, P.C., K.C., M.P.
Minister of Public Safety, Democratic Institutions and Intergovernmental Affairs

C.C. The Honourable Bill Blair, P.C., M.P.
Minister of Defence

The Honourable Mélanie Joly, P.C., M.P.
Minister of Foreign Affairs

The Honourable Chrystia Freeland, P.C., M.P.
Minister of Finance and Deputy Prime Minister of Canada