SEPT. 18 SEPT. 2023
SESSIONAL PAPER
DOCUMENT PARLEMENTAIRE
8512-441-266
HOUSE OF COMMONS
CHAMBRE DES COMMUNES

Ken Hardie, MP
Chair of the Special Committee on the Canada-People's Republic of China Relationship
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 would like to thank the Special Committee on the Canada-People's Republic of China Relationship (CACN) for its report entitled "*A Threat to Canadian Sovereignty: National Security Dimensions of the Canada-People's Republic of China Relationship*". I am pleased to receive the Committee's Report and thank all the members for dedicating their time and effort.

The Government is deeply concerned by evidence of foreign interference emanating from the People's Republic of China (PRC), which represents a significant danger to Canada's sovereignty, prosperity, and social fabric. The Government remains firm in its resolve that foreign interference activities in Canada and violations of Canadian sovereignty are unacceptable. This includes malicious cyber activities, disinformation, intimidation and harassment, threats to Canada's economic security, the establishment of so-called overseas police stations, espionage, and covert and malicious influence in Canadian democratic processes. The Government reiterates that these threats do not emanate from the Chinese people, but from the PRC government itself.

The thirty-four Recommendations outlined in the CACN's Report seek a wide rage of actions by the Government of Canada to respond to the PRC's activities that may threaten our national security. Recommended actions include enhancing Canada's domestic security framework, including combating foreign interference and disinformation, investigating intimidation, and protecting democracy and democratic institutions and economic and research security. The Government takes these issues very seriously and our response will highlight that.

The Government agrees-in-principle with 17 of the Committee's 34 recommendations. While the Government does not disagree with any of the recommendations, it does take note of certain recommendations.

As this response will show, Canada is already addressing a number of the recommendations made by CACN and already has numerous policies in place to protect our population, sovereignty, and economic security. These policies touch on a wide range of the Government's mandate and the response to the recommendations reflects actions being taken by more than twenty different federal departments and agencies.

Once again, on behalf of the Government of Canada, I would like to thank the members of the CACN for the diligence and commitment undertaken in your work. Enclosed is the Government Response to the CACN Parliamentary Committee's Third Report.

Sincerely,

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

Recommendation 1: ***That the Government of Canada convey, to the Ambassador of the People's Republic of China to Canada, that any interference with the rights and freedoms of people in Canada is unacceptable, will not be tolerated, will result in serious consequences for those responsible, and will damage the bilateral relationship between Canada and the People's Republic of China.***

The Government agrees with this recommendation, and is already taking steps to address this issue.

The Government is deeply concerned by evidence of foreign interference emanating from China, which represents a significant danger to Canada's sovereignty, prosperity, and social fabric. The government remains firm in its resolve that foreign interference activities in Canada and violations of Canadian sovereignty are unacceptable. This includes malicious cyber activities, disinformation, intimidation and harassment, threats to Canada's economic security, the establishment of so-called overseas police stations, espionage, and covert and malicious influence in Canadian democratic processes.

Both the Prime Minister and the Minister of Foreign Affairs have delivered strong messages on foreign interference in meetings with their PRC counterparts, most recently by the Prime Minister to President Xi Jinping at the November 2022 G20 Summit in Indonesia, and by the Minister of Foreign Affairs to then-Foreign Minister Qin Gang at the G20 Foreign Ministers' meeting in India in March 2023.

Global Affairs Canada has made multiple formal representations to China's Ambassador to Canada regarding Chinese foreign interference, including on the topic of "police stations" in Canada. In each of these meetings officials clearly conveyed that Canada will not tolerate any form of foreign interference, and that such behaviour erodes trust in the bilateral relationship. In addition, foreign representatives in Canada have been warned that if they engage in foreign interference, they will be sent home.

Recommendation 2: ***That, in light of the allegations of threats and intimidation against people in Canada, the Government of Canada continue to ensure that all accredited diplomatic personnel of the People's Republic of China continue to act within the strict confines of their official responsibilities.***

The Government agrees with this recommendation.

The Government of Canada takes any allegation of inappropriate or illicit behaviour by foreign representatives in Canada extremely seriously. The government has clearly stated its expectation that China comply with Canadian and international law, including the Vienna Convention on Diplomatic Relations and the Vienna Convention on Consular Relations. The government's message to China has been consistent, whether from the Prime Minister, from the Minister of Foreign Affairs, or from officials at Global Affairs Canada: there is no tolerance for foreign interference on Canadian soil.

The Government will continue to do what is necessary to protect all Canadians from foreign interference, uphold their rights and freedoms, and defend Canada's national security and interests. On May 8, 2023, after careful consideration, the government declared Mr. Zhao Wei *persona non grata*. Mr. Zhao held the position of Consul at the Consulate General of the People's Republic of China in Toronto. This decision was not taken lightly.

Recommendation 3: ***That the Government of Canada work with provinces and territories to establish measures supporting individuals or groups in Canada who are the target of state-backed harassment and intimidation. The measures should include the establishment of a widely disseminated and single point of contact to which people can report incidents. The measures should also include coordination mechanisms with other orders of government to ensure that all incidents requiring investigation are addressed in a consistent and timely manner so that state-backed harassment and intimidation are effectively deterred and countered.***

The Government agrees with this recommendation in principle and is already taking steps to address this issue.

Community leaders are encouraged to remain vigilant and report any suspicious activity, incidents, and harassment to their local police, as well as the Royal Canadian Mounted Police (RCMP) Information Network. The Canadian Security Intelligence Service (CSIS) also has a general hotline, where Canadians can report any concerns, including those related to foreign interference.

On a broader scale, on March 6, 2023, the Prime Minister announced the creation of a Counter-Foreign Interference Coordinator within Public Safety Canada to coordinate efforts to combat foreign interference and give Canada's current and future efforts greater focus, coherence and effect. Rooted in international best practices, the Office of the Counter-Foreign Interference Coordinator will provide a dedicated focus on foreign interference, enabling the Government of Canada to shift to a more proactive and coordinated approach in addressing current and emerging threats. It will also enhance partnerships between federal departments and agencies, other levels of government, and non-government partners, acting as a focal point both within the Government of Canada but also with external stakeholders.

In addition, the Government of Canada has reporting mechanisms in place to signal suspected incidents of foreign interference. When Canada's security and intelligence agencies are made aware of such threats, they use every tool at their disposal to investigate and lay charges for foreign interference-related offences.

Budget 2023 proposed $48.9 million over three years for the RCMP to help protect Canadians from harassment and intimidation by foreign actors, to increase its investigative capacity, and to more proactively engage with communities at greater risk of being targeted.

The Canadian Security Intelligence Service (CSIS) investigates threats to the security of Canada, advises the Government of Canada on such threats, and, when appropriate, takes measures to reduce threats. CSIS remains steadfast in its efforts to increase public awareness, engagement, and access to national security information. As such it has prioritized engagement with academia, business leaders, provincial, territorial, municipal, and indigenous governments, community leaders, and members and advocacy groups who may be targeted by threat actors to seek different insights and perspectives, to provide important security information, inform national security investigations, and build trust and resilience with diverse communities.

Recommendation 4: ***That the Government of Canada make clear that attempts by the People's Republic of China to apply the National Security Law in an extraterritorial manner is unacceptable.***

The Government agrees with this recommendation.

Through a June 30, 2022, statement by the Minister of Foreign Affairs on the 25th Anniversary of the establishment of the Hong Kong Special Administrative Region, a joint statement with Australia, the United Kingdom, and the United States following the January 2021 arrest of 50 Hong Kong politicians and activists, as well as multiple démarches to the PRC and Hong Kong governments, the government has made clear its serious concern with the Hong Kong National Security Law (NSL), including the law's purported extraterritorial application. Together with our allies and partners, the government has stated that the NSL is a clear breach of the Sino-British Joint Declaration; that it undermines the 'One Country, Two Systems' framework; that it has curtailed the rights and freedoms of the people of Hong Kong; and that it is being used to eliminate dissent and opposing political views.

Most recently, on August 24, 2023, Canada's Head of Mission in Hong Kong met with Hong Kong Secretary for Security Chris Tang to raise Canada's strong concern over the international arrest warrants and bounties issued in July 2023 by Hong Kong authorities against eight pro-democracy activists currently in exile. The Head of Mission again raised Canada's ongoing concerns regarding the widespread impact of the NSL on rights and freedoms in Hong Kong.

Recommendation 5: ***That the Government of Canada advise provincial governments, as well as Canadian universities and research institutions about the threats from the People's Republic of China to national security and intellectual property. The advice should include explicit guidance against research partnerships and collaboration with universities, entities, and researchers from the People's Republic of China in the five sensitive areas identified by CSIS (artificial intelligence, quantum technology, 5G, biopharma, clean tech). The Government of Canada should also conduct ongoing outreach and provide resources to assist universities and research institutions in developing robust mechanisms to protect national security and intellectual property, while respecting academic freedom and institutional autonomy.***

The Government agrees with this recommendation.

In Budget 2022, Public Safety Canada received funding to establish the Research Security Centre which is responsible for providing research security-related outreach to academic institutions, provinces, and researchers across the country. Through a network of six regional advisors located across the country, the Research Security Centre disseminates advice, conducts research security workshops, and aids external stakeholders in accessing Government of Canada services and information. This work is complemented by the Canadian Security Intelligence Service's Academic Outreach and Stakeholder Engagement (program). The program aims to share information as widely as possible, within security and legislative restrictions, to build understanding of the threat environment across Canada. This in turn enables stakeholders, including the academic community, to work in partnership with the Government of Canada and build resilience against threat-related activity while respecting the fundamental importance of international collaboration in advancing science and respecting academic freedom and institutional autonomy.

The Government of Canada has regular engagement with provincial and territorial senior and working-level counterparts to support consistent information sharing on research security threats, and promote aligned approaches and responses, where possible. Innovation, Science and Economic Development (ISED) also maintains the Safeguarding Your Research portal, which includes useful information, advice, and online training courses on how to best safeguard research and intellectual property. This portal is regularly updated as new information becomes available. Budget 2022 also included $25 million ongoing for the Research Support Fund to build research security capacity within post-secondary institutions to identify, assess and mitigate potential risks to research security.

The Public Health Agency of Canada also plays a role in protecting sensitive research through its Centre for Biosecurity. The Centre advises regulated parties, which include Canadian universities and research institutions, about threats to national security and intellectual property through many stakeholder engagement activities and products.

In addition to other ongoing efforts to ensure that key stakeholders are made aware of threats to research security, the Communications Security Establishment (CSE) and its Canadian Centre for Cyber Security (Cyber Centre) serve as the single unified source of expert advice and guidance, services and support on cyber security for Canadians and Canadian organizations, including higher education institutions.

Recommendation 6: ***That the Government of Canada, through a ministerial policy directive, ban the federal granting councils from funding research connected with universities, entities, and researchers from the PRC in the five sensitive areas identified by CSIS.***

The Government takes note of this recommendation.

In July 2021, the Government of Canada released the National Security Guidelines for Research Partnerships, which integrates national security considerations into the development, evaluation and funding of research partnerships for applications received by the tri-agency granting councils – the Social Sciences and Humanities Research Council of Canada (SSHRC), the Natural Sciences and Engineering Research Council of Canada (NSERC), and the Canadian Institutes of Health Research (CIHR)– and the Canada Foundation for Innovation. The Guidelines state that applications assessed to present an unacceptable risk to national security and/or

where the risks cannot be appropriately mitigated will not be funded. The Government of Canada's approach to research security is country-agnostic, recognizing that risks evolve and can come from anywhere.

Additionally, on February 14, 2023, the Ministers of Public Safety, Innovation, Science and Industry, and Health announced new enhanced measures on research security affecting the Canada Foundation for Innovation, SSHRC, NSERC, and CIHR. These new measures will prohibit researchers working in sensitive technology research areas from applying for federal funding if they have any affiliations with universities, research institutes, or laboratories connected to military, national defence or state security entities of foreign state actors that pose a risk to Canada's national security.

Recommendation 7: ***That the Government of Canada explore the possibility of issuing security clearances for key individuals in the non-profit sector, private sector, universities, and research institutions to allow them to receive comprehensive briefings from Canada's security and intelligence agencies so that they can take appropriate steps to protect their intellectual property.***

The Government takes note of this recommendation.

To facilitate more open discussion on sensitive national security considerations in academic research, ISED and PS chair a classified information exchange roundtable. This roundtable is attended by Government of Canada departments, select Canadian university administrators, and representatives of Universities Canada and U15 Group of Canadian Research Universities. The Government of Canada facilitated the sponsoring of security clearances for these external stakeholders. The roundtable aims to develop situational awareness of, and facilitate the sharing of classified information related to the research security landscape to inform strategic policy directions and build resilience.

Recommendation 8: ***That the Government of Canada undertake a review of its national security legislation, prioritizing the Canadian Security Intelligence Service Act, with the objective of ensuring Canada's security and intelligence agencies can engage more effectively with universities and research institutions in furthering the protection of Canada's national security and intellectual property.***

The Government takes note of this recommendation.

The Government is continuously evaluating the legislative framework for national security in Canada, including the *CSIS Act*, to ensure it keeps pace with evolving threats. In doing so, the Government will seek to ensure the framework facilitates strong lines of communication where appropriate, including between universities and research institutions and government.

Recommendation 9: ***That the Government of Canada work with provincial governments to encourage Canadian education institutions to be fully transparent about their agreements with Confucius Institutes.***

The Government takes note of this recommendation.

Educational agreements remain within the purview of provinces and territories, however the Government of Canada regularly engages with provinces and territories to promote aligned approaches and responses to threats, such as foreign interference, where possible. An example of this engagement is through Public Safety Canada's Research Security Centre, where regional advisors are in constant engagement with provincial governments on threats to national security in the research and academic context.

Recommendation 10: ***That the Government of Canada implement the four recommendations of the National Security and Intelligence Committee of Parliamentarians to improve the Critical Election Incident Public Protocol, as listed in paragraph 14 of its 2020 Annual Report:***

a) the Protocol's mandate should capture all forms of foreign interference, from cyber interference to more traditional methods;

b) ***the membership of the Protocol's Panel should be composed of non-partisan individuals, including prominent Canadians, who may carry more weight in the highly politicized context of an election;***

c) ***the government should engage frequently and substantively with political parties on the Protocol's purpose and operation to ensure the widest understanding of the Panel's nonpartisan role and the process for intervention; and***

d) ***further thought should be given to how the Panel would inform Canadians of an incident of foreign interference, including issues of attribution***

The Government takes note of this recommendation.

The Plan to Protect Canada's Democracy (the Plan), established in 2019, is a whole-of-government and whole-of-society approach to safeguard Canada's elections and democratic institutions against interference and to further strengthen them. The Critical Election Incident Public Protocol (the Protocol) is part of this effort.

The Government's approach is continuously evolving. The Protocol has already undergone two independent evaluations, one following the 2019 General Election, and one following the 2021 General Election. Both found that overall, the Protocol works well and that it forms one part of Canada's broader toolkit to protect the integrity of its elections. Furthermore, in his First Report, the Independent Special Rapporteur on Foreign Interference noted that the 2019 and 2021 elections "were well-protected by sophisticated mechanisms and monitored by some of the most experienced non-partisan public servants in the country."

With regards to public notification of an incident that threatens Canadians' ability to have a free and fair election, the Panel evaluates whether incidents, as reported by the Security and Intelligence Threats to Elections (SITE) Task Force, meet the threshold for informing Canadians. If a public announcement is deemed necessary, the Protocol lays out a clear process for the Panel to inform Canadians and provides information on what an announcement would focus on. The Protocol specifies that attribution of interference attempts may be challenging or even impossible within the timelines of the caretaker period. As such, it does not require that attribution be included in a public announcement. Rather, it is expected that an announcement would include a focus on what Canadian electors can do to protect themselves.

Work is ongoing to continuously improve the ways in which the Government raises awareness of the threat of foreign interference among Canadians, including Parliamentarians. The "Countering an Evolving Threat: Update on Recommendations to Counter Foreign Interference in Canada's Democratic Institutions" report acknowledges that more work needs to be done to ensure broader awareness of both the threats facing Canada, including amongst political parties, and the measures put in place to address them. For instance, the Privy Council Office will develop a strategy to better communicate with Canadians about the Protocol and how it fits within the suite of measures to counter foreign interference and protect democratic institutions. Response to recommendation 11 provides more information about how the Government is engaging with political parties.

Recommendation 11: ***That the Government of Canada in its engagement with political parties provide information of specific application, including information about foreign interference regarding specific candidates and donors, rather than just information of a general nature, allowing political parties to take measures to counter foreign interference.***

The Government takes note of this recommendation.

A key element of the Plan to Protect Canada's Democracy is to continuously engage with political parties on security issues. In the lead up to and during election periods, political parties are invited to nominate key personnel that receive security clearances and are provided with classified briefings to help them strengthen their internal security practices and to build awareness of foreign-influenced activities in Canada. The Communications Security Establishment also created a dedicated 24/7 hotline for high profile clients, including political parties, to deal with any cyber security issues that may arise.

While opportunities may exist to provide briefings on specific threats, this will vary from case to case. Providing information of specific application will frequently be subject to necessary limitations, including national security considerations, privacy, and other legal protections including those upheld by the *Canadian Charter of Rights and Freedoms*. This presents a unique challenge, as the provision of information must be balanced against the legitimate need to protect sensitive information, investigations, and sources, to ensure security and intelligence agencies can continue to protect Canada and Canadians effectively.

Briefings are also provided to political parties outside of election periods. The Parliamentary Protective Service provides security briefings to incoming Members of Parliament. To equip elected officials with the tools to identify and protect themselves from foreign interference, CSIS also provides briefings to Parliamentarians. In 2021, CSIS provided 45 briefings to Parliamentarians, comprised of two Senators and 43 Members of Parliament. In 2022, CSIS provided 49 briefings with federally elected officials and CSIS continues to provide briefings to officials as necessary.

Recommendation 12: ***That the Department of Canadian Heritage take measures to counter the prevalence of People's Republic of China-influenced media in Canadian diaspora communities. Such measures could include, but are not limited to:***

- ***Enacting initiatives to counter misinformation and disinformation disseminated by actors associated with the Government of the People's Republic of China and targeted at Chinese diaspora communities in Canada, including the funding of projects through the Digital Citizen Initiative;***
- ***Identifying the ownership of media organizations related to the PRC in Canada and their activities in Canada, including but not limited to misinformation campaigns, censorship, and intimidation;***
- ***Exploring ways to flag and address misinformation and censorship on Chinese state-controlled social media apps such as WeChat and TikTok; and***
- ***Exploring ways to reduce/eliminate Chinese state-controlled social media's presence in Canada.***

The Government takes note of this recommendation.

The Government is committed to addressing online disinformation and its effects on communities across the country. To this end, the Department of Canadian Heritage's Digital Citizen Initiative (DCI), established as part of the Plan to Protect Canada's Democracy, provides time-limited financial assistance to researchers and civil society organizations in Canada to explore the origins, spread, and impact of online disinformation and to build citizen resilience to it. Through its contributions program, the Digital Citizen Contribution Program (DCCP), the DCI has supported 109 projects with $21 million in funding. By supporting the academic and civil society space in Canada focusing on disinformation, the Government seeks build resilience to disinformation and to make it harder for those who would spread it.

The DCCP has provided over $1 million in funding projects that study or build citizen resilience to disinformation affecting Chinese communities in Canada. For example, in 2022 the DCCP funded a project by the University of Waterloo entitled Disinformation on Private Messaging Applications in Select Ethnocultural Communities: Mitigation, Counter-Messaging, and Social Cohesion. This project studied the online experiences of newcomers to Canada from China with an eye towards identifying mitigation strategies to address disinformation in these communities. The project looked specifically at how chat groups across direct messaging applications, including WeChat, to identify how disinformation spreads.

To effectively counter disinformation targeting diaspora communities in Canada, the Department of Canadian Heritage engages with its national security partners who may leverage their mandate and expertise to counter misinformation and disinformation through the various tools available to them, including stakeholder engagement, intelligence assessments and when appropriate, threat reduction measures.

The DCI will continue to fund projects that seek to better understand and build resilience to online disinformation through its regular calls for proposals. The Government will take note of the recommendation to take measures to counter the prevalence of People's Republic of China-influenced media in Canadian diaspora communities in future calls for proposals.

The Government acknowledges the risks pertaining to Chinese state-controlled social media in Canada. However, reducing or eliminating the presence of any social media or online speech in Canada must strike a careful balance between ensuring Canadians have access to a healthy and diverse information ecosystem and maintaining an open and free internet while protecting freedom of expression as guaranteed by the Charter of Rights and Freedoms.

In addition to Canadian Heritage's DCI, the Canadian Centre for Cyber Security (Cyber Centre), housed within the Communications Security Establishment (CSE), has published advice and guidance on identifying misinformation and disinformation, as well as shared information on social media as part of the Government of Canada's efforts to help inform Canadians on how to help stop the spread and protect themselves from disinformation. In addition, CSE and its Cyber centre collaborate with various government agencies, the private sector, and international partners to monitor, analyze, and, where appropriate, disrupt disinformation campaigns, share threat intelligence, and provide guidance to protect critical infrastructure. CSE recently launched a public awareness series on how to identify misinformation, disinformation, and malinformation.

Global Affairs Canada (GAC) also plays a pivotal role in monitoring the digital information environment for foreign information manipulation, including state-sponsored disinformation. As part of the Plan to Protect Canada's Democracy, GAC houses Rapid Response Mechanism (RRM) Canada, which also serves as the permanent secretariat to the G7 RRM.

In 2023, as part of the Plan to Protect Canada's Democracy, the Government invested $5.5 million over three years to create the Canadian Digital Media Research Network (CDMRN), which is to be administered independently by the University of Toronto and McGill University. The CDMRN will seek to bolster Canada's information resilience and support strategies for improving Canadians' digital literacy.

Recommendation 13: ***That the Minister of Canadian Heritage issue an order under Section 7 of the Broadcasting Act to direct the Canadian Radio-television and Telecommunications Commission to a new broadcasting policy of general application that authoritarian state-controlled broadcasters not be on the List of non-Canadian programming services and stations authorized for distribution.***

The Government takes note of this recommendation.

The CRTC is the independent public authority responsible for regulating and supervising Canada's broadcasting system, and it ensures that Canadians have access to a diversity of programming services, both domestic and foreign. The *Broadcasting Act* sets out Canada's broadcasting policy objectives. The CRTC, as a quasi-judicial administrative tribunal and regulator, implements these objectives in the public interest, and outside of the political sphere.

The CRTC is the body responsible for authorizing the distribution of non-Canadian services in Canada, which it does by adding them on the List of non-Canadian programming services and stations authorized for distribution (the List). Non-Canadian services do not hold a licence in the same way that many Canadian channels do. Instead, the CRTC authorizes Canadian distributors to distribute those services, should they choose to do so, via the List.

The CRTC is well placed to assess which non-Canadian broadcasters should be available for distribution in Canada, and which ones should not. The CRTC relies on complaints from viewers or distributors to assess these services' compliance with Canadian regulations. Where it suspects non-compliance, the CRTC has the power to initiate a process to remove non-Canadian broadcasting services from the List and thus, from Canadian distributors.

In March 2022, the CRTC removed RT (Russia Today) and RT France from the List after it determined that RT's programming was not consistent with the policy objectives set out in the *Broadcasting Act*, and that its continued broadcast was not in the public interest.

Recommendation 14: ***That the Government of Canada introduce legislation to establish a foreign agents registry that would require any individual or entity, including former public office holders, to publicly declare any contracts or remuneration with a hostile state, as determined by the Government of Canada, or any entity affiliated with that hostile state.***

The Government agrees with this recommendation in principle and is already taking steps to address this issue.

In March 2023, the Government of Canada launched public and stakeholder consultations on a Foreign Influence Transparency Registry (FITR). The online consultations lasted 60 days and produced nearly 1,000 responses from a wide range of respondents across Canada. This feedback is being examined by Public Safety Canada officials to guide the design of a registry and associated legislation. Roundtable and bilateral discussions with stakeholders on FITR including with community organizations, Indigenous groups and provincial/territorial stakeholders – are ongoing.

Recommendation 15: ***That Public Safety Canada report regularly to the Standing Committee on Public Safety and National Security detailing the extent, targets, methods and objectives of the People's Republic of China's interference activities in Canada, and that the Government of Canada, through its national security and diplomatic architecture, take immediate steps to counteract any interference that is taking place.***

The Government takes note of this recommendation

The Government of Canada reports, to the extent possible, on the threat posed by foreign interference and actions taken to counter this threat at various fora, including appearances at different Parliamentary committees, such as the Standing Committee on Public Safety and National Security (SECU). CSIS appears at committees to support the Minister of Public Safety, and act as a subject matter expert, when SECU and other committees are conducting studies on pertinent topics, such as foreign interference. At these appearances, CSIS provides information, engages in transparent discussions, and responds to questions, several of which touch on foreign interference activities in Canada, tactics and objectives of hostile states, and measures to combat foreign interference. In 2022-2023, CSIS had a total of 14 Parliamentary appearances, three of which were at SECU. CSIS will continue to provide critical information on foreign interference to Canadians and engage with SECU and other Parliamentary committees.

CSIS also publishes annual reports to inform Parliament and the Canadian public about Canada's security environment – including foreign interference – as well as its national security role to counter these threats while upholding the rule of law and individual rights and freedoms. In these public reports, CSIS has pointed to three main threat actors known to undertake foreign interference activities in Canada: the PRC, Russia and Iran. These reports include specific examples of threat activities and tactics used by these threat actors. CSIS has also published multiple reports on foreign interference, including Foreign Interference and You, detailing specific threat activities and protective measures available to the public in order to spread awareness and build societal resilience.

Similarly, as part of the Plan to Protect Democracy, both CSIS and the Communications Security Establishment (CSE) have published reports outlining the foreign interference threat to Canada's democratic institutions. In 2021, CSIS published a *Foreign Interference Threats to Canada's Democratic Process* report. In 2017, CSE published its first Cyber Threats to Canada's Democratic Process report, and provided subsequent updates in 2019 and 2021 in advance of those federal election. Additionally, CSE has published the renewed *National Cyber Threat Assessment 2023-2024* – a bi-annual report that highlights how online foreign influence activities have become the new normal, with adversaries seeking to influence elections.

Recommendation 16: ***That, as part of a whole-of-government plan to counter foreign interference, the Government of Canada establish a national counter foreign interference coordinator to oversee a comprehensive response to foreign interference. This office should work with Canada's security and intelligence agencies to develop threat assessments, coordinate outreach with communities at risk of foreign interference, and increase public awareness of – and resilience to – foreign interference activities.***

The Government agrees with this recommendation and is already taking steps to address this issue.

As highlighted under Recommendation 3, in March 2023, the Prime Minister announced the creation of a Counter-Foreign Interference Coordinator within Public Safety Canada to coordinate efforts to combat foreign interference. Budget 2023 proposed $13.5 million over five years and $3.1 million ongoing to establish this function and Office.

Recommendation 17: ***That the Government of Canada adopt a policy whereby no single foreign vendor's products compose over 30% of the equipment in a private telecommunications vendor's network.***

The Government takes note of this recommendation.

Canada, along with its allies and partners, has taken numerous steps to support telecommunications equipment (or supplier) diversity within telecommunications networks. This has included committing to the Prague Proposals on Telecommunications Supplier Diversity and endorsing the Open RAN Principles in December 2022. These proposals recognize that diversifying telecommunications infrastructure markets will require long-term effort and commitment and that public policy efforts must evolve to accommodate network advancements, increasing digital connectivity needs, and evolving network risks.

In addition, Canada's May 2022 statement in relation to Securing Canada's Telecommunications System, which bans the use of Huawei and ZTE equipment from Canada's 5G networks, as well as the tabling of Bill C-26, will both provide new authorities to address security risks within Canada's telecommunications system.

On June 14, 2022, the Government of Canada introduced Bill C-26, *An Act Respecting Cyber Security (ARCS)*. This proposed legislation seeks to amend the *Telecommunications Act* and enact the *Critical Cyber Systems Protection Act (CCSPA*). Bill C-26 seeks to (1) add "security" as a policy objective for the *Telecommunications Act;* (2) establish a regulatory framework requiring designated operators to protect the critical cyber systems that underpin Canada's critical infrastructure; (3) provide a strong framework for the Government to take measures where cyber security risks may be inadequately addressed and (4) increase collaboration and cyber threat information sharing between government and industry.

The proposed framework would provide the Government of Canada with a clear and explicit legal authority to prohibit Canadian telecommunications service providers from using high risk products and services. This would allow Canada to take strong action against threats to the security of our telecommunications sector, in line with its security partners.

Recommendation 18: ***That the Government of Canada prohibit state-owned enterprises, partial state-owned enterprises, and technology companies of the People's Republic of China from obtaining federal contracts or sub-contracts related to information and communication technology or security equipment or services.***

The Government takes note of this recommendation.

The Government acknowledges the sensitive nature of global procurement of information and communications technology, security equipment, or services. The Government recognizes the importance of managing risk where there are security sensitivities, including in the procurement and contracting of information and communications technology and security equipment and services, and to take concrete measures to mitigate these risks. The

Government has multiple mechanisms available to address such concerns, including the prioritization of business with Canada's trade partners.

As committed in Budget 2023, the Government is currently undertaking targeted consultations on reciprocal procurement measures to ensure that goods and services are only procured from countries that grant Canadian businesses a similar level of access to their procurement markets.

The GC's May 2022 policy statement on telecommunications security acknowledged the need for new legislative tools to promote security within the telecommunications system. Planned amendments to the *Telecommunications Act* in Bill C-26, if adopted, would provide the Government with a clear and explicit legal authority to prohibit Canadian telecommunications service providers from using high risk products and services.

Recommendation 19: ***That the Government of Canada explore how it could require social media platforms operating in Canada that are connected to the People's Republic of China to disclose their practices with respect to the collection, use and transfer of user data, as well as their moderation or restriction of any user content.***

The Government of Canada agrees with this recommendation.

The *Personal Information Protection and Electronic Documents Act* (PIPEDA) is Canada's federal level, private sector privacy law. PIPEDA applies to private-sector organizations across Canada that collect, use or disclose personal information in the course of a commercial activity. Organizations which are subject to PIPEDA must be transparent with the public in how they comply with these obligations. Additionally, all organizations that operate in Canada and handle personal information that crosses provincial or national borders in the course of commercial activities are subject to PIPEDA, regardless of the province, territory or country in which they are based.

Many of the major social networks that exist today have a physical presence in Canada and PIPEDA therefore applies to their collection, use and disclosure of personal information. However, PIPEDA has been deemed by the Federal Court of Canada to apply to organizations outside of Canada, provided that they have a "real and substantial connection" to Canada.

In a case where a foreign organization exists outside of Canada but collects, uses or discloses personal information of Canadians, they may be deemed to have a real and substantial connection to Canada under PIPEDA. If this occurs, then PIPEDA will apply to their practices regarding collection, use and disclosure of personal information relating to Canadians in addition to their transparency requirements.

In June 2022, the Government introduced Bill C-27, the *Digital Charter Implementation Act*, 2022. This Bill seeks to strengthen Canada's private sector privacy law by proposing the *Consumer Privacy Protection Act* (CPPA) which would replace PIPEDA and thoroughly update and modernize its provisions, most notably around the Privacy Commissioner of Canada's enforcement powers. This includes, for example, the ability to order an organization to take any reasonable measure to address a problem or to cease a particular activity that is contravening the law, the ability to review assessments that organizations undertake when relying on the legitimate interest exception to consent, and the ability to initiate an audit where there are reasonable grounds to believe that the organization has contravened, is contravening or is likely to contravene the Act.

If the CPPA is enacted, Canada will have one of the most modern and comprehensive privacy laws in the world. It is anticipated that the CPPA would continue to apply in international contexts where there is a real and substantial connection to Canada.

Recommendation 20: ***That the government examine the establishment of criteria for the federal procurement of Information Technology equipment, whereby the Communications Security Establishment would automatically be called upon to conduct supply chain cybersecurity risk assessments and/or supply chain integrity assessments if certain conditions are met, including equipment application and country of origin.***

The Government takes note of this recommendation.

The Communications Security Establishment (CSE)'s Canadian Centre for Cyber Security (Cyber Centre) already provides, upon request, to Government of Canada departments and agencies, a supply chain cyber security risk assessment. This assessment provides departments and agencies with a better understanding of the supply chain risks related to the information communications technology products being considered for procurement.

During procurement, CSE supports Shared Services Canada (SSC) by conducting supply chain integrity (SCI) checks for information and communications technology (ICT)-related purchases intended for deployment in the Government of Canada's IT infrastructure. These checks are intended to identify security vulnerabilities or risks in the context in which the goods and services are purchased. If security risks are identified, CSE provides SSC with recommendations on mitigation measures to be put in place to reduce overall risk prior to the potential procurement.

SCI assessments provide advice, guidance, best practices, and mitigations that GC departments and agencies can consider when making decisions relating to their IT procurements. The Cyber Centre does not provide general assessments about companies, nor does it make statements to GC departments and agencies dictating procurement decisions.

Beyond the procurement of what are considered strictly Government of Canada IT assets, working with Public Safety Canada, the Cyber Centre, and other security and intelligence partners, Public Services and Procurement Canada (PSPC) is developing a screening tool to identify potential national security risks associated with products or services. Based on the level of risk identified from the planned screening tool, one potential risk mitigation measure that could be required is that an SCI assessment be completed.

Recommendation 21: ***That the Government of Canada collaborate with provinces, major national security agencies, and federal departments involved to improve our resilience to cyber-attacks.***

The Government agrees with this recommendation.

The Government of Canada is already working with provinces, national security agencies, and federal departments to improve Canada's cyber resilience. For example, provinces and territories have recently been invited to participate in cyber defence exercises alongside federal departments and agencies as part of the NATO Cooperative Cyber Defence Centre of Excellence's exercise, LOCKED SHIELDS 23. It is clear that increasing cyber resilience and security will only be possible by adopting a whole-of-society approach, which includes engagement with all stakeholders. Public Safety Canada is currently in the process of updating its National Cyber Security Strategy (the Strategy) as a mandate letter commitment. In developing this strategy, the Government of Canada has conducted public consultations to identify gaps and challenges that exist in the cyber realm. For example, workforce shortages have been identified as a key challenge to ensuring Canada's cyber resiliency, which will require close collaboration with provinces, territories, and other stakeholders in order to solve.

CSE and its Canadian Centre for Cyber Security (Cyber Centre), continues to collaborate and coordinate with partners across government to protect critical infrastructure and improve cyber security in Canada. For example, the Cyber Centre held briefings for Canadian critical infrastructure organizations, including the provinces and territories on the increased risk of cyber threat activity.

Recommendation 22: That Public Safety Canada report regularly to the Standing Committee on Public Safety and National Security on the extent and impact of organized crime, drug trafficking and concealing beneficial ownership information in Canada.

The Government takes note of this recommendation.

The Government recognizes that organized crime, drug trafficking and the misuse of legal entities due to the lack of beneficial ownership transparency is detrimental to Canadians and community safety. Transparency and information sharing, including public reporting both domestically and internationally, is a key part of the overall approach to building a safer and more resilient Canada.

Domestically, the Government advances reporting through a range of fora. For example, the annual public Statistics Canada crime report shares critical data and statistics on offences related to organized crime, including money laundering, smuggling and homicides. In addition, the Criminal Intelligence Service of Canada's *Report on Organized Crime in Canada* provides an annual public assessment of organized crime groups operating in Canada, the serious threats they pose, and the impacts they have on Canadian communities. Furthermore, from a law enforcement perspective, the Royal Canadian Mounted Police shares publicly the *Federal Policing Annual Report,* which highlights achievements, priorities and threats in relation to combatting organized crime. Similarly, to address drug trafficking, the Government ensures it shares critical information by way of informative reports.

The Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) also reports publicly through its annual report on its efforts to support law enforcement investigations and the combatting of illicit financial flows that enable organized crime, drug trafficking and money laundering. To demonstrate the importance of beneficial ownership transparency, an initial set of legislative amendments to the *Canada Business Corporations Act* (CBCA) received Royal Assent on June 23, 2022. Under these amendments, Corporations Canada will be required to make certain information public, while introducing an exemption regime to protect certain categories of individuals.

As outlined above, public reporting and disclosure is already a key pillar of the approach to combating organized crime, drug trafficking and the lack of transparency associated with beneficial ownership information in Canada. The Government would support any study undertaken by the Standing Committee on Public Safety and National Security.

Recommendation 23: ***That the Government of Canada explore ways to target organized crime groups and prevent them from entering Canada and expanding or forming alliances in Canada.***

The Government takes note of this recommendation.

Organized crime poses a serious threat to the safety and security of Canadians and Canadian institutions. To combat this threat, the Government of Canada has a strong and robust framework in place to target organized crime networks operating in Canada and to prevent additional organized crime groups (OCGs) from entering the country through a number of targeted global strategies and initiatives.

The Government utilizes a joint response to counter OCGs, particularly through cooperation among the RCMP, Canada Border Services Agency (CBSA), PS, and FINTRAC. These agencies work together and actively engage with partners to develop assessments and screening tools to evaluate and monitor global OCG threats, identify and disrupt OCGs present in Canada, increase understanding of emerging trends, strengthen information sharing, and help target, disrupt and dismantle organized criminal networks that threaten Canada and those who live in Canada. This includes the RCMP's participation in the Canadian Integrated Response to Organized Crime (CIROC), which coordinates a national effort to disrupt organized crime.

Budget 2023 confirmed the Government's intention to develop a Canada Financial Crimes Agency (CFCA), which will strengthen efforts to combat OCGs. The CFCA will bring together the expertise necessary to increase money laundering charges, prosecutions and convictions, and asset forfeiture results in Canada. The Government committed in Budget 2023 to provide further details on the structure and mandate of the CFCA in the Fall Economic Statement 2023.

Beyond Canada, the RCMP's International Network aims to identify, prevent, disrupt and deter criminal activity before it reaches Canada or impacts Canadian interests. To do this, the RCMP

promotes international law enforcement cooperation and operational efforts towards combating all forms of transnational crime, as well as deployments which include 14 resources deployed to the Indo-Pacific region. These international efforts are crucial in the fight against organized crime activity with a nexus to Canada and the relationships developed through international partnerships are fundamental in ensuring that Canada responds to the globalized threats posed by transnational and serious OCGs.

As organized crime becomes increasingly globalized and sophisticated, Canada is committed to advancing unified strategies and policies to address and combat transnational and serious organized crime.

Recommendation 24: ***That the Government of Canada expand its proposed beneficial ownership registry to include real estate and entities incorporated under provincial law.***

The Government takes note of this recommendation.

In Canada, responsibility for corporate law is shared among federal, provincial and territorial (FPT) governments. Corporations Canada and its provincial and territorial counterparts maintain registries of all companies incorporated under the laws of their respective jurisdictions.

Representatives from the federal, provincial and territorial governments have collaborated since 2016 through an FPT working group on measures designed to increase beneficial ownership transparency. As a result of this work, the majority of provinces and territories have amended their domestic legislation to require business corporations to maintain records about their beneficial owners at their corporate head office.

In Budget 2022, the Government committed to work with provincial and territorial partners to advance a national approach to a beneficial ownership registry of real property similar to other countries including the United Kingdom. In Budget 2023, the federal government noted that it would continue to call upon provincial and territorial governments to advance a national approach to beneficial ownership transparency to strengthen the fight against money laundering, tax evasion, and terrorist financing.

As part of the Government's outreach to provinces and territories, the Minister of Innovation, Science and Economic Development Canada (ISED) and the Minister of Finance and Deputy Prime Minister sent a joint letter to their respective Ministerial counterparts on June 5, 2023 requesting their continued commitment to strengthen corporate ownership transparency in Canada and an agreement in principle to work together to establish a pan-Canadian beneficial ownership approach that would cover all Canadian corporations while respecting jurisdictional responsibilities for corporations.

On March 31, 2023, Quebec launched a public beneficial ownership registry, which covers corporations incorporated in Quebec and all other legal entities registered to do business there. British Columbia passed legislation to create a public beneficial ownership registry, which they plan to launch in 2025.

The Government of Canada is engaging with Quebec and British Columbia to explore business and technical requirements that could ultimately support unified, pan-Canadian access to beneficial ownership information. Several other provinces and territories have expressed an interest to observe these discussions.

Recommendation 25: ***That the Government of Canada explore ways to increase access to information regarding infectious disease outbreaks in the People's Republic of China through international entities like the World Health Organization.***

The Government agrees with this recommendation.

PHAC monitors and reports on international cases of certain infectious diseases and receives data from countries, including China, through the World Health Organization (via the Health Portfolio Operations Centre) or from public websites. The Global Public Health Intelligence

Network (GPHIN) will also maintain its capacity to undertake event-based surveillance in Chinese languages and will share information with the WHO's Epidemic Intelligence from Open Sources (EIOS) system.

Negotiations on proposed amendments to the International Health Regulations (IHR, 2005), will seek to advance strengthened information sharing requirements for IHR (2005) States Parties with respect to the sharing of timely and sufficiently detailed information about public health events, which could include information about infectious disease outbreaks. Any amendments will have to be agreed by consensus of all IHR (2005) States Parties, including China. A package of amendments to the IHR (2005) is expected to be presented for adoption by the 77th World Health Assembly in May 2024.

Recommendation 26: ***That Health Canada, through the Public Health Agency of Canada, study Taiwan's pandemic response and explore ways to increase information sharing with public health agencies in Taiwan.***

The Government agrees with this recommendation.

Efforts are underway to strengthen the Health Portfolio's engagements with Taiwan, including to enhance information-sharing efforts with public health agencies.

On May 9th, 2023, Canada's Health Portfolio entered into a Memorandum of Understanding (MOU) with the Taiwan Ministry of Health and Welfare as a mechanism to enhance health cooperation. The MOU aims to focus and maximize the impacts of engagement with Taiwan on issue areas of strategic advantage to Canada, including global health security, digital health, health products, mental health, and non-communicable diseases. Cooperation will occur via the exchange of best practices, sharing of expertise, consultations, and collaborative research projects.

Canada also continues to support Taiwan's meaningful participation in international organizations and technical fora where there is a practical imperative and where Taiwan's absence would be detrimental to global health interests. This includes Taiwan's participation as an observer in the World Health Assembly (WHA), in which Taiwan's engagement would facilitate greater information sharing between Taiwan and the global health community.

Recommendation 27: ***That Global Affairs Canada designate an individual to serve as a dedicated advocate for Canadians, regardless of where they were born and Canadians who hold dual citizenship, who are arbitrarily detained abroad, whose responsibilities include but are not limited to:***

- ***Working with countries and multilateral organizations to promote the Declaration Against Arbitrary Detention in State-to-State Relations to more jurisdictions.***
- ***Assisting with consular affairs regarding Canadians who are arbitrarily detained abroad.***
- ***Exploring ways to protect Canadians from the practice of arbitrary detentions, more particularly in state-to-state relations.***

The Government agrees with this recommendation.

The Minister of Foreign Affairs takes her responsibility seriously when it concerns the conduct of diplomatic and consular relations on behalf of Canada. Her current mandate letter also includes a specific commitment to "continue to expand the broad coalition of states supporting Canada's initiative to condemn and eradicate the practice of arbitrary detention and advancing an action plan to coordinate collective international responses to specific incidents of arbitrary detention."

Under the Minister's authority, the Assistant Deputy Minister (ADM) of Consular Affairs is the senior official who is designated to lead on responding to individual cases of arbitrary detention of Canadians, as well as for working with countries and multilateral organizations on the promotion of the Arbitrary Detention Initiative, which includes the Declaration Against Arbitrary Detention in State-to-State Relations and its accompanying Partnership Action Plan.

The ADM of Consular Affairs coordinates Canadian activities advancing the Initiative by seeking to increase the number of endorsements of the Declaration through regional outreach and implementing the Action Plan through activities that include engaging with academics and civil society organizations to deepen understanding and support advocacy and furthering the development of international law and norms in order to increase deterrence.

The Declaration reaffirms international obligations under the Vienna Convention on Consular Relations, including the provision to allow consular access to detained nationals, including those with multiple citizenship. That is to say, no foreign nationals are to be arrested, detained or sentenced for diplomatic leverage, and refused consular access, regardless of other citizenship status. As each consular case is unique, the department takes a tailored approach and adapts individual interventions to each local context and circumstance. The Government of Canada allows Canadians to hold multiple citizenships and does not make distinctions in its provisions of services abroad based on this. However, not all countries recognize multiple citizenships and may prevent consular access to those they consider to be nationals of that country. Canadian consular officials will always advocate for consular access to, and the rights of all Canadians detained abroad, regardless of multiple citizenship status.

Recommendation 28: ***That, as part of a whole-of-government plan to protect Canada's interest and sovereignty in the Arctic, the Government of Canada increase investment in scientific research and security of waterways, energy resources, mineral deposits, and critical technologies.***

The Government agrees with this recommendation.

Arctic and northern research in Canada is carried out by a wide range of federal, provincial and territorial governments, academia, the private sector, Indigenous and northern organizations, non-governmental organizations, together with a wide range of international players. It is increasingly carried out in partnership with, or under the leadership of, Indigenous communities and organizations, to ensure local knowledge and Indigenous knowledge and approaches are incorporated appropriately and meaningfully in all phases of research planning and implementation. Domestic and international collaboration and coordination are particularly important given the complexities, interconnectedness and high costs related to Arctic and northern science and research.

Over the past two decades, the Government has made significant investments that have collectively enhanced Canada's position on the global map of leading nations in Arctic and northern science. These include: the construction of the world-class Canadian High Arctic Research Station and other infrastructure investments through the Canada Foundation for Innovation and the Arctic Research Infrastructure Fund, and upgrades to Canada's network of meteorological stations such as Eureka; the establishment of Polar Knowledge Canada as the federal organization responsible for advancing Canada's knowledge of the Arctic and strengthening Canadian leadership in polar science and technology; logistical support through the Polar Continental Shelf Program; and program investments such as the International Polar Year, the ArcticNet Network of Centres of Excellence and Amundsen Science, Tri-Council core funding programs, and more.

In respect of investments in security of energy resources and mineral deposits, Natural Resources Canada's Polar Continental Shelf Program (PCSP) facility in Resolute Bay, Nunavut, is one of a handful of federal multi-use infrastructure presences in the Canadian Arctic.

PCSP's mandate is to provide safe, efficient, and cost-effective logistics in support of science, sovereignty, and federal government priorities, particularly in Canada's North. It delivers air and field logistics support each year to scientific field projects, federal operations, and training projects. PCSP shares the resolute Bay facility with the Canadian Armed Forces Arctic Training Centre, where it is used to stage Arctic training and exercises.

Natural Resources Canada (NRCan) and the Department of National Defence (DND) are exploring expanding this arrangement to other appropriate multi-use infrastructure in the North to facilitate science and sovereignty operations under their respective mandates. More

information on DND and the Canadian Armed Forces' (CAF) investments into the Arctic can be found under recommendation 29.

NRCan manages the Geo-Mapping for Energy and Minerals (GEM) program, now in its third iteration ($100 million over seven years — 2020-2027), focuses on mineral potential, including critical minerals, and sustainable land use for economic development in Canada's North (north of the 57th parallel) in the context of a changing climate. The geoscience knowledge generated through the program's research helps mineral exploration in the North and Northern governments and communities plan land use and successfully develop the infrastructure that supports economic development.

Recommendation 29: ***That the Government of Canada recognize the threat to Canadian Arctic sovereignty posed by the PRC in a renewed defence policy and commit the necessary resources to protect Canada's Arctic.***

The Government of Canada agrees with this recommendation.

The Government recognizes growing interest and activity in the region by Arctic and non-Arctic states alike, with some using a broad range of military and state-controlled assets to position themselves to access or control sensitive sites, infrastructure, and strategic resources. As a result Canada will continue to monitor for malign activities and, as the Arctic becomes increasingly accessible, be prepared to detect, deter, and defend against an even greater range of threats.

Canada's 2017 defence policy, *Strong, Secure, Engaged (SSE),* commits to exercising the full extent of Canada's sovereignty in Canada's North and continuing to carefully monitor military activities in the region and conduct defence operations and exercises as required. Notably, *SSE* commits to further strengthening the Canadian Armed Forces (CAF)'s ability to monitor and, if necessary, respond to threats in the Arctic through the integration of a range of new sea, land, air and space capabilities into a 'system-of-systems' approach to Arctic surveillance. These commitments are further reinforced in the 2019 whole-of-government *Arctic and Northern Policy Framework*, and in subsequent mandate letters to the Minister of National Defence.

As a result of this policy guidance, Canada is making significant investments to enhance the CAF's mobility, reach, and ability to operate in the Arctic, including through the acquisition of a new fleet of F-35 fighter aircraft; space-based surveillance and communications capabilities; remotely piloted aerial systems; and six ice-capable Arctic and Offshore Patrol Ships (AOPS), three of which are already in the water, with the other three anticipated to be delivered by 2025. In addition, work is ongoing to complete the Nanisivik Naval Facility, which is expected to become operational in August 2025 and serve as a refueling site for Royal Canadian Navy and other Government of Canada vessels. The CAF also maintains the ability to operate effectively in the North through annual operations. For example, Operation NANOOK, the CAF's signature Arctic training operation, strengthens the CAF's ability to project and sustain forces in the Canadian Arctic, in collaboration with domestic and international partners and allies.

Moreover, Canada's NORAD modernization plan announced in June 2022 and supported by an investment of $38.6 billion over twenty years will deliver a number of capabilities that will bolster continental defences and support the Canadian Armed Forces' presence and operations in the Arctic. These include: next-generation surveillance for the North, including new Arctic and Polar Over-the-Horizon Radar systems; expanded air-to-air refueling capability and upgraded Northern basing and other infrastructure upgrades to better sustain operations and expand the CAF's reach in the region, including to accommodate the F-35; and dedicated new research, development and innovation funding for the defence of North America, with a significant focus on the Arctic. These investments will support the CAF's ability to detect, deter, and defend against emerging and future threats, including in the northern approaches to Canada and North America and through NORAD.

Finally, in Budget 2022 the Government of Canada committed to conduct a review of SSE in order to update it for a world that has become less secure and less predictable. Updating Canada's defence policy will be vital to ensuring that the Defence Team has the necessary

direction, resources, and future-ready capabilities to adapt to an increasingly dynamic and complex operating environment, including in the Arctic. Notably, the need to strengthen the resilience of Canada's Arctic region and the CAF's readiness and capacity to operate there are key considerations as the Government updates the defence policy.

The Department of Fisheries and Oceans (DFO) and the Canadian Coast Guard (CCG) support whole-of-government efforts in the Arctic with their expertise and maritime surveillance capabilities. DFO and CCG are fulfilling their mandate by providing ships, aircraft, and other maritime services in support of other government departments and agencies. This includes new law enforcement and security departments and agencies, such as the RCMP and CBSA.

Recommendation 30: ***That the Government of Canada expand its work with Indigenous communities in the Arctic to respect Indigenous rights while ensuring the security of Indigenous groups and Canadian sovereignty.***

The Government agrees with this recommendation.

The Government of Canada continues to take steps to explore new opportunities to support Indigenous Peoples in the Arctic, meaningfully engage with communities across Inuit Nunangat and more broadly in the North, and expand cooperation through its international commitments and projects to maintain security and sovereignty in the region.

The *Arctic and Northern Policy Framework's* vision – strong, self-reliant people and communities working together for a vibrant, prosperous and sustainable Arctic and Northern region at home and abroad, while expressing Canada's enduring Arctic sovereignty – reflects the goals and objectives co-developed with Indigenous, territorial and provincial partners.

Reconciliation is both a goal of the Framework and a guiding principle that runs through all of its other goals and objectives. Under the Framework, Crown-Indigenous Relations and Northern Affairs Canada (CIRNAC) collaborates with northern and Indigenous partners to support the social and political self-determination that underpins reconciliation and continuously engages with other government departments to ensure Indigenous and northern communities are meaningfully consulted on and benefit from efforts to defend Arctic sovereignty. This has included engagement through the Arctic and Northern Policy Framework Leadership Committee, chaired by the Minister of Northern Affairs, and supporting officials-level Working Groups.

Goal #7 of the Framework, *The Canadian Arctic and North and its people are safe, secure, and well-defended*, underscores the importance the Department of National Defence and Canadian Armed Forces (DND/CAF) places on the collaboration with other government departments, Indigenous and Northern peoples and communities, and international partners to enhance its ability to operate in the Arctic. A key example of this partnership is DND's ongoing efforts to build relationships with Northern territorial and Indigenous governments and organizations at the strategic and local level in the last several years in its efforts to modernize NORAD in its Northern Basing Infrastructure project. Furthermore, Joint Task Force North (JTFN) routinely engages territorial and Indigenous governments and organizations as part of CAF planning and activities in the Arctic. An essential element of Operation NANOOK— the CAF's signature Northern operation—involves engaging with Northern and Indigenous partners, territorial emergency planners, and other government departments to identify threats to Northern communities, create pre-crisis communication networks and plan for disaster response to support community security and development.

Canada is also a signatory to the *Agreement to Prevent Unregulated High Seas Fisheries in the Central Arctic Ocean* (CAOFA), which entered into force in June 2021, and includes many like-minded Arctic states. Canada works closely with like-minded Arctic states at the CAOFA to promote multilateral cooperation and information sharing with the objective of preventing unregulated commercial fishing in the high seas portion of the Central Arctic Ocean (CAO).

DFO has championed the effective inclusion of Indigenous Knowledge and Indigenous participation within the CAOFA governance mechanisms. Furthermore, it continues to support

the meaningful participation and engagement of representatives of Arctic communities in the development of the Agreement's scientific programs, and ensure that the emerging body of science equally recognizes and considers scientific, Indigenous and local knowledge systems.

It is critical that Canada support Indigenous and Arctic communities as they face hostile activities from foreign states seeking to target communities and exploit natural resources. The underdevelopment of infrastructure in Arctic communities is a significant vector for hostile state activity and while some foreign investments can bring economic benefits to the region, they also afford foreign states access to target communities for their strategic gain, to Canada's detriment.

Recommendation 31: ***That the Government of Canada work with like-minded Arctic states to promote multilateral cooperation, information sharing and collective security/defence.***

The Government agrees with this recommendation.

Canada continually advances its national and international Arctic interests by cooperating with key Arctic partners to ensure a well-governed region supported by legal frameworks. Canada's key partners in the Arctic include the United States and our Nordic allies: Kingdom of Denmark, Finland, Iceland, Norway, and Sweden.

The Arctic Council is the leading multilateral forum through which Canada advances its Arctic interests internationally. Canada has been actively working with like-minded Arctic states and with Indigenous Permanent Participants on the joint commitment to the enduring value of the Arctic Council for the benefit of circumpolar cooperation, and northern and Indigenous communities in Canada.

Within and beyond the Arctic Council, the Government is liaising with its international partners in international fora to promote multilateral cooperation on topics relating to emergency protection and preparedness response in the Arctic. These fora provide an opportunity for members to discuss collaborative emergency response and preparedness measures. They also provide an opportunity for likeminded members to discuss the exchange of information regarding significant maritime events in the Arctic such as search and rescue operations, illegal, unreported and unregulated fishing, and maritime disputes, and to work together in developing tools, methodologies, and exercises that promote coordination and collaboration on marine environmental response, radiation, search and rescue, wildfires, and other incidents involving other hazards in the Arctic context. Notably, Canada is a member of the Arctic Coast Guard Forum (ACGF), which is an independent, non-treaty bound, informal, operationally-driven organization that aims to foster safe, secure, and environmentally responsible maritime activity in the Arctic.

Canada continues to promote its vision for a stable and secure Arctic region, including through participation in annual foreign ministry dialogues on Arctic security issues with likeminded Arctic states. Canada is also deepening defence cooperation with like-minded Arctic nations, including through meetings at the Chiefs of Defence and ministerial levels. These fora allow Canada to exchange perspectives on Arctic defence and security issues and will continue to provide valuable opportunities for collaboration on strategic challenges moving forward.

With the United States, Canada's closest Arctic ally and partner in Arctic defence, Canada will continue to deepen collaboration through regular engagements, including through the Canada-U.S. Arctic Dialogue. Canada is also working closely with the United States to ensure the North American Aerospace Defense Command (NORAD) is modernized to detect, deter, and defend against evolving aerospace threats to North America, including in our Arctic and Northern regions. Canada's investments will help strengthen its capacity for Northern operations and contribute to defence and security in the Arctic, including through new Arctic and Polar Over-the-Horizon-Radar, space-based surveillance and communications, capabilities to improve operational mobility and sustainability in the North and Arctic, and investments in Northern basing.

Recommendation 32: ***That the Government of Canada explore ways to reduce non-Arctic***

states' influence on/participation in resource exploration and exploitation, fishing, and scientific research in the Arctic.

The Government takes note of this recommendation.

The Government of Canada is committed to preserving Arctic state leadership in managing the Arctic region. In pursuit of this goal, Canada cooperates closely with domestic partners and like-minded Arctic states on a variety of issues including Arctic governance, resource development, fisheries, and scientific research. At the same time, the Government of Canada recognizes the benefits of pursuing cooperation with non-Arctic states on certain issues that advance our national interests. For example, foreign investment and international scientific exchanges have the potential to improve the lives of Northerners and contribute to strong and healthy Arctic peoples and communities. However, we are not complacent and recognize that some foreign investment and activities could seek to advance interests that may be in opposition to those of Canada. For this reason, Canada will continue to balance needed economic development while ensuring that the security and interests of Canada and its Northerners is maintained.

The Canadian Minerals and Metals Plan and Critical Minerals Strategy seeks to encourage a competitive, sustainable and responsible minerals and metals sector and recognize the importance of attracting Foreign Direct Investment (FDI) to address the substantial capital requirements of an industry that creates economic opportunities, drives economic growth and competitiveness, and secures more resilient supply chains. They also recognize that these objectives must be balanced with the protection of Canadian assets and the promotion of stronger Canadian ownership. As an investigative body under the *Investment Canada Act*, NRCan contributes to national security reviews of foreign investments, including in the mining sector, which can affect Arctic security. These reviews assess mining assets, such as deposits, operations, processing facilities, and related infrastructure deemed strategically important due to their economic significance, potential impact on supply chains, or their role in supporting critical industries.

On October 28, 2022, the Minister of Innovation, Science and Industry announced a new policy under the *Investment Canada Act* (ICA) on foreign investments in critical minerals. The policy states that significant transactions by foreign state-owned enterprises in Canada's critical minerals sectors will only be approved as of likely net benefit on an exceptional basis. These transactions will also be subject to enhanced scrutiny under the ICA's national security review process.

On Arctic fisheries, Canada's approach is guided by international law, including the *UN Convention on the Law of the Sea* (UNCLOS). The CAO falls outside the exclusive economic zone of any Arctic Ocean coastal state. It is therefore considered part of the high seas and all States may exercise a number of freedoms in this area, including with respect to fishing and scientific research (subject to conditions outlined in UNCLOS and other relevant instruments).

Fishing activities in the CAO are guided by the CAOFA, an initiative of the Arctic Ocean coastal states, which entered into force in June 2021. The Agreement brings together Canada, other Arctic Ocean coastal states (Denmark, on behalf of the Faroe Islands and Greenland, Norway, Russia, and the United States), but also additional parties with an interest and potential capacity to fish in the CAO (European Union, China, Japan, South Korea, and Iceland). The intent of the Agreement is to: (1) prevent unregulated commercial fishing in the high seas portion of the CAO; (2) improve the scientific knowledge of the area; and, (3) determine whether fish stocks might exist that could be harvested on a sustainable basis in the future. The Agreement will be in force for an initial period of 16 years (until June 2037). The CAOFA includes a number of deliverables that the Parties have committed to implementing including a Joint Program of Scientific Research and Monitoring (JPSRM) and conservation and management measures for exploratory fishing.

All Parties to the Agreement, which includes both Arctic and non-Arctic states, have rights to participate in and be privy to the scientific research undertaken pursuant to the Agreement, and will have rights to any high seas fisheries that could result in the future. Fisheries and

Ocean Canada's (DFO's) participation in the CAOFA is consistent with Canada's priorities to combat illegal, unreported and unregulated fishing.

Recommendation 33: ***That the Government of Canada explore ways to increase security cooperation and cooperation on artificial intelligence, critical technologies and infrastructure with like-minded countries in the Indo-Pacific region and multilateral organizations.***

The Government agrees with this recommendation.

The recently adopted Indo-Pacific Strategy (IPS) recognizes the significance of the region for Canada's long-term growth, prosperity and security. It specifically recognizes the necessity to expand security cooperation in the region as well as the growing importance of artificial intelligence, critical technologies and infrastructure as highly strategic domains on which cooperation with Canada's partners must be reinforced. Continued cooperation among partners on emerging technologies and defence innovation will be integral to demonstrate unity and defend shared interests.

Under its Indo-Pacific Strategy (IPS), the Government will expand regional defence and security programming and support new partnership initiatives starting in 2023-2024. For instance, the government will launch a new cyber governance and security initiative to increase regional engagement on cyber issues, bolster cyber security capacity, and strengthen partnerships in defence, law enforcement, and security with partners in the Indo-Pacific.

These security cooperation efforts will complement the defence-related initiatives under the IPS which include augmenting Canada's naval presence in the Indo-Pacific, enhancing Canadian Armed Forces' participation in regional multilateral exercises, and building the capabilities of regional partners' armed forces, including a specific focus on Women, Peace and Security. Canada will work closely with likeminded partners in the Indo-Pacific, as well as with our Five Eyes partners, to support these initiatives and to increase defence and security cooperation in the region.

With respect to artificial intelligence, the Government had begun exploring opportunities to expand cooperation on artificial intelligence with Japan under the Six Shared Priorities Action Plan agreed to in 2022 and with South Korea under the Canada-South Korea Comprehensive Partnership Agreement adopted in 2023. Canada also supports the G7 Hiroshima Process on Artificial Intelligence and looks forward to collaborating with G7 partners on this issue. Separately, the Government participated in the 2023 Summit on Responsible Artificial Intelligence in the Military Domain (REAIM) which was co-hosted by the Netherlands and the Republic of Korea (ROK).

Recommendation 34: ***That the Government of Canada undertake a comprehensive national security review that culminates in the publication of a national security policy. The review should include an assessment of the effectiveness of the current national security approach, laws, and practices that identifies areas where improvements can be made; an assessment of the role and mandate of key national security agencies; and an examination of the role played by international cooperation in Canada's national security approach and opportunities for enhanced cooperation.***

The Government takes note of this recommendation.

The Government of Canada is continuously evaluating the legislative framework for national security in Canada to ensure we keep pace with evolving threats.

Public Safety Canada has led preparations for the statutorily required parliamentary review of the *National Security Act, 2017* (former Bill C-59). Bill C-59 enacted new national security review bodies within the Government of Canada, established the Intelligence Commissioner, and enacted the *Communications Security Establishment Act*, among numerous other reforms and key legislative components. A review of Bill C-59 could feed into an examination of the national security landscape and impact any resulting policies or strategies.