23.

National Security Law

"National security" is not a defined term in Canadian law; it is what the government says it is and for this reason, individuals and businesses are vulnerable to unpredictable and even arbitrary action by government — action that can reduce profit margins, disrupt productivity, and even end commercial viability.

In practical terms, national security relates to any action or event that could materially impact the health, safety, security, or economic well-being of Canadians, or the effective functioning of Canada's governments. Events surrounding COVID-19 have highlighted the degree to which Canada's critical infrastructure can be compromised and the well-being of Canadians adversely impacted. This has resulted in a sharply increased focus on national security by the Government of Canada in the context of its legislative, regulatory, and policy activities. These impacts are particularly relevant in the areas of Foreign Investment, Privacy and Cybersecurity, Procurement and Government Contracts, Export Controls, Controlled

Goods, Economic Sanctions, and Anti-bribery and Corruption, White Collar Defence and Investigations and Labour and Employment.

Foreign Investment

Foreign investment is generally considered beneficial to Canada, to the foreign investors involved, and to the commercial enterprises resulting from or impacted by those investments. Foreign investment has the potential to enhance growth and innovation in Canada, to create quality jobs, to raise living standards, and to help spread good practices in management and responsible business conduct. For these reasons and others, Canada generally welcomes foreign investment.

However, foreign investment can –under certain circumstances– raise concerns related to Canada's national security. In recent years, these concerns have generated a higher degree of serious review and consideration. Canada has introduced mechanisms that allow for the review of certain investment proposals. Efforts in this area have advanced significantly since the national security review procedures under the *Investment Canada Act* (ICA) were introduced in 2009.

The Governor in Council (i.e., the federal Cabinet) may review an investment implemented or proposed by a non-Canadian to, among other things, acquire control of a Canadian business or to partially or fully acquire or establish an entity carrying on all or any part of its operations in Canada. Where the responsible minister under the ICA has reasonable grounds to believe that such an investment could be injurious to national security, a review may occur regardless of whether or not the investment is subject to a net benefit review or notification under the ICA.

Revised Guidelines on the National Security Review of Investments issued under the ICA on March 24, 2021 inform foreign investors of the factors the government will take into consideration when administering a security review process, thereby providing a clearer picture as to the circumstances under which the Government of Canada may initiate a national security review.

As of August 2, 2022, the *Regulations Amending the National Security Review of Investments Regulations* provide non-Canadian investors with the ability to voluntarily and officially subject themselves to the security review process on a pre-closing basis, even though their proposed investment is not otherwise subject to mandatory notification or net benefit review.

In light of Canada's Critical Minerals Strategy, applications for acquisitions of control of a Canadian business involving Critical Minerals by a foreign state-owned enterprise will only be approved on an exceptional basis. Further, all investments, including greenfield and minority investments, regardless of value, whether direct or indirect, whether controlling or non-controlling, and across all stages of the value chain, will be subject to the national security review process of the ICA.

Canada's Minister of Innovation, Science and Industry announced on December 7, 2022 Bill C-34, which will significantly amend the ICA for the first time since 2009. These amendments, if passed, will provide, among other changes, new filing requirements prior to the implementation of investments in prescribed business sectors and strengthen penalties for non-compliance.

For more information about the ICA, see Investment Policy Chapter.

Privacy and Cybersecurity

Privacy and cybersecurity present unique opportunities and risks across business operations. Legal frameworks and market forces in these areas are rapidly evolving, at a pace that outstrips the ability of government and regulatory authorities to keep up. The risks of economic cyber espionage, ransomware attacks, and distributed denial-of-service (DDoS) attacks pose increasing threats to businesses' operational technologies, critical infrastructure, and informational assets ranging from trade secrets to personal data. Businesses must be aware of their obligations and respond to threats through data protection legislation compliance, preventative cybersecurity planning and risk management, and data breach investigations and response planning. Businesses must also remain up-to-date regarding the evolving legal and regulatory landscape, as governments respond to these threats.

For more information about privacy and cybersecurity, see Privacy and Anti-Spam Laws Chapter.

Procurement and Government Contracts

Public procurement and government contracts form a remarkably complex area of the law. The procurement landscape varies by jurisdiction and within jurisdictions, and is influenced by a multitude of factors, including common law, statutes, regulations, international and national treaties, directives, policies and customs.

While often considered an issue in the federal realm, increasingly, all levels of the public sector are increasingly addressing security considerations when they purchase goods and services. Security reviews are increasingly being required as part of the procurement process, and can involve security and risk assessments of the supplier and its personnel, the physical and technical infrastructure of the supplier, and the supply chain. Export controls and sanctions compliance is not static, as the Government of Canada responds to security risks to Canada and Canadians.

For more information about procurement and government contracts, see Procurement in Canada Chapter.

Export Controls, Controlled Goods, Economic Sanctions, and Anti-bribery and Corruption

A national security review under the *Investment Canada Act* can risk delaying, blocking, or unwinding a transaction. The Canadian government has issued guidelines for the national security review process, which explicitly include concerns related to export controls, controlled goods, and may also involve sanctions and anti-bribery and corruption laws. It is important that companies understand their obligations in relation to these issues in order to avoid significant monetary and criminal penalties, costly delays or prohibitions to business activities, and reputational damage to the business and individuals.

Failure to comply with export controls, controlled goods, sanctions and anti-bribery and corruption laws and regulations can result in extremely severe penalties, consequential delays to transactions, and substantial reputational damage that can harm future business opportunities.

For more information about export controls, controlled goods, economic sanctions, and anti-bribery and corruption laws, see Doing Business in Canada Guide – International Trade Chapter.

White Collar Defence and Investigations

Businesses failing to adhere to security and regulatory requirements may be subject to investigation and criminal charges. Even businesses that are not suspected of wrongdoing may find themselves the subject of investigations with a national security dimension. When persons or businesses operating in Canada or abroad are subject to criminal charges or investigations with a national security element, the stakes are particularly high.

In addition to the possibility of corporate staff facing prison time, a business may receive monetary fines and suffer reputational damage that can imperil the goodwill upon which the company has built its business and maintains its competitive advantages.

Cases raising national security concerns present unique challenges not found in typical litigation or investigations – they demand a team with experience in criminal, regulatory and national security matters. Litigation involving disclosure of classified information may attract the application of s. 38 of the *Canada Evidence Act*.

Criminal, regulatory or other investigations implicating national security concerns may emerge from many sources relating to allegations of foreign or domestic corrupt practices, immigration violations, commercial fraud, tax evasion and breaches of international sanctions. Investigations may also follow privacy breaches or cyber-attacks and the theft of sensitive information.

Labour and Employment

Although not always thought of as having a "national security" angle, employers and their employees who operate in critical infrastructure areas; examine, possess, or transfer controlled goods, export outside of Canada, or have access to protected or classified government information or assets are subject to various laws and regulatory requirements surrounding national security. These requirements can raise employment-related considerations not addressed in standard-form employment agreements or that may not have existed when an employee was hired. Canada's employment laws do not provide that employees are hired "at will". The ability to impose new terms of employment arising from security-related requirements post-hire, combined with the impact of privacy laws, make this an area where national security-related requirements need to be carefully navigated and addressed.

For more information about labour and employment issues, see Labour and Employment Chapter and Privacy and Anti-Spam Chapter.