Written Submission for the Department of Finance Canada's Pre-Budget Consultation 2025

By: CIRA, the Canadian Internet Registration Authority

August 28th, 2025

Summary

CIRA recommends a national investment strategy to bring Canada's cybersecurity for public institutions up to modern standards and peer-country comparable, consistent with the treatment of other "critical infrastructure" under Bill C-8. By making these investments, Canada can achieve exponential returns, reducing the costs of cyber incidents, strengthening national resilience and advancing digital sovereignty in a way that supports long-term economic growth and public trust.

Recommendation 1

The federal government should recapitalize the Get Cyber Safe campaign with $22.5 million over five years to expand public awareness, community partnerships and promote trusted free Canadian cybersecurity services that strengthen national digital resilience.

Recommendation 2

The federal government should invest $250 million over five years, through existing programs like the Cyber Security Innovation Network (CSIN), to help Canada's universities adopt baseline cybersecurity controls recommended by the Canadian Centre for Cyber Security, in a manner that supports existing provincial initiatives.

Recommendation 3

The federal government should invest $600 million over five years, through existing programs like the Coordinated Accessible National (CAN) Health Network, to bolster healthcare cybersecurity by driving adoption of Canadian technologies and funding training, audits, and awareness to protect sensitive health data, in a manner that supports existing provincial initiatives.

Recommendation 4

The federal government should invest $420 million over five years in Canadian and sector-specific cybersecurity centres, like the Ontario Centre of Innovation (OCI) to

cira

319 McRae Avenue, Suite 700,
Ottawa, ON K1Z 0B9

319, avenue McRae, bureau 700
Ottawa, ON K1Z 0B9

cira.ca
cira.ca/fr

strengthen collaboration, data sharing and collective defense across Canada's public and private sectors.

About CIRA

The Canadian Internet Registration Authority (CIRA) manages the .CA top-level domain (TLD) on behalf of all Canadians and develops new, enterprise-level cyber security services such as CIRA DNS Firewall. The organization operates one of the fastest-growing country code top-level domains (ccTLD) in the world, a high-performance global domain name system (DNS) network and one of the world's most advanced back-end registry management solutions.

As a member-based, mission-driven not-for-profit, CIRA also has a goal to promote a trusted internet for Canadians. As part of this, the organization reinvests millions of dollars each year into projects like CIRA Canadian Shield, the CIRA Internet Performance Test and its annual $1.25M granting program, among others

Recommendation 1

The federal government should recapitalize the Get Cyber Safe campaign with $22.5 million over five years to expand public awareness, community partnerships and promote trusted free Canadian cybersecurity services that strengthen national digital resilience.

Cybersecurity threats targeting Canadians are growing in both frequency and sophistication, affecting households, small businesses, and public institutions alike. According to the Canadian Centre for Cyber Security (Cyber Centre), Canadians are a frequent target of phishing campaigns, malware, and other cyber-attacks. These attacks not only threaten the privacy and security of individuals but also undermine confidence in Canada's digital economy.

The Government of Canada's Get Cyber Safe campaign has been an effective platform for raising public awareness of online threats and promoting safe digital practices. Given

cira
319 McRae Avenue, Suite 700, Ottawa, ON K1Z 0B9
319, avenue McRae, bureau 700 Ottawa, ON K1Z 0B9
cira.ca
cira.ca/fr

the accelerating pace of cyber threats, the campaign can be recapitalized to expand its reach and sustain its effectiveness. CIRA submits that a dedicated annual investment of $22.5 million over five years ($4.5 million annually) would allow the government to broaden public awareness efforts, including education about trusted, Canadian-operated firewall and DNS protection services that are available free of charge to households.

This investment could be directed across four priority areas to maximize impact: national, traditional and digital advertising and outreach to broaden awareness; development of bilingual resources and practical tools that promote Canadian-operated protective technologies such as free firewall services; partnerships with schools, libraries, Indigenous organizations, and community groups to embed cyber awareness locally; and capacity-building through training for community leaders. By structuring the investment this way, the government can ensure the campaign reaches Canadians broadly, equips them with actionable tools and evolves to address emerging threats.

CIRA submits this initiative would support Canada's economic and security priorities by strengthening digital resilience, enhancing public trust, and reducing the cost created by cybercrime, while also advancing sovereignty in critical sectors using domestically operated infrastructure.

Recommendation 2

The federal government should invest $250 million over five years, through existing programs like the Cyber Security Innovation Network (CSIN), to help Canada's universities adopt baseline cybersecurity controls recommended by the Canadian Centre for Cyber Security, in a manner that supports existing provincial initiatives.

Canada's universities and colleges drive research, innovation, and workforce development. In 2024, approximately $18.5 billion was invested in higher education research and development, representing about 34% of all research and development conducted in Canada.

cira

319 McRae Avenue, Suite 700,
Ottawa, ON K1Z 0B9

319, avenue McRae, bureau 700
Ottawa, ON K1Z 0B9

cira.ca
cira.ca/fr

However, these institutions face growing pressure to safeguard sensitive research data, intellectual property, and the personal information of millions of students, staff, and faculty. Many higher education institutions face budget pressures that limit their ability to adopt baseline cybersecurity protections, leaving critical education and research infrastructure vulnerable.

The federal government has already taken important steps to strengthen Canada's cybersecurity ecosystem, notably through the CSIN, led by the National Cybersecurity Consortium, which supports research and development, commercialization, and training. Yet there is a significant opportunity to expand support for direct adoption of proven, Canadian cybersecurity tools and services by post-secondary institutions.

CIRA submits that a dedicated investment of $250 million over five years ($50 million annually) would help fill this gap by supporting the adoption of baseline cybersecurity controls recommended by the Cyber Centre, including firewalls, cybersecurity awareness training, and secure device configurations, amongst others. With more than 300 universities, colleges, and polytechnics across Canada, this investment would help ensure that institutions responsible for educating millions of Canadians and stewarding sensitive research data are equipped with these protections.

By building on existing federal programs like CSIN, this initiative can be delivered efficiently, complementing ongoing efforts to expand Canada's cybersecurity capacity while addressing an urgent gap in adoption at the institutional level.

cira
319 McRae Avenue, Suite 700,
Ottawa, ON K1Z 0B9
319, avenue McRae, bureau 700
Ottawa, ON K1Z 0B9
cira.ca
cira.ca/fr

Recommendation 3

The federal government should invest $600 million over five years, through existing programs like the Coordinated Accessible National (CAN) Health Network, to bolster healthcare cybersecurity by driving adoption of Canadian technologies and funding training, audits, and awareness to protect sensitive health data, in a manner that supports existing provincial initiatives.

Healthcare remains one of the most vulnerable sectors in Canada to cyber-attacks, with hospitals and clinics increasingly targeted by ransomware and data breaches. These incidents compromise sensitive patient information, disrupt service delivery, and highlight systemic risks within Canada's healthcare infrastructure. Cybersecurity adoption is no longer optional; it is essential to maintaining public trust and safeguarding critical services.

The federal government has already recognized the importance of modernizing healthcare through the CAN Health Network, which helps hospitals and providers adopt and scale innovative Canadian technologies. Building on this model, there is an opportunity to extend the mandate to cybersecurity, equipping organizations that manage sensitive patient data and critical operations with leading Canadian-built security tools. With more than 1,000 hospitals across Canada, CIRA submits that a targeted investment of $600 million over five years would help ensure that institutions at the heart of healthcare delivery can implement the Cyber Centre's baseline controls. This investment would include the deployment of secure DNS services, firewalls, cybersecurity awareness training, device protection and threat monitoring solutions measures amongst other controls that are essential to strengthening national resilience and protecting Canada's digital sovereignty.

By embedding cybersecurity adoption into CAN Health's existing model, the government can deliver a targeted and high-impact investment without creating new program infrastructure. This would improve healthcare resilience, safeguard sensitive health data,

cira
319 McRae Avenue, Suite 700,
Ottawa, ON K1Z 0B9
319, avenue McRae, bureau 700
Ottawa, ON K1Z 0B9
cira.ca
cira.ca/fr

and reinforce Canada's sovereignty in digital infrastructure, all while creating growth opportunities for Canadian cybersecurity firms.

Recommendation 4

The federal government should invest $420 million over five years in Canadian and sector-specific cybersecurity centres, like the Ontario Centre of Innovation (OCI) to strengthen collaboration, data sharing, and collective defense across Canada's public and private sectors.

Canada's cybersecurity landscape is increasingly fragmented, with organizations facing similar threats but often working in silos. Cybersecurity analysts are costly to train and security operations centres can be costly, putting advanced protection out of reach for many institutions, particularly in the public sector and smaller organizations. This limits Canada's ability to collectively defend against growing cyber threats.

Regional innovation hubs, such as the OCI, provide a proven model for building ecosystems of collaboration and resource-sharing. Expanding this approach to cybersecurity would create dedicated innovation centres across regions and sectors, enabling institutions to pool expertise, share threat data, and access shared services such as monitoring and incident response. This approach reduces duplication, ensures broader coverage, and builds resilience.

CIRA submits that the proposed $420 million (over five years) should prioritize Canadian companies and solutions. Too often, organizations default to procuring U.S.-based infrastructure, creating dependencies that weaken Canada's digital sovereignty.

By enabling secure collaboration and shared investment in capabilities that no single institution can easily sustain alone, centres of innovation would lower barriers to adoption, strengthen defenses across sectors, and ensure that Canada's digital security infrastructure is both resilient and distinctly Canadian.

cira
319 McRae Avenue, Suite 700, Ottawa, ON K1Z 0B9
319, avenue McRae, bureau 700 Ottawa, ON K1Z 0B9
cira.ca
cira.ca/fr

Conclusion

CIRA thanks the Department of Finance Canada for the opportunity to contribute to its consideration of recommendations for Pre-Budget Consultation 2025.

Additional information or citations are available upon request. Please do not hesitate to contact Josh Tabish, Director of Policy and Advocacy (josh.tabish@cira.ca) should you require further details.

cira

319 McRae Avenue, Suite 700,
Ottawa, ON K1Z 0B9

319, avenue McRae, bureau 700
Ottawa, ON K1Z 0B9

cira.ca
cira.ca/fr