Minister of Public Safety,
Democratic Institutions
and Intergovernmental Affairs

Ministre de la Sécurité publique,
des Institutions démocratiques
et des Affaires intergouvernementales

Ottawa, Canada K1A 0P8

The Honourable John MacKay, M.P.
Chair of the Standing Committee on National Defence
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 Fifth Report of the Standing Committee on National Defence, The Cyber Defence of Canada. I would like to commend the Committee for its efforts to examine this important topic.

Recommendation 1: ***That the Government of Canada establish an ongoing multistakeholder platform for collaboration and engagement on cybersecurity issues. The objectives of this platform could be modelled after the Industry 100, in the United Kingdom. It should be established to create a collaborative space where industry and cyber officials meet to exchange information, best practices and establish forms of reporting private sector cyberattacks to lead to better information sharing and prevention of future attacks.***
The Government of Canada supports this recommendation.

The Government of Canada supports this recommendation.

The National Cyber Security Strategy Mid-Term Review found that a strong and secure digital environment will depend on enhanced collaboration across federal organizations, as well as with a broad range of stakeholders nationally and internationally. In the Review, it was recommended that national key stakeholders increase collaboration to ensure Canadian systems are secured against existing and emerging threats.

The Government of Canada recognizes that protecting Canada’s cyber security requires cooperation at all levels of government and with industry. New and meaningful relationships with industry need to be created and leveraged to find solutions to Canada’s cyber security challenges.

Under Canada's 2018 National Cyber Security Strategy, the Government of Canada created the Canadian Centre for Cyber Security (Cyber Centre) as part of the Communications Security Establishment (CSE) as the single unified source of expert technical advice, guidance, and services for Canada. To advance this mission, the Cyber Centre has developed close relationships with stakeholders across Canada in the private sector, academia, and other levels of government and hosts many multi-stakeholder platforms for collaboration. For example, the Cyber Centre hosts a bi-weekly joint threat brief with representatives from several sectors, including health, academia, transport, energy, Internet Service Providers, the Defence Industrial Base, Crown Corporations, and provinces and territories. Some sectors also have sector-specific community calls.

The Cyber Centre has also begun to host on-site sector-specific workshops to meet with IT security professionals and senior executives to identify areas of cyber security concern, and work on solutions to mitigate these concerns. Recent examples include sector-specific briefings as well as the Federal, Provincial, Territorial Roundtable, and Canadian Gas Association / Independent Electricity System Operator Workshop, both hosted at the Cyber Centre.

Cyber Centre's Partnerships team has developed an analysts' exchange strategy, similar to the UK's Industry 100, and is poised to run the first pilot with a partner in the Finance sector.

The Canadian Security Intelligence Service (CSIS) engages in various collaborative efforts across the cyber community in order to fulfill its mandate of investigating and reducing threats to Canada's national security. The Service conducts victim notifications in instances where there has been cyber incidents related to national security, post-victim discussions with entities who were targeted in cyber attacks or interference, and collaborates through information sharing efforts with both allied countries and Canadian federal departments.

Recommendation 2: ***That the Government of Canada invest in its own network infrastructure cybersecurity and undertake a comprehensive assessment of additional requirements necessary to harden government systems and third-party network infrastructure on which its data is stored, with the goal of ensuring that its sensitive data is protected and secure.***

The Government of Canada supports this recommendation.

The Government works continuously to enhance cyber security in its services by preventing attacks through implementation of protective security measures, identifying cyber threats and vulnerabilities, and by preparing for and responding to cyber incidents to better protect Canada and Canadians.

As the cyber threat landscape evolves, the government assesses its cyber security posture and determines the necessary investments to keep pace.

The Standard on Enterprise Information Technology Service Common Configurations, established under the Policy on Service and Digital and the Directive on Service and Digital, provides direction to departments on the management of IT components essential to IT services. This includes minimum cyber security configuration requirements that departments are expected to implement.

In addition, the GC has an established Supply Chain Integrity process which ensures that no untrusted equipment, software or services are procured by Shared Services Canada (SSC) and are used in the delivery and support of Government of Canada services.

Finally, as per the Policy on Government Security, departments and agencies are expected to ensure that security requirements associated with contracts and other arrangements, which include the use of third-party services that host GC data, are identified and documented, and related security controls are implemented and monitored throughout all stages of the contracting or arrangement process to provide reasonable assurance that information, individuals, assets and services associated with the contract or arrangement are adequately protected.

The CSE’s Cyber Centre has developed and deployed cyber security services that have been instrumental in defending federal institutions’ networks for more than a decade. The suite of services includes a network detection and response solution (NDR), end points detection and response solution and cloud detection and response solution, integrated with an analytical platform. Approximately 95 departments and agencies are protected by the NDR service deployed at SSC internet and cloud gateways. The Cyber Centre has also completed 90 deployments of its cloud detection and response service.

The Cyber Centre is continuing the deployment of its security services to additional federal institutions. As an example, as part of the Small Department and Agency 43 initiative (an initiative led by SSC and CSE to onboard 43 small departments and agencies to enterprise security services), small departments and agencies will be transitioned to the Government of Canada enterprise internet gateways and at the same time benefit from the Cyber Centre NDR solution.

Recommendation 3: ***That the Government of Canada work with our Five Eyes partners to adopt a Cybersecurity Maturity Model Certification (CMMC) that would be consistent and recognized by our partners to ensure that Canadian defence companies are not disadvantaged by having different security standards in Canada compared to our Five Eyes partners.***

The Government of Canada supports this recommendation.

To shore up the protection of unclassified information held by Canada's defence suppliers, the Government of Canada is establishing the Canadian Program for Cyber Security Certification (CP-CSC), which will introduce mandatory cyber security certification requirements in select defence contracts.

Increasing the cyber security resilience of the Government of Canada's defence industrial base will reinforce the goals of Canada's National Cyber Security Action Plan and National Cyber Security Strategy.

The new program will closely mirror the U.S. Cyber Security Maturity Model Certification (CMMC) program, to ensure that defence contractors which do business in both Canada and the U.S., will only need to be certified under a single regime.

Furthermore, in the longer term, the Government of Canada will explore alignment with other Five Eyes partners and close partners, so that Canadian firms improve access to international procurement opportunities where cyber security certification is required.

Recommendation 4: ***That the Government of Canada take steps to incentivize companies, which could include tax credits, to adopt cybersecurity measures, such as the "CyberSecure" standard established by ISED and CSE for small and medium organizations*****.**

The Government takes note of this recommendation.

Industry, Science and Economic Development Canada (ISED) helps small and medium-sized enterprises (SMEs) adopt cybersecurity measures through the Cybersecure Canada program, which provides SMEs with a low-cost way to demonstrate compliance with baseline cybersecurity controls, raising the confidence levels of their customers and partners.

The program aims to:

- raise the cybersecurity baseline among SMEs in Canada;
- increase consumer confidence in the digital economy;
- promote international standardization; and
- better position SMEs to compete globally.

With respect to tax measures, SMEs 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 percent 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 5: ***That the Government of Canada expedite the renewal of Canada's national cybersecurity strategy and establish an ongoing review that can better keep pace with the changing nature of cyber threats.***

The Government of Canada takes note of this recommendation.

In his 2021 mandate letter, the Prime Minister instructed the Minister of Public Safety to work with the Ministers of National Defence; Foreign Affairs; Innovation, Science and Industry; and others, to develop and implement a renewed National Cyber Security Strategy, which would articulate Canada's long-term strategy to protect our national security and economy deter cyber threat actors, and promote norms-based international behaviour in cyber space. Following the release of the mid-term evaluation in 2022, Public Safety, in collaboration with partners, is working to meet this commitment.

Recommendation 6: ***That the Government of Canada continue its ongoing dialogue with critical infrastructure owners/operators such as municipalities, Provincial, Territorial, Indigenous governments, and private sector operators such as utility companies; and, that this ongoing work be formalized to have consistent and ongoing dialogue to discuss potential threats as well as best practices.***

The Government of Canada supports this recommendation.

The Government continues to engage with the broader community of critical infrastructure owners and operators on potential threats and best practices under the auspices of the 2009 National Strategy for Critical Infrastructure and its associated action plans.

This dialogue occurs in multiple formats, including standing bodies of public and private stakeholders such as the National Cross Sector Forum and Sector Networks, direct meetings with public and private stakeholders, online targeted consultations and email submissions. The insights gained from these discussions are being used to inform the development of a forward-looking vision for critical infrastructure resilience.

Recommendation 7: ***That the Government of Canada examine the CSIS Act to ensure that CSIS has the legislative tools it needs to keep pace with technological advancements, modern digital realities, and the ever-evolving cybersecurity threats facing Canada.***

The Government of Canada supports this recommendation.

The rate and speed of technological advancements have created a complex operational and technological environment. State actors increasingly use digital technology to advance their strategic, political, economic and military objectives, often times to the detriment of Canada's national security. State and non-state cyber actors also continue to pose a threat to Canada's national security, critical infrastructure, and core institutions.

In the face of these developments, the Government is engaged in continuously evaluating the legislative framework for national security in Canada, including the Canadian Security Intelligence Service (CSIS) Act. In doing so, the Government seeks to ensure the framework provides CSIS, and other departments and agencies, with the tools they need to effectively investigate and counter cyber-based threats to the security of Canada.

Recommendation 8: ***That the Government of Canada work with provinces and industry to create requirements for private sector critical infrastructure operators to report ransomware and cybersecurity incidents to the Canadian Centre for Cyber Security within a designated time-period; create appropriate safeguards for victims of cyberattacks to mitigate or eliminate disincentives to reporting; and that the government incentivize owners and operators of critical infrastructure to cooperate with relevant authorities in identifying, reporting, and eliminating vulnerabilities.***

The Government of Canada supports this recommendation.

On June 14, 2022, the Minister of Public Safety introduced Bill C 26, An Act Respecting Cyber Security, in the House of Commons. Part 2 of the bill would enact the Critical Cyber Systems Protection Act (CCSPA), which would establish a regulatory framework to strengthen baseline cyber security for services and systems that are vital to national security and public safety. This proposed legislation is intended to increase cyber threat information sharing.

The CCSPA would require designated operators in four federally regulated critical infrastructure sectors – finance, telecommunications, energy, and transportation – to report cyber security incidents affecting their critical cyber systems to CSE. Mandatory incident reporting would provide CSE's Cyber Centre with a broad view of the threats and vectors in Canada, and allow the Cyber Centre to disseminate vital threat information back to all cyber infrastructure operators in Canada, including technical advice and suggested actions to contain the compromise, recover from the incident, and prevent further incidents. In this way, the CCSPA is intended to improve Canada's overall cyber security posture.

This legislation can serve as a model for provinces, territories, and municipalities to help secure critical infrastructure outside federal jurisdiction. In sectors that use the same standards across jurisdictions, there is an opportunity for the CCSPA to help build cyber security capacity and expertise to support more resilient systems across sectors, across the country.

Recognizing that many services and systems that are designated under the CCSPA are dependent on, or interconnected with, other cyber systems that fall outside federal jurisdiction, the Government of Canada will continue to engage with provinces and territories to discuss how to better protect Canada's cyber systems through a comprehensive, collaborative Canadian cyber security protection framework.

While Bill C-26 would introduce mandatory cyber security incident reporting, the Cyber Centre continues to encourage the voluntary reporting of cyber incidents. Critical infrastructure operations, businesses, IT professionals, and government institutions can report cyber security incidents directly to the Cyber Centre at cyber.gc.ca, by email (contact@cyber.gc.ca), or by telephone (1-833-CYBER-88). Information provided to the Cyber Centre, including personal information, is held securely, with strictly limited access. Reporting helps keep Canada and Canadians safe online by enabling the Cyber Centre to provide cyber security advice, guidance, and services.

CSE's Cyber Centre continues to work with industry partners, including government and non-government partners, to share information to ensure that they have access to the cyber security experts and resources they need to defend against and recover from malicious cyber activity, and that cyber security standards are met and reported on. On its bi-weekly Threat Brief Calls, the Cyber Centre also discusses the value of reporting directly with stakeholders, highlights the reporting statistics by sector, and encourage all partners to report incidents, big or small, regardless of whether they need Cyber Centre support

The Government of Canada continues to examine the issue of cyber incident reporting to understand barriers and disincentives to reporting. For example, Public Safety's Canadian Survey of Cyber Security and Cybercrime surveys businesses to understand the impact of cybercrime on the Canadian public service and crown corporations, including aspects such as investment in cyber security measures, cyber security training, the volume of cyber security incidents, and the costs associated with responding to these incidents. The current iteration of the survey includes questions related to cyber incident reporting to the Government of Canada to better understand motivations and incentives to reporting.

Recommendation 9: ***That the Government of Canada work with industry partners to improve cyber-security at the development stage of hardware and software, in order to help shift the cyber-security burden away from individual users.***

The Government of Canada supports the recommendation.

Canada trades extensively in hardware and software products. Industry partners, both domestic and foreign will need to be part of solutions. The Government of Canada is working with allied countries to improve cybersecurity of hardware and software products in order to shift the burden of securing networks away from individual users of these products to hardware manufacturers and software developers of cyber security products.

In this regard, the Cyber Centre has joined the U.S. Cybersecurity and Infrastructure Security Agency (CISA), FBI and other likeminded international partners to jointly publish guidance Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security-By-Design and Default urging manufacturers to take urgent steps necessary to ship software and hardware products that shift the burden of cyber security risk away from consumers – whether they are individuals or organizations, and instead encourage technology manufacturers to design safe products that are secure by design and by default.

The 'first-of-its-kind' hopes to encourage investment and the cultural shift needed to enhance cybersecurity in future. A future where security will be built-in from the ground up, all the way from the design stage to product development, not as an afterthought (secure by design), and products are safe to use out of the box with little to no configuration changes necessary and are available without additional cost (secure by default). Secure-by-Design products make the security of customers a core business requirement, not just a technical feature. This will ensure that Canadians are not responsible for preventing cyber breaches caused by product design flaws.

The guidance further encourages manufacturers to build their products in a way that prevents customers from having to constantly perform monitoring, routine updates, and damage control on their systems to mitigate cyber intrusions.

The guidance also outlines three core principles to guide this work including: 1) Taking ownership for security outcomes; 2) Embracing transparency and accountability; and 3) Building an appropriate organizational structure to allow software manufacturers to make executive level commitments to prioritize security as a key component of product development.

In addition to this work, the Government of Canada also continues to monitor Internet-of-things (IoT) device labelling and cybersecurity guidelines that are currently under consideration in other partner jurisdictions, including the US (US Cyber Trust Mark) and EU (EU Cyber Resilience Act) and their implications for Canadian producers and consumers.

Recommendation 10: ***That the Government of Canada take steps to retain Canadian-developed information technology intellectual property in Canada, including commercialization measures that maintain Canadian ownership of cyber-technologies.***

The Government of Canada agrees with the recommendation.

Positioning Canadian innovators to successfully protect and leverage information technology intellectual property (IP) is increasingly important as reliance on digital devices and networks in businesses' and individuals' activities continues to grow. As such, the Government supports innovators in developing their IP savviness, by protecting their IP, and making strategic IP decisions specific to their business needs. For instance, the National Intellectual Property Strategy (IP Strategy) was launched in 2018 to assist Canadian businesses, creators, entrepreneurs, and innovators in understanding, protecting, and accessing IP through its three pillars: IP education and advice, strategic IP tools for growth, and IP legislation. These initiatives are complemented by subsequent programs such as ElevateIP and IP Assist, which provide support for strategic IP decision-making. Additionally, CanExport SMEs assists small- to medium-sized enterprises develop export opportunities for products and services, including by funding the application process for IP protections in international markets.

The Government has also invested in commercialization opportunities, notably in the formation of the Cyber Security Innovation Network (CSIN). The CSIN, led by the National Cybersecurity Consortium will help foster a strong national cyber security ecosystem by increasing collaboration between academia and the private sector. The network will support research and development in cyber security, accelerate the commercialization of cyber security products, services, and processes, and support the development of skilled cyber security talent across Canada. In order to take appropriate steps to protect IP resulting from the network's activities, the National Cybersecurity Consortium will implement an IP strategy to define clear policies on the creation, use, protection, ownership, commercialization, and enforcement of, and access to, any IP associated with network activities to maximize economic and innovation benefits to Canada. The core objectives of the IP strategy include:

- the creation of IP as part of the growing research and development in Canada's cybersecurity ecosystem;
- the ownership of IP to empower cybersecurity innovators in commercializing their knowledge and products;

- the sharing of IP knowledge among the network to support in the management of IP and when appropriate, sharing IP within the National Cybersecurity Consortium membership; and
- the protection of IP by promoting the use of legal tools and services that uphold IP rights in a fair and secure manner.

Additionally, the National Cybersecurity Consortium will implement an organizational cyber security plan to ensure cyber resilience and protect the networks data and IP from potential cyber security incidents.

Recommendation 11: ***That the Government of Canada, in collaboration with civil society, industry and allies, further develop resources to deal with foreign cognitive warfare activities—such as misinformation, disinformation and malinformation—to better protect Canadians and ensure the public can access accurate information.***

The Government of Canada supports this recommendation.

The Government of Canada is already implicated in developing resources in collaboration with civil society and industry through the Digital Citizen Initiative. Approximately 100 projects have been funded since the program's inception in 2019, supporting digital media literacy campaigns and research from a Canadian perspective. The projects funded by the Digital Citizen Initiative aim to build resilience in Canadians by building critical thinking and digital media literacy skills, which ensure the public can access accurate information.

In recognition that misinformation and disinformation, among other vectors of foreign interference, threatens democracy and undermines national security, G7 leaders committed to standing up the G7 Rapid Response Mechanism (G7 RRM) during the Charlevoix Summit in 2018. Led by Canada on an ongoing basis, the G7 RRM is mandated to identify and respond to foreign threats to democracy. Since its inception, the G7 RRM has focused its attention on tackling Foreign Information Manipulation and Interference – a set of malign online activities that include disinformation. Besides coordinating the G7 RRM, GAC also monitors the digital information environment for signs of foreign interference on key government of Canada priorities, including during elections, as part of Security and Intelligence Threats to Elections (SITE) Task Force. This includes a stand-alone team focused on countering Russian disinformation, announced by the Prime Minister last summer (2022).

The CSE and its Cyber Centre have 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. CSE continues to provide the Government of Canada with the most comprehensive information available related to Canada's intelligence priorities, directly furthering Canadian safety, security, and prosperity.

States employ foreign interference activities against a range of Canadian interests, and leverage sophisticated cyber tools and online platforms to spread misinformation/disinformation. CSIS advises the Government of Canada on the threat from foreign interference and engages in extensive outreach and awareness efforts to keep Canadians informed. CSIS has reported on foreign interference in all its annual public reports for the last 30 years, and has published unclassified reports, including 'Foreign Interference and You'. These reports and other publicly available resources on foreign interference are published in a range of foreign languages in order to ensure that vulnerable communities can access threat information in their language of choice. CSIS is also an active member of SITE, working with federal partners to combat foreign interference targeting our elections. CSIS also partners with allies to develop joint products to advise the Government on threats national security, including cyber security, and to determine attribution, motivations and capabilities of threat actors. Moving forward, increased engagement with civil society, industry, and allies is essential for CSIS to collect actionable intelligence and combat evolving security threats, which impact communities, and Canadians, and inform CSIS' advice to the Government of Canada.

Recommendation 12: ***That the Government of Canada ensure federal departments and contracts are audited to confirm the information security standards are being met by government and contractors.***

The Government of Canada takes note of this recommendation.

The existing suite of policies related to information security for departments and agencies, as well as those related to contracting and other arrangements, provide comprehensive direction on managing information security. Those policies establish clear accountabilities for implementing the direction as well as verifying compliance.

For example, as per the Treasury Board Policy on Government Security (PGS), clear responsibilities are established for line departments, Lead Security Agencies, and Internal Enterprise Service Organizations. Departmental Chief Security Officers are uniquely positioned under the PGS to conduct and report independently to their Deputy Heads on all security activities, including compliance with policy and direction. Also, departmental security is one of the areas of management evaluated through the Management Accountability Framework.

In addition to the performance audits conducted by the Office of the Auditor General of Canada, which reports to Parliament, internal audit functions exist in all large departments. These functions are independent from line management and have a mandate to assess areas of risk, control, and governance, including risks associated with IT security, based on their assessment of risks and priorities. Similarly, the Office of the Comptroller General's audit operations division conducts periodic horizontal audit engagements on a range of risk areas over time. Several horizontal engagement relating to information technology security have been completed in recent years.

Security risks will continue to be considered together with other risk and government priorities as part of multi-year risk-based internal auditing planning, and as part of annual updates to departmental security plans.

Recommendation 13: ***That the Government of Canada work with provinces to establish minimum standards for cyber security for small and medium organizations and incentivize companies to adopt the latest security measures to protect from both high-risk low probability and low-risk frequent attacks.***

The Government of Canada takes note of 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. The Government of Canada continues to work to further strengthen coordination and collaboration among federal, provincial, and territorial systems, including for cyber security matters. Through regular engagement at both the Ministerial and officials' levels, federal, provincial, and territorial counterparts share observations of the current cyber threat landscape and consider policy approaches that would enhance the cyber security of Canadians and Canadian businesses.

To ensure that small and medium-sized organizations have access to resources to help bolster their cyber security and overall resiliency, the CSE and its Cyber Centre have helped develop and deliver tailored advice and guidance, as well as learning programs (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.

Additionally, CSE's Cyber Centre regularly develops, and updates advice and guidance tailored to small and medium-sized organizations. This includes the baseline cyber security controls for small and medium organizations, top measures to enhance cyber security for small and medium-sized organizations, the Ransomware Playbook (a publication that introduces ransomware, threat actor motivations and gains, and measures to prevent cyber attacks), 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 14: ***That the Government of Canada expand its collaboration with Canadian security and defence industries to bolster Canada's offensive and defensive cyber infrastructure amidst the growing assertiveness of malign foreign states.***

The Government of Canada supports this recommendation.

Under the Communications Security Establishment Act, CSE may conduct defensive or active foreign cyber operations to help protect Canada and Canadians. Defensive cyber operations defend Canada against foreign cyber threats by taking action online. This authority can also be used to defend systems designated by the Minister of National Defence as being of importance to the Government of Canada such as: energy grids, telecommunications networks, healthcare databases, banking systems, and elections infrastructure. Active cyber operations allow CSE to take action online to disrupt the capabilities of foreign threats to Canada such as foreign terrorist groups, foreign cyber criminals, hostile intelligence agencies, and state-sponsored hackers. The threats CSE disrupts must relate to international affairs, defence, or security.

CSE and its Cyber Centre also work to counter the malicious cyber activities of hostile state actors by sharing cyber threat information and mitigation advice with the operators of these critical networks and deploying, upon request, its cyber security tools to help defend their networks.

Earlier this year, the CSE's Cyber Centre began reaching out to, and engaging with, the Defence Industrial Base (DIB). They have been onboarding partners in this sector to Cyber Centre services and will be involved in workshops on cyber security with some of the smaller to medium sized DIB entities. The Cyber Centre participated at CANSEC (A Canadian Association of Defence and Securities Industries-run Conference) for the first time this year and are also working with other Government of Canada departments on the development and implementation of the Cyber Security Maturity Model Certification for Canadian DIB organizations.

Furthermore, the Canadian Security Intelligence Service (CSIS) Act permits CSIS to conduct active and defensive cyber operations. CSIS utilizes a suite of threat reduction measures, outlined in the CSIS Act, to combat cyber incidents threatening the national security of Canada, both domestically and outside of Canada. In doing so, the Service collaborates with various government departments to bolster Canada's cyber security, and jointly works to counter foreign interference across cyber space.

Recommendation 15: ***That the Government of Canada undertake a comprehensive cyber security analysis to identify existent cyber vulnerabilities in Canada, including but not limited to critical infrastructure, and prioritize eliminating current vulnerabilities and intrusions by hostile actors.***

The Government of Canada supports this recommendation.

The Government of Canada continuously undertakes this type of activity in an effort to better protect Canadians, their data, and the critical services upon which they rely.

Public Safety Canada delivers a suite of targeted awareness-raising, exercise and assessment programs to help specific critical infrastructure owners and operators identify and address vulnerabilities. The majority of participants have reported that these programs have increased their levels of awareness of the diverse and evolving risks to critical infrastructure, along with stronger incident response to threats targeting their organizations.

CSE and its Cyber Centre continue to work towards improving authentication solutions, collaborating with lead government of Canada security agencies and industry to identify Multifactor Authentication (MFA) solutions for internal and external services. CSE and the Cyber Centre will also be publishing Cyber Security Guidance pertaining to Secure Management of Digital Identities. This was developed in partnership with industry (Microsoft) and was based on recent vulnerabilities observed. It focuses on the administration of directory services and how to effectively manage secure environments through improved authentication solutions and dedicated workstations.

To address zero-day vulnerabilities, CSE and its Cyber Centre deliver reminders on the importance of patch management, as well as continue to work with Cloud Service Providers (CSPs) to improve security services and cyber resiliency.

To address ongoing vulnerabilities that can be mitigated from proper ‘housekeeping’, CSE and the Cyber Centre routinely issue guidance publications on Cyber Security Best Practices covering several topics including password management, patching, and the importance of monitoring and logging security events. In addition, the proposed Bill C-26, An Act Respecting Cyber Security, would help designated critical infrastructure operators in the transportation, energy, financial, and telecommunications sectors to address ongoing vulnerabilities and lower their cyber risk.

To help government and critical infrastructure sectors understand their environment and develop more robust cyber solutions, CSE and its Cyber Centre have developed a Threat and Risk Analysis tool, called ASTRA, to help with the development of secure environments. CSE and its Cyber Centre also offer a course on how to use the tool through their Learning Hub.

Recommendation 16: ***That the Government of Canada include space-based platforms as critical infrastructure and, ensure they are protected and secure.***

The Government of Canada agrees to further examine this recommendation.

Since the Fall of 2021, the Government has engaged with the broader critical infrastructure community as part of the National Strategy for Critical Infrastructure renewal. Stakeholders indicated support for the option of adding a Space sector due to the essential role that space-based platforms play in underpinning all other forms of critical infrastructure and environmental monitoring. As the Strategy renewal progresses, the Government will continue to explore the identification of space-based platforms as critical infrastructure.

Recommendation 17: ***That the Government of Canada clearly define the roles and responsibilities of each government department currently responsible for monitoring, responding, and employing cyber capabilities in Canada.***

The Government of Canada supports this recommendation.

Cyber security is a shared responsibility in the Government of Canada, with roles and responsibilities defined in departmental mandates and Treasury Board policy instruments such as the Policy on Government Security and the Policy on Service and Digital.

Recommendation 18: ***That the Government of Canada reviews all cyber-related infrastructure, used for the operational functions of the Department of National Defence and the Canadian Armed Forces, to ensure it is free from sensitive technology designed, assembled and operated, either directly or indirectly, by malign foreign states, which could pose a cybersecurity risk or otherwise compromise protected information.***

The Government of Canada supports this recommendation.

The Government of Canada is actively engaged in ensuring that untrusted equipment, software, or services are not used in the delivery and support of Government services.

The DND/CAF Security Program and Cyber Mission Assurance Program ensure that risks to military infrastructure, including information technology, platform technology and operational technology are identified and mitigated before procurement and operational use.

In addition, the Communication Security Establishment's Supply Chain Integrity Program works with Shared Services Canada to evaluate risks related to Information Communications Technology equipment being procured for Government of Canada systems and networks. This program is evolving to meet the increasing demand and complexity of cyber supply chain risks, including working with a broader range of government and industry partners.

Recommendation 19: ***That the Government of Canada mandate all federal government departments and request provincial, territorial, municipal, and Indigenous governments to provide a detailed list of critical infrastructure to Treasury Board and the Communications Security Establishment and update it annually.***

The Government of Canada agrees to further examine this recommendation.

The Government recognizes the multi-jurisdictional nature of how critical infrastructure is owned, regulated, and protected. As such, we will continue to connect with the appropriate
stakeholders to address issues as they pertain to national security, including on issues related to critical infrastructure lists.

Recommendation 20: ***That the Government of Canada increase funding to the Canadian Centre for Cyber Security to improve coordination between federal and provincial cybersecurity systems to better address incidents.***

The Government of Canada supports this recommendation.

The CSE and its Cyber Centre continues to work to further strengthen coordination between federal and provincial systems when it comes to addressing incidents, including the possibility of establishing a dedicated line for incident reporting and direct support to provinces and territories.

Recommendation 21: ***That the Parliament of Canada create a special joint committee on cybersecurity, information warfare and artificial intelligence.***

The Government of Canada takes note of this recommendation.

Special joint committees are established by orders of reference from both Houses to deal with matters of great public importance. Special committees are independent from the Government, and the decision to create them falls under the purview of Parliament.

Recommendation 22: ***That the Government of Canada immediately undertake a comprehensive review and expeditious reform of the procurement process for military equipment, including cyberwarfare equipment—this would include Treasury Board guidelines on competition and sole sourcing—with the intent to bring project times down from years to months or weeks.***

The Government of Canada agrees in principle with this recommendation.

Streamlined and flexible procurement is necessary for the successful and timely delivery of the modern capabilities required to ensure the Canadian Armed Forces (CAF) are ready and equipped to conduct operations. Defence procurement is a whole-of-government effort, and project management of complex defence procurement projects, such as fighter aircraft and NORAD modernization, requires skills that are built over many years.

DND/CAF works collaboratively with key partners at PSPC, Innovation, Science and Economic Development Canada, Defence Construction Canada, Shared Services Canada and the Treasury Board of Canada Secretariat to improve the speed at which they deliver capabilities and to consider more innovative approaches to procurement. Procurement processes aim to meet current and future operational requirements while ensuring that Canada realizes industrial, technological and societal benefits from these substantial investments and preserves the principles of openness, transparency and fairness.

There are existing mechanisms and procedures that enable the government to rapidly respond to urgent operational requirements. For example, the PSPC-led Risk-based Approach to Contract Approval for low-risk defence projects has sped-up the approval process, improving timeliness for the delivery of projects and capabilities. Moreover, DND/CAF works collaboratively with industry partners to ensure alignment, find realistic solutions and deliver on schedule.

Recommendation 23: ***That the Government of Canada adapt and develop a comprehensive plan for the recruitment and retention of cyber operators which is competitive with the private sector to ensure positions are filled and the cyber skills gap is closed in the Canadian Armed Forces and the Communications Security Establishment.***

The Government of Canada supports this recommendation.

The Canadian Armed Forces (CAF) recognize the importance of recruiting and retaining qualified cyber operators. Strong, Secure, Engaged (SSE) directed the CAF to establish a Cyber Operator occupation to conduct defensive and offensive cyber operations in support of military missions. The first class of Cyber Operators graduated from the Canadian Forces School of Communications and Electronics in September 2021.

The CAF has a number of recruitment initiatives in place to recruit new members. The CAF website highlights the Cyber Operator trade as a potential career choice, and provides an overview of the occupation, roles and responsibilities, required training, entry plans, direct entry options, and information on CAF pay and benefits.

DND/CAF's Cyber operators' salaries take into account their specialized skillset in comparison to other CAF members.

Recommendation 24: ***That the Government of Canada develop and deploy "persistent engagement" capacity in collaboration with the Canadian Armed Forces.***

The Government of Canada supports this recommendation.

Strong, Secure, Engaged directed the Canadian Armed Forces to assume a more assertive posture in cyberspace to harden defences, and to conduct offensive cyber operations in support of government-authorized military missions. The CAF recognize the importance of both offensive and defensive capabilities to secure its own networks and systems and project power in cyberspace.

The CAF have been working to defend and protect its internal networks and systems by proactively responding and adapting to new and evolving cyber threats. In addition, the CAF recognizes the importance of collective defence and has been working closely with allies and partners to deter, defend against, and respond to the full range of malicious cyber activities. For example, the CAF has stood up a Cyber Task Force (CTF) team to help Ukraine bolster its cyber defence capabilities. This CTF provides Ukraine with cyber security expertise, cyber threat intelligence, and software tools and technical solutions to better defend their networks against malicious cyber activity. The CAF has also deployed a persistent Canadian Task Force to Latvia to conduct joint defensive cyber operations on Latvian critical infrastructure.

Recommendation 25: ***That the government of Canada implement a system for allowing veterans to maintain security clearances equivalent to the clearances they had with the Canadian Armed Forces when transferring out of service thus enabling a seamless continuity in clearance in order to facilitate their employment in the Department of National Defence. The government should also examine a system of fast-tracking security clearance for veterans seeking employment in other federal departments.***

The Government of Canada supports this recommendation.

The Standard on Security Screening (SSS) makes a distinction between a security status and a security clearance. A security status, also referred to as a reliability status, is the minimum standard of security screening for positions requiring unsupervised access to Government of Canada assets, facilities or information technology systems. A security clearance grants access to classified information, assets, facilities or information technology systems (secret or higher). For the purpose of this recommendation, the Government of Canada understands the term "security clearance" as encompassing both security status and security clearance.

The transfer of security clearances from the CAF to the DND is routinely done. DND/CAF is continually monitoring the process to find ways to reduce wait times and expedite transfers.

Clearances can also be transferred for CAF members joining other government departments. The timeline for transferring clearance information from DND to another federal department can vary, but on average does not take more than 2 weeks from when the request to transfer the clearance is received. The timeline is dependent on the volume of transfer requests received by DND at any one time.

As such, valid security clearances for currently serving CAF members can be transferred to any government departments when they transfer to a civilian position in the federal public service. However, when a member leaves the CAF, they have to return to a position in the federal public service before their clearance expires (within 12 months for secret or higher clearances and within 2 years for reliability statuses).

While departments follow the Treasury Board Policy on Government Security, including its SSS, each department is responsible for the conduct of its own security screening once DND transfers the file.

Any person who is medically released from the Canadian Armed Forces for reasons attributable to service has a statutory priority entitlement. They are first in the order of precedence established by the Public Service Employment Act, as long as they meet the essential qualifications of the position. This priority entitlement begins when the veteran is medically certified as ready to return to work, and lasts for 5 years.

The Government of Canada will continue to explore avenues to facilitate veteran's transition to the public service.

Recommendation 26: ***That the Government of Canada take steps to clearly define the duties and responsibilities of the Canadian Armed Forces and the Communications Security Establishment as they relate to cyber security in Canada and abroad.***

The Government of Canada supports this recommendation.

The duties and responsibilities of the CAF and the CSE are clearly defined. The CSE is the lead federal technical authority for cyber security, while the CAF are mandated to defend and protect internal DND/CAF networks, as well as conduct cyber operations in support of government-authorized military missions.

As part of its responsibilities, the CSE provides critical foreign intelligence to help inform the Government of Canada's decision making and protect national security. CSE's sophisticated cyber and technical expertise also helps detect, monitor, and investigate potential threats against Canada's systems and networks, and helps take active measures to address them.

The CAF and the CSE have a longstanding partnership in developing highly technical and specialized capabilities to support CAF operations, which continues to evolve as cyber threats and capabilities develop. For example, the CSE works in close collaboration with the CAF to integrate, prioritize and deconflict military signals intelligence operations in support of defence intelligence requirements. This partnership ensures that the CAF has improved domain awareness and force protection as it conducts its operations globally.

This relationship helps achieve mission objectives by ensuring that the right tools and capabilities are used, while reducing unnecessary duplication of efforts. At present, the CAF has several members embedded within a joint team at the CSE to conduct foreign cyber operations. The CAF is also able to request technical and operational assistance from the CSE for CAF cyber operations through section 20 of the CSE Act. The CSE and the CAF partner operationally and strategically at every level to align our strategic outcomes and maximize Canada's strategic advantage in international affairs, defence, security, and cyber security.

Recommendation 27: ***That the Government of Canada take immediate steps to address logistical support issues in the Canadian Armed Forces, including the Cyber Forces***

The Government of Canada agrees with this recommendation in principle.

A critical component of guaranteeing that the Canadian Armed Forces have the logistical support they require to carry out their mandate is ensuring Information Management/Information Technology (IM/IT) equipment is secure from malfunctions and cyber attacks.

DND/CAF works with Government of Canada partners to ensure IM/IT equipment is secure, resilient, and recoverable from malfunctions and cyber attacks in a timely manner so as not to impact the operations of the department or the CAF, including the Cyber Forces.

Likewise, the DND/CAF security Program and Cyber Mission Assurance Program ensure that risk to military infrastructure, including network assets such as software and hardware, are identified and mitigate before their operational use.

Recommendation 28: ***That the Government of Canada ensure the future viability of the CAF Cyber Forces by creating a retention program for its Cyber Operators and supplying them with the necessary cyber infrastructure.***

The Government of Canada supports this recommendation.

Retention is a challenge that affects several occupations within the CAF and is being addressed under the Canadian Armed Forces Retention Strategy which aims to keep our talented people in uniform with a welcoming and healthy work environment. The provision of appropriate training and supporting infrastructure is a recognised challenge for which options are currently being examined.

As noted in Strong, Secure, Engaged, to support the women and men of the Canadian Armed Forces, CAF will substantially improve recruitment, retention, and training of personnel. We will better forecast occupational requirements and engage in more targeted recruiting, including capitalizing on the unique talents and skill-sets of Canada’s diverse population.

The rapidly changing global and technological landscape is presenting CAF and DND with multiple challenges and complexities regarding developing, generating, employing, sustaining and managing military capabilities efficiently and effectively while also pursuing digital transformation. Since the publication of SSE in 2017, DND/CAF continues to work on key cyber initiatives. These include the development of active cyber capabilities so that they can be employed against potential adversaries in support of government-authorized military missions, the creation of the new CAF Cyber Operator occupation to attract Canada's best and brightest cyber talent, and the use of Reservists with specialized skill-sets to fill elements of the CAF cyber force.

Recommendation 29: ***That the Government of Canada continuously update the legal framework for dealing with cyberattacks, which includes guidelines for attribution, response and liability.***

The Government of Canada supports this recommendation.

There is a policy framework for attribution, which also informs response decisions. GAC is currently consulting with several departments to review and update the attribution framework. The Government of Canada must remain attentive to the evolution of international law and the multilateral framework for responsible state behaviour in cyberspace.

Recommendation 30: ***That the Government of Canada work with our allies to update international laws, such as the Rome Statute and the Geneva Convention, to include state-sponsored cyberwarfare as a war crime.***

The Government of Canada takes note of this recommendation.

The Government of Canada supports the rules-based international order, and affirms that existing international law applies to the activities of every State in cyberspace.

The Government of Canada will continue to encourage States to publish national views on how international law applies in cyberspace.

Recommendation 31: ***That the Government of Canada immediately adopt all outstanding recommendations of the Auditor General's Report 7—Cybersecurity of Personal Information in the Cloud, tabled to Parliament on November 15, 2022.***

The Government of Canada supports this recommendation.

TBS is working collaboratively with SSC, PSPC, and CSE to implement the recommendations in the Auditor General's Report 7—Cybersecurity of Personal Information in the Cloud as per the government's response outlined in the "Recommendations and Responses" section of the report.

Recommendation 32: That the Government of Canada use existing sanctions regimes to target individuals and entities targeting Canadians with misinformation, disinformation and/or malinformation.

The Government of Canada agrees to further examine this recommendation.

Canada is judicious in its approach to imposing sanctions, and is committed to their effective and coordinated use when appropriate. To that end, Canada has established a rigorous due diligence process to consider and evaluate possible cases of gross human rights violations, corruption or other circumstances that may warrant the use of sanctions. Recognizing that every situation is unique, the broader domestic and international contexts are also important considerations when evaluating whether sanctions or any other tools in Canada's foreign policy toolbox may be an appropriate response mechanism.

Canada's autonomous sanctions legislation outlines the legal thresholds that must be met in order to impose sanctions. In addition, the availability of credible, open source information is also an important factor when considering the use of sanctions, as rationales to impose Canadian autonomous sanctions against specific targets must be substantiated with open sources available in the public domain.

Canada has previously imposed sanctions against individuals and entities involved in misinformation, disinformation and/or malinformation, most prominently as part of the broader sanctions response effort to the Russian invasion of Ukraine.

The G7 Rapid Response Mechanism (G7 RRM) led by Canada on an ongoing basis, forms an important part of the Plan to Protect Canada's Democracy (Plan). In recognition that misinformation and disinformation, among other vectors of foreign interference, threatens democracy and undermines national security, G7 leaders committed to standing up the G7 Rapid Response Mechanism (G7 RRM) during the Charlevoix Summit in 2018. Led by Canada on an ongoing basis, the G7 RRM is mandated to identify and respond to foreign threats to democracy. Since its inception, the G7 RRM has focused its attention on tackling Foreign Information Manipulation and Interference – a set of malign online activities that include disinformation. Besides coordinating the G7 RRM, GAC also monitors the digital information environment for signs of foreign interference on key government of Canada priorities, including during elections, as part of Security and Intelligence Threats to Elections (SITE) Task Force. This includes a stand-alone team focused on countering Russian disinformation, announced by the Prime Minister last summer (2022).

We will continue to monitor possible instances of misinformation, disinformation and/or malinformation, and will continue to consider autonomous sanctions as a possible response mechanism, where appropriate.

Recommendation 33: ***That the Government of Canada impose effective sanctions on countries which condone or deploy cybercriminals for purposes such as theft of funds, theft of intellectual property, information warfare, and other malicious intents.***

The Government of Canada agrees to further examine this recommendation.

Canada is committed to prevent and counter cybercrime and is actively working with international partners to promote and protect Canadian interests that are increasingly targeted by this crime. Further to the response to Recommendation 32, and acknowledging the legal thresholds outlines in Canada's autonomous sanctions legislation, if actions conducted by cybercriminals are found to constitute gross human rights violations, acts of significant corruption, or grave breaches of international peace and security that have or are likely to result in a serious international crisis, sanctions could be considered as a possible response mechanism.

We will continue to monitor possible actions of countries which condone or deploy cybercriminals, and will examine whether such actions fit the criteria under which Canada can impose autonomous sanctions as a possible response mechanism, where appropriate.

Recommendation 34: ***That the Government of Canada open a review of existing cyber-defence policy and hold bilateral conversations with allies, such as the US, to ensure cohesive and consistent policies are being used.***

The Government of Canada supports this recommendation.

Canada's defence policy, Strong, Secure, Engaged, directed the Canadian Armed Forces (CAF) to assume a more assertive posture in cyberspace and develop and use offensive cyber capabilities in support of military missions.

The CAF habitually reviews its internal policies to ensure it has the necessary direction, resources, and future-ready capabilities to respond to the challenges of today and of the future. DND/CAF remains adaptive in the face of the changing international security environment and pivots its priorities accordingly.

Canada regularly engages in bilateral conversations with allies to ensure the consistent application of relevant policies. For example, in March 2023, Prime Minister Trudeau and President Biden released a joint statement recognising that cyber threats can impact both Canadians and Americans particularly when directed at cross-border systems upon which both nations rely. Canada and the US remain committed to better protecting against these threats and to deepening cooperation on driving improvements to the cybersecurity and resilience of critical infrastructure.

Recommendation 35: ***That the Government of Canada share Finland and Sweden's cognitive warfare education for civilians with the provinces.***

The Government of Canada supports this recommendation.

As stated by the Government in its April 6, 2023 report Countering an evolving threat: Update on recommendations to counter foreign interference in Canada's democratic institutions, the Government has and will work together with provincial, territorial, municipal and Indigenous officials. Over the past few years, the Royal Canadian Mounted Police, the Canadian Security Intelligence Service, the Canadian Centre for Cyber Security, and Public Safety Canada have engaged with provincial, territorial and municipal colleagues, as well as with critical infrastructure owners and operators to increase awareness of foreign interference threats and build resilience.

Sustained, regular, and coordinated engagement with partners is essential to detect threats, build resilience, and effectively counter foreign interference activities. The new National Counter Foreign Interference Coordinator will work on expanding briefing mechanisms with provincial, territorial, municipal and Indigenous officials. The Protecting Democracy Unit within the Privy Council Office, which coordinates, develops and implements Canadian government-wide measures designed to combat disinformation and protect our democratic institutions and processes, will expand its work with provinces and territories.

The Digital Citizen Initiative, established as part of the Plan to Protect Canada's Democracy (the Plan), is connected with other government agencies, researchers and civil society and aids in resource and information sharing amongst these stakeholders. Through the DCI, the Government in June 2023 announced a $5.5 million investment to create the Canadian Digital Media Research Network (CDMRN). The CDMRN will further strengthen Canadians' information resilience by researching how quality of information, including disinformation narratives, impact Canadians' attitudes and behaviours and by supporting strategies for Canadians' digital literacy. The CDMRN is independently administered by the Media Ecosystem Observatory at University of Toronto and McGill University. Research and reports by the CDMRN will be public and as such, available to all Canadians, including officials at provincial, territorial, municipal, and Indigenous governments.

The G7 Rapid Response Mechanism (G7 RRM) led by Canada on an ongoing basis, also forms an important part of the Plan. The G7 RRM is mandated to identify and respond to foreign threats to democracy. Since its inception, the G7 RRM has focused its attention on tackling Foreign Information Manipulation and Interference – a set of malign online activities that include disinformation. In 2021, the G7 Rapid Response Mechanism (RRM), welcomed Sweden as an observer with a view to leveraging expertise and avoiding duplication. The Government of Canada will also continue to liaise with the Swedish Psychological Defence Agency.

The Government of Canada will continue to work with Sweden and explore working with Finland to capitalize on their efforts in the cognitive warfare civilian education domain.

Recommendation 36: ***That the Government of Canada establish clear boundaries in the operations of the Communications Security Establishment between their signals intelligence and cybersecurity mandates, including ministerial authorization processes and reporting mechanisms.***

The government takes note of this recommendation.

Canada’s existing legal framework ensures that there is an appropriate and robust level of separation between the different aspects of Communications Security Establishment’s (CSE) mandate, while still allowing for some exchange of information within the CSE. Those exchanges are done strictly in accordance with the Communications Security Establishment Act (the CSE Act), the Privacy Act, and the Canadian Charter of Rights and Freedoms, and are critical to CSE’s ability to provide first-class and timely cyber security advice, guidance, and services that protect the privacy and security of Canadians. It is also important to note that under the CSE Act, CSE cannot direct its activities at Canadians anywhere or at anyone in Canada.

In 2016, the government, through Public Safety Canada, consulted with Canadians across the country, asking for their thoughts on the direction that cyber security management should take in Canada. This feedback was included in the planning for the 2018 National Cyber Security Strategy. As a key initiative of this Strategy, the operational cyber security functions from three departments were united to establish the Canadian Centre for Cyber Security (Cyber Centre), as a part of CSE. This decision recognized the value and importance of more focused federal management of cyber security, which benefits from the innovative environment, technical expertise, and strategic insight resident within CSE, leading to a greater capacity to identify, address, and share knowledge about systemic threats, risks and vulnerabilities. This model is also replicated in the cyber security frameworks of other Five Eyes partners.

Pursuant to subsection 15 of the CSE Act, CSE has one mandate with five aspects. Foreign intelligence and cybersecurity are two of those aspects, each of which is described separately in s.16 and s.17 of the CSE Act, respectively. As is required by the CSE Act, CSE maintains separate Ministerial Authorizations for the foreign intelligence and cybersecurity aspects of its mandate, each of which is subject to individual approval by the Intelligence Commissioner. The Intelligence Commissioner functions as an external, independent entity responsible for ensuring that Authorizations issued by the Minister are consistent with the specific aspect of the CSE's mandate under which they are being issued and are reasonable, proportionate, and necessary.

The activities under each Authorization are also subject to review by the National Security and Intelligence Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians (NSICOP).

In addition, within 90 days of the repeal or expiry of each Authorization, CSE must report on the activities conducted under the Authorization to the Minister, a copy of which is provided to both the Intelligence Commissioner and NSIRA. In line with the Authorizations themselves, reporting on foreign intelligence Authorizations and cybersecurity Authorizations are done separately.

Recommendation 37: ***That the Government of Canada appoint a cybersecurity ambassador.***

The Government of Canada agrees to further examine this recommendation.

The Government of Canada is actively exploring this option. A senior-level official would help to increase engagement globally and advance our international security priorities, in coordination with Canada's cyber diplomats. In an era of profound digital transformation, it may be warranted to consider a broader portfolio than solely cyber security.

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 bolster its defences against malicious cyber activity.

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 François-Philippe Champagne, P.C., M.P.
Minister of Innovation, Science and Industry

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