Appearance before the House Standing Committee on Public Safety and National Security, February 27, 2019

Good afternoon. My name is Christopher Parsons. I am a research associate at the Citizen Lab, which is a part of the Munk School of Global Affairs & Public Policy at the University of Toronto. I appear at this committee in a professional capacity that represents my views and those of the Citizen Lab. My comments today focus on a range of securitization practices that, if adopted, would mitigate some of the contemporary risks that participants in the financial sector face.

Canadian government agencies, private businesses and financial institutions, as well as private individuals rely on common computing infrastructures. We use the same iPhone and Android operating systems, the same customer service interfaces and e-commerce platforms, the same underlying codebases, and largely identical third-party cloud computing infrastructures. The sharedness of these platforms means that efficiencies can leveraged to improve productivity and efficiency, but these benefits are predicated on the overall security of these shared products. To be blunt, the state of computer insecurity is profound and the large number of vulnerabilities in these shared products, writ large, threaten the financial sector to the detriment of Canada’s national security interests.

In my remaining time I want to point to four issues that I believe need to be taken up to ensure that Canada’s national interests are better secured in the future than they are, today. They include the need for Canada to formally establish a responsible national encryption policy, update Canada’s vulnerability equities programs, develop a vulnerability disclosure program framework, and promote two factor authentication. I now turn to the issue of responsible encryption policies

1. Responsible Encryption Policies

Given the state of computer insecurity, it is imperative that the Government of Canada adopt and advocate for responsible encryption policies. Such policies entail commitments to preserving the right of all groups in Canada to use computer software using strong encryption. Strong encryption can be loosely defined as encryption algorithms for which no weaknesses or vulnerabilities are known or have been injected, as well as computer applications that do not deliberately contain weaknesses designed to undermine the effectiveness of the aforementioned algorithms.

The benefits of strong encryption cannot be overstated. In a technological environment marked by high financial stakes, deep interdependence, and extraordinary complexity, ensuring digital security is of critical importance and extremely difficult. The cost of a security breach, theft, or loss of customer or corporate data can have devastating impacts for private sector and individuals’ interests. Any weakening of the very systems that protect against these threats would represent irresponsible policymaking. Access to strong encryption encourages consumer confidence that the technology they use is safe.

And it is important to recognize that there are risks to the availability of strong encryption. As an example, one of Canada's closest allies, Australia, has adopted irresponsible encryption policies which may introduce systemic vulnerabilities into code used by the financial sector, as well as other sectors of the economy. Once introduced, such vulnerabilities might be exploited by actors holding adversarial interests towards Canada. Threat activities might be carried out against the SWIFT network, as just one of many examples, should any element of that network rely on cryptographic products made vulnerable by Australian demands.

Furthermore, strong encryption prevents our closest allies from monitoring Canadian financial activities beyond the above-the-board processes associated with FINTRAC. As one example, the Globe and Mail revealed that the United States' National Security Agency was monitoring Royal Bank of Canada's Virtual Private Network tunnels. The story suggested that the NSA's activities could be a preliminary step in broader efforts to "identify, study and, if deemed necessary, "exploit" organizations' internal communications networks."

In light of these kinds threats, the Government of Canada should adopt a responsible encryption policy. Such a policy would entail a firm and perhaps legislative commitment to require that all sectors of the economy have access to strong encryption products, and would stand in opposition to irresponsible encryption policies, such as those calling for 'backdoors'.

I now turn to the management of computer vulnerabilities by the Government of Canada itself.

2. Vulnerabilities Equities Program

Vulnerabilities in computer code are acquired by Canada's Communications Security Establishment, or the CSE. Thereafter, the CSE determines whether to retain or disclose the vulnerabilities. The CSE is motivated to retain vulnerabilities to obtain access to foreign systems as part of its signals intelligence mandate and, also, to disclose vulnerabilities to better secure government systems. To date, the CSE has declined to make public the specific processes by which it weighs the equities in retaining or disclosing vulnerabilities. In contrast, the United States publishes how all federal government agencies evaluate whether to retain or disclose the existence of a vulnerability.

The CSE's stockpiles of vulnerabilities can potentially be uncovered and used by adversaries, and this has happened to both the United States' NSA and CIA, to the effect of costing billions in direct economic damage. The ongoing presence of these stockpiles, and lack of clarity concerning what vulnerabilities are retained, mean that businesses and private individuals will have a reduced confidence in the reliability and security of products that are needed to enhance Canada's economic efficiency and productivity, and prospectively slow Canadians' adoption of contemporary and next-generation software, platforms, and infrastructure.

To alleviate these concerns, the Canadian government should publicize its existing vulnerabilities equities programs and hold consultations on their effectiveness in protecting software and hardware that is used in the course of financial activities. Furthermore, the government should include the business community and civil society stakeholders in the existing, or reformed, vulnerabilities equities programs. Including these stakeholders will encourage heightened disclosures of vulnerabilities and thus improve the availability of well-written software, and reduce threats faced by the financial sector.

3. Vulnerabilities Disclosure Program

It’s important to recognize that security researchers routinely discover vulnerabilities in hardware and software that are used in all walks of life, including the financial sector. Relatively few organizations, however, have explicit procedures that guide researchers in how to responsibly disclose such vulnerabilities to the affected companies. Disclosing computer insecurities absent a vulnerability disclosure program can lead companies to inappropriately threaten litigation to whitehat security researchers. Such potentials reduce the willingness of researchers to disclose vulnerabilities.

Beyond studying the laws around unauthorized access to computer code, I would recommend that the government create a draft policy for the financial sector companies to adopt. Such a disclosure policy should establish to whom vulnerabilities are reported, how reports are treated internally, how long it takes for a vulnerability to be remediated, and insulate security researchers from legal liability so long as they do not publicly disclose the vulnerability ahead of the pre-established delimited period of time. Moreover, the government should move to develop and adopt a similar disclosure programs for its own departments to benefit from researchers’ reporting of vulnerabilities in government systems.

4. Two Factor Authentication

Finally, I turn to the topic of two factor authentication, or 2FA. 2FA refers to where an individual must be in possession of at least two ‘factors’ to obtain access to their accounts. The ‘factors’ most typically used for authentication include something that you know (e.g. a PIN or password), something you have (e.g. hardware token or random token generator), or something that you are (biometric, e.g. fingerprint or iris scan). These multiple factors mean that losing a login and password pair does not enable third-parties to access a protected system or data store.

It is important for consumer-facing systems to have strong 2FA to preclude unauthorized parties from obtaining access to personal financial accounts; such access can lead to better understandings of whether persons could be targeted by a foreign adversary for espionage recruitment, cause personal financial chaos designed to distract a person while a separate cyber activity is undertaken, or direct money to parties on terrorist or criminal watchlists.

Some Canadian financial institutions do offer 2FA but typically default to a weak mode of second factor authentication. This is problematic because SMS is a weak communications medium, and can be easily subverted by a variety of means. This is why entities such as the United States’ National Institute of Standards and Technology no longer recommends SMS as a two factor authentication channel.

To improve the security of customer-facing accounts, I recommend that financial institutions should be required to offer 2FA to all clients and that the pro-offered 2FA utilize hardware or software tokens. Implementing this recommendation will reduce the likelihood that unauthorized parties will obtain access to accounts for the purposes of recruitment or disruption activities.

To conclude, Canadian businesses and private individuals rely on digital tools for all aspects of their lives, including activities which intersect with the financial sector. To be clear the proposals I have recommended will not solve all of the computer insecurity problems that threaten Canada's national security interests nor the financial sector. But these proposals represent good efforts towards resolving the most basic threats and, also, would serve to build trust in the security of our digital tools.

Thank you for your time, and I look forward to your questions.