The American Registry for Internet Numbers (ARIN)

Written Submission for the Pre-Budget Consultations in Advance of the 2021 Budget

Standing Committee on Finance

House of Commons
Ottawa ON K1A 0A6
Canada

Contact: Mr. John Curran
ARIN, Chief Executive Officer
(703) 227-9850
jcurran@arin.net

Stephen M. Ryan, Esq.
ARIN, General Counsel
(202) 756-8333
sryan@mwe.com

- **Recommendation 1:** The American Registry for Internet Numbers (ARIN) recommends that the Government of Canada continue to work in collaboration with industry stakeholders, including but not limited to Canadian Internet Service Providers (ISP), law enforcement agencies, intellectual property content owners, and civil society to ensure that ARIN's number resource directory continues to be free and publicly available, to meet the needs of Canadian society.

- **Recommendation 2:** The Government of Canada should formerly recognize the importance of ARIN's role by way of public declarations of support.

Introduction

The American Registry of Internet Numbers (ARIN) thanks the members of the House of Commons Standing Committee on Finance for the opportunity to contribute to its consideration of recommendations for Budget 2021.

As the complexity of security and economic challenges online has grown, the Government of Canada has made important investments in recent years to ensure that law enforcement agencies and civil society had the tools to address a changing world. Budget 2018 saw $507.7 million over five years invested in Canada's National Cyber Security Strategy and the creation of the Canadian Centre for Cyber Security, along with $116.0 million to support the creation of the National Cybercrime Coordination Unit within the Royal Canadian Mounted Police (RCMP). Budget 2019 saw further investments, including $144.9 million over five years to strengthen the cyber security of critical infrastructure, $80 million over four years to support Canadian cyber security networks, and $30.2 million over five years to protect Canadian democracy from cyber attacks and misinformation.

COVID-19 has further laid bare online vulnerabilities and the importance of strong cybersecurity frameworks and policies. Health misinformation has spread online, including websites imitating coronavirus websites of the Government of Canada. Bad actors have targeted individuals looking to access government support programs and people working from home on less secure networks. Health researchers have faced cyber attacks from those looking to steal valuable data.[1] The RCMP even warned that child predators were increasing their online activity, believing the pandemic offered them increased access to children. In late April, the RCMP told the CBC that it had identified at least 852 IP addresses in Canada that had shared child sexual exploitation material over in the 30 days previous.[2]

For over 20 years, a foundational element giving Canadian law enforcement and civil society the ability to trace and investigate illegal activities online has been the public availability of ARIN's Whois database of internet number addresses. ARIN's strong and effective industry supported self-governance framework has ensured that this important resource has remained available without government funding, management or direction. It is important for policy makers to ensure that the ability to identify possible sources of cybercrime and illicit activities online is maintained.

About ARIN

Established in 1997, the American Registry for Internet Numbers (ARIN) is a non-governmental, non-profit, member-based organization that supports the governance of the Internet through the management and registration of Internet Protocol ('IP') number resources throughout our service region (comprised of Canada, the United States, and numerous Caribbean and North Atlantic islands). No government funding is provided to support ARIN's activities. ARIN's IP number address registry is currently freely utilized by Canadian private sector entities, law enforcement, and foreign counterintelligence.

ARIN's Whois Directory

Since 1997, Internet service providers of all sizes in Canada – ranging from large nationally known entities and corporate end users to small entrepreneurial ISPs – have successfully participated in a self-governance framework for Internet address coordination that works collegially with both the private sector and government entities.

[1] Canadian Centre for Cyber Security, Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity, 27 April 2020, https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threat-activity

[2] CBC News, *Online sexual predators eager to take advantage of greater access to kids during COVID-19*, police warn, 24 April 2020, https://www.cbc.ca/news/canada/sexual-predators-children-online-pandemic-1.5542166

When requested, ARIN issues the rights to utilize large blocks of IP numbers to ISPs. An ISP may then sub-allocate these numbers to their own customers as required. ARIN maintains the definitive registry IP numbers issued in our service region in our "Whois" IP directory, where records for holders of large blocks of IP numbers must include a name and business contact details for a designated employee responsible for responding to enquiries.

It should be noted that ARIN and Whois do not hold any information on individuals who have been sub-allocated IP numbers, ensuring that privacy is protected for citizens online. ARIN registry policies have been developed jointly with industry, government, and civil society that provide appropriate mechanisms to avoid identification of IP address assignments that might be associated with single households.

Whois is of significant value to any Canadian individual, business or government entity with the need to identify which ISP has been issued a specific IP number. The designated employee contact identified in Whois must be able to be reached at 24 hours a day should information be needed on an address they hold. This ensures that those needing to urgently trace an internet address, such as law enforcement tracking a cyber attack, can reach the appropriate person without significant delays.

Canadian national and provincial law enforcement and counter intelligence agencies (and their public/private partners in cyber security and anti-abuse) rely on open access to the ARIN Whois directory so they can update government files used in a range of agency activity, which can be as diverse as law enforcement investigations of cyber bullying, resolving cyber attacks, or investigating cybercrimes more generally.

Whois is also essential to protecting the rights of Canadian cultural content creators. For example, if a Canadian artist discovered that a website was illegally making their copyright protected work available for download and wanted to take steps to stop this activity, Whois would be the first stop for the artist or their legal representatives. A search of Whois would locate the organization holding the IP address that the website is using. Whois would contain no details on the operator of the website but would reveal that the number is part of a block of addresses allocated to a large ISP. The artist's legal representatives would then reach out to the designated contact for the ISP to notify them of the illegal activity and would be required to follow all standard legal processes compel the ISP to warn the operators of the offending website or disclose identifying information on the customer to whom the ISP had allocated that IP number.

Maintaining the ARIN Whois Directory

The Internet has historically relied upon 32-bit Internet Protocol Version 4 (IPv4) Internet numbers to uniquely identify connected devices. These IPv4 addresses were issued in blocks to ISPs, with requests for new numbers fulfilled only upon a demonstration that the ISPs previously issued allocations were sufficiently utilized to justify the need for a new block of numbers. This demonstration of need also required ISPs to ensure that their IP allocations recorded in Whois were up to date.

With the supply of IPv4 numbers from the ARIN registry now depleted, the Internet is now transitioning to its successor, Internet Protocol Version 6 (IPv6), providing enormous capacity for accommodating future Internet growth. While IPv4 supported approximately 4 billion devices total for the global Internet, IPv6 enables 340 trillion trillion trillion IP addresses to be used - more than 100 times the number of atoms on the surface of the Earth. However, this transition does not diminish the need for accurate records.

The technical standards of the Internet established by the Internet Engineering Task Force ("IETF") require that the initial IPv6 assignment to each ISP be quite sizable. In fact, for efficiency of the Internet routing system, it is required that each of these individual ISP IPv6 allocations be larger than the entire global IPv4 number pool. While ARIN policy requires each ISP to record when it sub-allocates space from its IPv6 block, the frequency of

updates or the accuracy of records will not be routinely reviewed by ARIN due to the lack of any need for the ISPs to regularly obtain additional IPv6 address blocks.

Non-Monetary Encouragement and Continued Recognition by Canada's Government

The Royal Canadian Mounted Police, the Federal Bureau of Investigation, and U.S. Drug Enforcement Administration have come together in a cross-border effort to address this exact issue. They presented recommendations resulting from a collaboration of these law enforcement agencies (LEA) which address their need that accurate registry records be maintained. They provided specific examples of the benefit to Canadian law enforcement of having such updated records, as well as cautionary information about the impact of non-updated records that do not permit the LEA to serve process on the ISP that that has supplied specific IP number to the person or business entity for an Internet address of interest. We are happy to share their presentation with members of the Committee.

The House of Commons Standing Committee on Industry, Science and Technology also recognized the importance of ARIN's Whois for the protection of the intellectual property of Canadian creators. In the Committee's June 2019 report on the statutory review of Canada's Copyright Act, it included the following recommendation:

> Recommendation 26
> That the Government of Canada examine ways to keep IPv6 address ownership information up-to-date in a publicly accessible format similar in form and function to American Registry for Internet Numbers' iPv4 "Whois" service.

We encourage the Government of Canada to demonstrate its support for the principle of Internet self-governance and a free and effective Whois directly by formally recognizing the importance of ARIN's role by way of public declarations of support.

We also recommend that the Government of Canada continue to work in collaboration with ARIN and industry stakeholders, including but not limited to Canadian Internet Service Providers (ISP), law enforcement agencies, intellectual property content owners, and civil society to ensure that ARIN's Whois directory continues to be free and publicly available, to meet the needs of Canadian society.

Conclusion

Canada has made important investments in cybersecurity and COVID-19 has reinforced the necessity of ensuring strong defences from online threats. ARIN believes that the current successful principle of Internet self-governance can continue to meet the needs of Canadian law enforcement and security services, as well as other Canadian civil society stakeholders. We would be pleased to meet with the Finance Committee to further discuss how the Government of Canada can ensure that the services provided in Canada such as the ARIN registry and IP number Whois directory remains free, effective and available to support efforts and investment to strengthen cybersecurity in Canada and combat cybercrime and other illicit online activities.