CYBER SECURITY
COOPERATIVE
RESEARCH
CENTRE

Question on notice: What similar powers do other Five Eyes states have to those proposed in the SLAID Bill?

Given the diversity of legislative mechanisms, law enforcement and intelligence functions across the Five Eyes, it is difficult to make direct comparisons with the measures proposed in the SLAID Bill. However, it is important to note that our allies also recognise the threats posed by the dark web and anonymising technologies and the distinct and unique challenges they present for law enforcement. Hence, steps have been taken by several Five Eyes' states – namely the United States, the United Kingdom and Canada – to counter the proliferation of crime committed on the dark web and via anonymising technologies. Below the CSCRC sets out three examples of similar capabilities in these states.

The United States

The Federal Bureau of Investigations (FBI) is the United States' federal law enforcement agency, responsible for domestic intelligence and security. The United States' warrant framework provides significant flexibility in the application of warrants as they pertain to the commission of online crime, enabled via Rule 41 of the *Federal Rules of Criminal Procedure*. This includes via search and seizure warrants, which may be used to access (including remotely) and search electronic devices.

United Kingdom

In the United Kingdom, the *Investigatory Powers Act 2016* (the Act) is the principal legislation that governs the use of electronic surveillance powers by law enforcement, security and intelligence agencies. The Act includes legislative mechanisms for agencies to access and interfere with electronic devices to obtain data. The Act also enables the utilisation of bulk interception, communications data and equipment interference powers. The Act has served in practice to identify threats and assist in the application of targeted powers to address these threats.

Canada

Canadian law enforcement agencies can use general warrants under the *Criminal Code 1985* to respond to cyber-enabled crime to enable activities not covered by other warrants. General warrants provide the mechanisms for investigative techniques, such as account takeover. Furthermore, general warrants are focused on obtaining information relevant to criminal investigations.