OSLER

Canada's defence build-up and the new M&A playbook

MAY 25, 2026 20 MIN READ

Related Expertise

- Artificial Intelligence
- Banking and Financial Services
- Competition and Foreign Investment
- Defence, Security and Aerospace
- Emerging and High Growth Companies
- Foreign Investment Review
- International Trade
- Mergers and Acquisitions
- Privacy and Data Management
- Private Equity
- Technology

Authors: Hugo-Pierre Gagnon, Michael Fekete, Shuli Rodal, Jesse Goldman, Éloïse Gratton, Ad. E., Stéphane Eljarrat, Sam Ip, Marta Rochkin, Raphaël Amram, Justin Dharamdial, Chelsea Rubin, Kevin Li

Executive summary

Canada's accelerated defence spending, procurement reform and emphasis on sovereign industrial capacity are reshaping the domestic M&A market. For buyers, investors and portfolio companies, the opportunity is significant, particularly in dual-use technology, aerospace, cybersecurity, digital infrastructure and supply chain assets. At the same time, defence-related transactions require early attention to national security review, procurement eligibility, security clearances, export controls, controlled goods compliance, sanctions and broader supply chain enforcement risk. In practice, the most successful transactions will be those that combine commercial discipline with regulatory readiness from the outset.

Canada has officially hit the 2% NATO spending benchmark as of March 2026 and is firmly committed to NATO's Defence Investment Pledge of 5% of GDP by 2035.[1] This increase in defence-related spending includes a focus on dual-use technologies, as shown by the recently announced $200-million investment for a Canadian-owned spaceport in Nova Scotia.[2] These investments, coupled with changes to the government procurement process and Canada's new membership in the Security Action for Europe (SAFE) initiative, create new opportunities in the Canadian M&A landscape and raise several key considerations outlined below.

Overview of changes to Canada's defence-related spending

The NATO commitment

Over $14 billion of the total defence expenditure from the Canadian government in 2025–2026 came from departments outside of National Defence, with heavy allocations toward cybersecurity, space and related procurement.[3] This indicates that dual-use tech startups and commercial IT firms are actively capturing defence dollars, making them highly attractive targets for scale-up capital and roll-up strategies.

Additionally, the government is injecting billions into hard assets and operational capacity.

This includes $648 million for new aviation support facilities (supporting the CP-8A Poseidon and CQ-9B Guardian fleets), $1.2 billion for critical power and infrastructure modernization at CFB Halifax and $82.5 million to acquire the 475-acre Halifax Gate industrial site.[4] These projects offer immediate, tangible contracting and supply chain opportunities.

Canada's undertakings

Removing barriers in the procurement process is a crucial step in increasing Canada's defence spending. To that end, the government has highlighted the newly formed Defence Investment Agency (DIA) as the primary vehicle for cutting red tape, streamlining procurement and rapidly growing the domestic defence industrial base.[5] Legislation will be introduced this spring to make the DIA a standalone entity that will act as the point of contact for defence-related investment and procurement.[6]

In parallel, the newly released Defence Industrial Strategy (DIS) acts as the foundational blueprint designed to position Canadian industry for $180 billion in procurement and $290 billion in capital investment over the next decade. It formally enforces a strict "Build-Partner-Buy" procurement framework, making domestic production the absolute default starting point across 10 identified sovereign capabilities.[7]

> Dual-use tech startups and commercial IT firms are actively capturing defence dollars, making them highly attractive targets for scale-up capital and roll-up strategies.

As previously mentioned, the announcement of a $200-million investment in Maritime Launch Services, a Canadian-owned spaceport, further signals Canada's commitment to developing its defence capabilities and dual-use technologies.[8] The government hopes to achieve operational capability by 2028 and is providing $105 million through the *Launch the North* contest to award innovators that help advance Canada's space launch capabilities.[9] So far, NordSpace, Canada Rocket Company and Reaction Dynamics have each been conditionally approved for $8.3 million in funding through the first round of this contest.[10] Canada is also in the planning stages of constructing a ground station for NATO satellites, which would be the first of its kind in North America if the project is approved.[11]

Lastly, the Business Development Bank of Canada (BDC) raised the funding cap of its Defence Platform to $6 billion in a bid to further support small- and medium-sized enterprises (SMEs) in Canada's defence ecosystem.[12] Within the Defence Platform is the new StrongNorth Fund, a $300-million venture capital fund which will support early-stage startups developing defence-focused or dual-use technologies.[13]

The Defence, Security and Resilience Bank

The Defence, Security and Resilience Bank (DSRB) is designed to be a multilateral financial institution that pools allied credit strength and mobilizes private capital for global defence and security initiatives.[14] Canada is set to become the host country of the bank's headquarters, and six of the 11 commercial banks that will back the DSRB are Canadian.[15] With Canadian banks backing this strategic initiative, commercial lending for defence-related undertakings may expand significantly.

Once established, the DSRB will have three strategic implications. First, the DSRB will be able

to provide long-term, low-cost financing for defence firms across NATO member nations.[16] Second, the DSRB will address structural capital gaps that constrain SMEs operating within complex, long-cycle defence procurement environments.[17] Third, any equity contributions made by member states to capitalize the DSRB will count toward achieving the NATO GDP defence spending targets, which creates a new avenue for member states to meet their 5% spending target.[18]

Canadian financial institutions have historically been reluctant to finance the defence industry, in part because the sector was not viewed as sufficiently "bankable" and because of political and regulatory complexity. That may now be changing. As Canadian banks back this strategic initiative, commercial lending for defence-related undertakings may broaden materially.

If the DSRB achieves the strong credit profile expected of it, participation in defence financing will be meaningfully de-risked for Canadian financial institutions. That, in turn, should lower financing costs for defence firms, improve lender comfort with the sector and support more standardized and scalable lending models. Over time, increased familiarity with defence projects may also accelerate the rollout of commercial lending solutions.

Key considerations for buyouts and equity investments

Defence-related deals in North America are up 123% year-on-year as geopolitical shifts have pulled a broad pool of capital into the market.[19] Defence sector investment is evolving from a niche strategy into a core focus area for investors across technology, industrials and infrastructure as increased military budgets accelerate deal activity.[20]

However, buyout transactions and equity investments in the sector are often highly bespoke. The defence industry is heavily regulated and subject to heightened governmental and cross-border scrutiny because of the security concerns that surround the sector. Even where targets are not purely defence businesses, but instead design, develop, manufacture, distribute or sell dual-use products with primarily civilian purposes and important military or security applications, transactions tend to involve complex legal and regulatory issues that require sophisticated planning. This is true regardless of deal size.

In this section, we highlight key diligence considerations and regulatory pitfalls that should be addressed early in transaction planning.

The Canadian M&A landscape

The Canadian M&A market achieved a stable footing in late 2025, moving away from previous macroeconomic volatility. In the third quarter of 2025, Canada recorded 642 deals, with a total announced value of $138.8 billion.[21] Dealmaking is increasingly characterized by domestic consolidation, with local transactions — where Canadian buyers invest in Canadian targets — now representing half of all M&A activity in the country and expected to anchor the market through 2026.[22]

In the aerospace and defence sectors, two catalysts are likely to shape transaction pace and structure through 2026.

First, a succession gap in the $5-million to $50-million enterprise value range is driving private equity and Entrepreneurship Through Acquisition (ETA) roll-up strategies aimed at preserving viable supply chain assets. This dynamic reflects a broader demographic shift:

more than 75% of Canadian small business owners plan to exit within the next decade, yet fewer than 9% have a formal succession plan.[23]

Second, the release of Canada's DIS earlier this year established a strict "Build-Partner-Buy" framework that prioritizes domestic production and suppliers. This is aligned with the "Policy on Prioritizing Canadian Materials in Federal Procurements," which prioritizes the use of Canadian-produced steel, aluminum and wood products in major federal construction and defence projects. Pursuant to a parallel policy on prioritizing Canadian suppliers and Canadian content in strategic federal procurements, Canadian suppliers (including some foreign-headquartered entities) receive a 10% reduction to the value of their financial proposals for bid evaluation purposes in specified categories of procurements. A price-based evaluation credit of up to 25% is also available to account for Canadian value-added goods or services that form part of a proposal. A forthcoming SME Procurement Program will create tailored streams for SMEs and provide support to help SMEs navigate federal procurement requirements.

That said, heightened scrutiny under the *Investment Canada Act* (ICA) and a revamped federal *Competition Act* means that regulatory preparedness is paramount.

This shift in federal policy, combined with a significant influx of capital, is also expected to drive private equity roll-up strategies across Canada's fragmented small- and medium-sized business landscape, potentially creating a high-growth strategic asset class and enabling national champions to emerge.

Cybersecurity, AI and digital infrastructure

Cybersecurity has become a critical consideration in defence sector M&A transactions. With over $14 billion of defence expenditure flowing through departments outside of National Defence, much of it directed toward cybersecurity and related procurement, acquirors must conduct rigorous cybersecurity due diligence to assess both value and risk. This is particularly important given that dual-use technology firms and commercial IT companies are now capturing significant defence dollars, making them attractive targets for consolidation.

From a due diligence perspective, buyers should carefully assess a target's cybersecurity posture, including its compliance with applicable privacy and data protection laws, incident response capabilities and history of security breaches. In the defence sector, this analysis takes on heightened importance because targets often handle sensitive government information, classified data and personal information of individuals with security clearances. Any gaps in data governance or cyber hygiene can expose acquirors to regulatory enforcement, reputational harm and potential disqualification from government contracts.

> Even where targets are not purely defence businesses, transactions tend to involve complex legal and regulatory issues that require sophisticated planning.

Buyers should also consider Canada's evolving regulatory landscape for cybersecurity. The proposed *Critical Cyber Systems Protection Act* (CCSPA),[24] if enacted, will establish a new federal framework governing the cybersecurity of Canada's critical infrastructure, a category that will likely capture many defence-adjacent businesses. The legislation will designate certain organizations as operators of "critical cyber systems" and require them to implement formal cybersecurity programs, address risks arising from their supply chains and third-party technologies and report cybersecurity incidents that meet prescribed thresholds. The CCSPA will grant a range of federal regulators broad inspection, audit and order-making powers,

including the authority to direct operators to cease non-compliant activities or undertake specific corrective measures.

As such, if enacted, the CCSPA will significantly elevate cybersecurity obligations across sectors critical to national security and economic stability, requiring more robust governance, risk management and operational safeguards, alongside stricter supply chain oversight, enhanced due diligence, stronger contractual protections and continuous monitoring of third-party risks. It will also expand incident reporting and regulatory transparency requirements, increasing the likelihood of follow-up reviews and mandated remediation, while placing greater accountability on boards and senior leadership for cybersecurity readiness and resource allocation. In doing so (and if passed), the legislation will materially raise Canada's regulatory baseline for cybersecurity, reinforcing a more stringent compliance environment with direct implications for defence strategy and M&A activity.

Additionally, firms handling controlled goods or operating under government contracts may be subject to specific cybersecurity requirements under the Controlled Goods Program (CGP),[25] a Canadian federal regulatory program that governs the possession, examination and transfer of sensitive military and defence-related goods and technology within Canada, and related procurement frameworks. Parties should assess the target's compliance with these regimes and factor any remediation costs into transaction pricing.

Finally, cybersecurity considerations intersect with national security review under the ICA,[26] a Canadian federal law governing foreign investment in Canada. Transactions involving targets with access to sensitive technologies or government systems attract enhanced scrutiny. Parties should proactively assess whether cybersecurity vulnerabilities or data handling practices could raise national security concerns that might delay or jeopardize regulatory approval.

Government procurement and security clearances

In the context of M&A, procurement and security clearance regimes often determine whether the target can continue to perform government work post-acquisition. This is a particularly significant consideration where revenue is heavily dependent on government contracts and is contingent on maintaining procurement eligibility and required clearances.

Key considerations for buyers include the following:

- **Assessment of procurement frameworks.** Buyers should assess a target's participation in federal procurement frameworks (e.g., standing offers and defence-specific contracting vehicles). Change-of-control provisions may trigger notice or consent requirements and, in some cases, impact eligibility for ongoing or future work.
- **Security clearances.** Under Canada's Public Services and Procurement Canada's Contract Security Program (CSP), contractors must hold facility security clearances, and key personnel must hold individual clearances to access protected or classified information and to perform certain government contracts. These clearances are not automatically transferable on closing and are impacted by changes in ownership, control and foreign involvement.
- **Standard clauses.** Government contracting frameworks, including the Standard Acquisition Clauses and Conditions (SACC), are often rigid and not often aligned with

commercial market practices, particularly for high-growth technology companies. Buyers should understand how these terms allocate risk and IP ownership, and the extent to which they can be mitigated.

- **Approvals and timing.** A buyer cannot assume that it can simply "step into the shoes" of the target. A change of control may trigger a reassessment of the target's facility clearance or require new clearances. If the buyer does not already hold the requisite clearance, there is a real risk of delay, suspension of work or even loss of eligibility for certain contracts. Timing to obtain or update clearances can be material, are often uncertain and should be treated as a core execution risk in deal planning.

Procurement eligibility and clearance continuity should be treated as core transaction risks and addressed early in diligence and transaction structuring.

AI, intellectual property, quantum and technology

In the current defence environment, where Canadian policy is increasingly focused on sovereignty and domestic capability, the value of AI and other advanced technologies is increasingly about whether it can be owned, controlled and deployed within those constraints.

Key considerations for buyers include the following:

- **Open data and open source.** AI and quantum systems necessarily rely on open-source software and open datasets. Buyers should assess the provenance and licensing of training data, including whether datasets are subject to open-source or "copyleft"/ "viral" obligations that may constrain commercialization or conflict with government use requirements. Deficiencies or gaps can impact the ability to deploy within government contexts.
- **Collaboration with research institutions and universities.** Many AI and quantum companies operate in partnership with universities and research institutions, which often impose institution-specific IP policies. These arrangements may limit exclusivity, impose licensing obligations or otherwise restrict control over the underlying technology. In an M&A context, these constraints can materially affect the acquiror's ability to commercialize or scale post-closing.
- **Sovereignty considerations.** Digital sovereignty has become top of mind for the Canadian government as it navigates through a host of digital strategies and modernization initiatives.[27] As a result, Canadian defence policy and funding frameworks increasingly prioritize domestic development and data residency. Technologies developed, hosted or controlled outside Canada, or subject to foreign ownership or influence, may face limitations in procurement eligibility or access to funding. Buyers should assess whether the target's technology stack and operating model align with these expectations.
- **Alignment with international standards.** Oversight in Canada is increasingly shaped by industry standards, such as ISO/IEC 42001. In the defence sector, these standards may be referenced in or inform procurement requirements and can serve as a proxy for regulatory expectations. In practice, alignment helps to signal that AI systems are auditable,

controlled and suitable for use in sensitive environments.

The key diligence question is not only where the target has developed or owns these AI and other advanced technologies, but also whether they can be used, controlled and commercialized in a manner that aligns with Canadian defence considerations and broader sovereignty expectations.

National security

All foreign investment into Canada is subject to the ICA. The ICA imposes a mandatory filing regime for certain investments, including acquisitions of control of Canadian businesses through M&A. The ICA also includes a discretionary national security review regime, which applies broadly; the government may review an investment on national security grounds whether or not a filing is required in connection with the investment.

In March 2024, the Canadian government enacted significant amendments to the ICA through Bill C-34.[28] Many of the most consequential elements of these amendments are expected to come into force in 2026. In particular, the amendments, once in effect, establish a mandatory pre-closing notification obligation for foreign investments of any size in a Canadian entity, where the entity is operating in an enumerated sector and prescribed indicia are satisfied. The sectors will be set out in regulations, with a draft expected to be released shortly for public comment.

Industrial Technological Benefits Policy

Participating in Canadian M&A could give non-Canadian investors a competitive advantage in Canadian government contracts. Canada's Industrial and Technological Benefits (ITB) Policy requires that companies awarded major defence procurement contracts (above certain enumerated value thresholds) undertake business activity in Canada equal to the value of the contract. The policy is designed to ensure that defence procurement generates domestic economic benefit, including through the development of key industrial capabilities. Importantly, where a non-Canadian is acquiring a Canadian target with existing obligations under the Industrial and Technological Benefits Policy, the acquiror must be prepared to assume and fulfill these commitments. Failure to do so could result in restrictions on future government contracting opportunities.

Investors should be mindful that the Canadian government is reviewing the program and may amend the criteria and calculations this year or next year to reflect updates to developing government priorities.

Export controls and controlled goods

Canadian defence companies frequently handle goods, technology and technical know-how that is subject to transfer restrictions. More specifically, such items may be regulated under Canada's *Export and Import Permits Act*, and a permit may be required to export such items from Canada, including for transfers between affiliates. A change of control of an entity holding export permits may affect the validity of existing export permits and necessitate new applications. Foreign buyers and buyers with material operations outside of Canada should carefully consider whether export permits are required in connection with the carrying on of the Canadian business and determine whether the Canadian business has obtained all of the required permits.

The analysis should not end there. If a Canadian defence sector business does not have export control permits in place, acquiring parties should understand why this is (whether, for example, the company does not have export business or relies on a specific exclusion), and

determine whether this aligns with commercial objectives moving forward.

> Companies operating in the defence sector should have particular regard to supply chain diligence and compliance, which can be a significant source of risk.

Canadian businesses that examine, possess or transfer goods, technology or technical know-how that is controlled under Canada's *Defence Production Act* are required to register in Canada's CGP, a program administered by Public Services and Procurement Canada. Registered parties are required to adhere to various conditions of registration. The program was established to promote regulatory alignment between Canada and the United States; more specifically, registering with the CGP, and adhering to the conditions of that registration, allows Canadian defence contractors to transfer many U.S.-origin defence articles (controlled under the *International Traffic in Arms Regulations* (ITAR)) into Canada without a separate ITAR license.[29] Given the historical importance of the U.S. market to the Canadian defence sector, this exemption has been critical for Canadian industry.

Where an investor acquires 20% or greater control of a registered entity, notification must be provided to the Controlled Goods Program Directorate. The investor must satisfy the Program's eligibility requirements in order for the Canadian entity to maintain its registration. Foreign ownership may complicate registration, particularly where the acquiring entity is associated with a state that is not a close defence ally of Canada. Parties acquiring or investing in entities registered with the CGP — either directly or indirectly — should familiarize themselves with these eligibility requirements and conduct diligence to ensure that the registered entity (1) has a valid registration and (2) has met the requirements of that registration.

Sanctions

While not specific to the defence sector, businesses looking to invest in the Canadian defence sector should be mindful of the sanctions profile of the Canadian business. Of particular relevance in this sector, Canada maintains arms embargoes and controls on other forms of defence technologies both in accordance with multilateral commitments and under its autonomous sanctions regime. Canadian defence companies — like all businesses in Canada, as well as Canadians abroad — are required to ensure that their business activities fully comply with Canadian sanctions. This is particularly true of foreign acquirors, who may not be familiar with the Canadian sanctions regime; importantly, while Canada does commonly enact sanctions in concert with its allies (such as the United States and the European Union), there are notable differences.

An acquiror must be prepared to assume responsibility for the target's ongoing sanctions compliance obligations. Accordingly, as part of a diligence process, an acquiror should carefully assess the sanctions compliance profile of a Canadian defence sector target and understand the specific steps it takes to ensure compliance with applicable sanctions laws, including whether the target has any permits in place from Global Affairs Canada to conduct enumerated activities that would otherwise violate Canadian sanctions laws. In the context of a share purchase acquisition, the acquiror may assume liability for actions by the target that occurred prior to the acquisition, further enhancing the need for comprehensive diligence.

Compliance and enforcement risks

Defence companies may face unique and significant enforcement risks, owing to government contracting, complex supply chains and significant regulatory oversight.

Companies operating in the defence sector should have particular regard to supply chain diligence and compliance, which can be a significant source of risk. Canadian companies may face criminal liability for actions and omissions of representatives of the organization, which may include contractors. This risk is particularly acute in the context of increasingly complex supply chains and in sectors subject to significant government and regulatory oversight, including the defence industry.

Governments and enforcement authorities in recent years have increasingly focused on supply chain compliance issues. For instance, Canada's *Fighting Against Forced Labour and Child Labour in Supply Chains Act*,[30] in force since January 1, 2024, now requires companies meeting certain asset, revenue and employment thresholds to submit annual reports on steps taken each year to prevent or reduce the risk of forced labour or child labour in their supply chains. While this legislation is directed toward forced and child labour specifically, supply chain compliance issues may also extend where offences have been committed by contractors and suppliers such as economic and national security offences. The complexity of supply chains in the defence industry and accompanying incremental risk make proper supply chain oversight crucial.

The defence sector also faces elevated risks insofar as companies convicted of certain significant offences may face prohibitions from government contracting pursuant to applicable debarment regimes. The Canadian government's Ineligibility and Suspension Policy[31] provides for mandatory and/or discretionary suspension or debarment/ineligibility of suppliers from contracting with the Canadian government following (among other things) conviction of certain designated offences, as well as breaches of the government's Code of Conduct for Procurement. Certain provincial and foreign governments maintain similar regimes. The risk of ineligibility or debarment from government contracting is a significant risk where insufficient controls are in place to ensure compliance by contractors and suppliers.

To guard against these risks, Canadian companies operating in the defence industry should maintain robust policies, procedures and internal controls governing compliance matters, both within the organization and across their supply chains. Companies should also maintain compliance audit rights over contractors and suppliers. It is paramount that defence companies work only with reputable business partners following appropriate diligence processes, to ensure that they have a thorough understanding of who they are doing business with and that compliance expectations are communicated throughout their organization and supply chain.

Conclusion

Canada's defence sector is at an inflection point. Higher NATO-related spending, procurement reform and a stronger emphasis on sovereign industrial capacity are reshaping the market and opening meaningful M&A opportunities across the sector.

For buyers, the core takeaway is clear: commercial opportunity and regulatory complexity are rising in parallel. The most attractive targets are likely to be businesses with differentiated technology, procurement access and strategic relevance to Canada's domestic defence priorities. But successful execution will depend on addressing national security, procurement, clearance, export control, sanctions and compliance issues early enough to price risk accurately, structure around obstacles and preserve deal certainty.

[1] "Canada achieves the 2% of gross domestic product defence spending benchmark," Government of Canada, Department of National Defence (2% GDP).

[2] "Minister McGuinty Announces Strategic Investments in Sovereign Space Launch," Government of Canada, Department of National Defence (March 16, 2026) (Spaceport).

[3] 2% GDP.

[4] 2% GDP.

[5] "Prime Minister Carney launches Canada's first Defence Industrial Strategy," Prime Minister of Canada (February 17, 2026) (DIA/DIS Launch).

[6] DIA/DIS Launch.

[7] DIA/DIS Launch.

[8] Spaceport.

[9] Spaceport.

[10] Spaceport.

[11] "NATO wants to build a state-of-the-art satellite ground station in Canada," *The Logic* (May 15, 2026).

[12] "BDC boosts Defence Platform up to $6B after providing $92M in financing since late December, names StrongNorth Fund leader," Business Development Bank of Canada (March 12, 2026) (BDC).

[13] BDC.

[14] "Canada Hosts Charter Negotiations for New Allied Defence Financing Institution," Vanguard Canada (March 26, 2026) (DSRB).

[15] "Canada's biggest banks get into defence after years of avoiding military financing," *The Logic* (March 30, 2026); "Canada welcomes progress towards the establishment of the Defence, Security and Resilience Bank and hosting its headquarters," Department of Finance Canada (April 29, 2026).

[16] DSRB.

[17] "Canada hosts partners to advance establishment of the Defence, Security and Resilience Bank," Department of Finance Canada, March 23, 2026) (DSRB – Dept. of Finance Release).

[18] DSRB.

[19] "Private equity piles into defense as arms race gathers pace," *Dealspeak North America* (Tom Cane, Rachel Stone, Richard Tekneci and Akshaya Hari) (Dealspeak).

[20] Dealspeak.

[21] "2026 Canadian M&A outlook," PWC (December 9, 2025) (PWC).

[22] PwC's 2026 Canadian M&A outlook notes that local deals account for half of all M&A activity in Canada and are expected to continue anchoring the market through 2026.

[23] "How to make a succession plan," Business Development Bank of Canada (September 23, 2025).

[24] The CCSPA is Part 2 of Canada's cybersecurity legislation originally introduced as Bill C-26 and later reintroduced as Bill C-8.

[25] The CGP operates under Canada's *Defence Production Act* and is administered by Public Services and Procurement Canada. See "Controlled goods: Examining, possessing or transferring," Government of Canada.

[26] R.S.C., 1985, c. 28 (1st Supp.).

[27] "Digital Sovereignty: A Framework to improve digital readiness of the Government of Canada," Government of Canada.

[28] *National Security Review of Investments Modernization Act* (Bill C-34), Parliament of Canada.

[29] For more information on the ITAR exemption and the establishment of the CGP, see "Key events that shaped the Controlled Goods Program," Government of Canada.

[30] *Fighting Against Forced Labour and Child Labour in Supply Chains Act* (S.C. 2023, c. 9).

[31] *Ineligibility and Suspension Policy* (updated as of May 31, 2024).