Canadian Chamber of Commerce
Chambre de Commerce du Canada

Because Business Matters.
Parce que les affaires comptent.

October 12, 2021

Office of the Deputy Assistant Secretary of Defense for Industrial Policy
United States Department of Defense
Washington, D.C.

**RE: Federal Register Notice of Request for Written Comments in Support of the Department of Defense's One-Year Response to Executive Order 14017, "America's Supply Chains"
Docket Number: DoD-2021-OS-0100**

Thank you for the opportunity to comment on the Department of Defense's work related to this supply chain review. The Canadian Chamber of Commerce is the country's largest business association, representing companies of all sizes in all sectors and regions across the country.

Since the Ogdensburg Agreement of 1940, the United States and Canada have developed an integrated approach to continental defence, reinforced with the creation of the North American Aerospace Defense Command (NORAD) in 1957. In addition to this continental defence has been the integration of the defence industrial bases between the two countries. This includes binational agreements, such as the Defence Production Sharing Arrangement (DPSA) and the Defence Development Sharing Agreement (DDSA) and unilateral U.S. actions like the National Technological Industrial Base (NTIB) and Defense Federal Acquisition Regulations, which treat Canadian companies as legally equivalent to American companies.

These continental security and industrial arrangements have grown under successive U.S. Administrations and Congresses. The Canadian Chamber's members welcome the commitment by the President in his remarks on February 24, 2021 that the United States government intends to work "more closely with our trusted friends and partners, nations that share our values, so that our supply chains can't be used against us as leverage."

The Canadian Chamber wishes to offer its comments under the following questions posed in the Federal Register notice.

Question 3. How does the federal government effectively mitigate supply chain risks?

Defence procurement practices have a significant degree of flexibility to not be subject to trade agreement disciplines due to national security exemptions. This makes procurement a tool that governments can use to incentivize and build out essential supply chains, which in turn will reduce the likelihood of gaps in critical capabilities that could be injurious to national security. Given our unique geographic and trade realities, Canadian and American national security interests are inextricably linked.

NORAD will remain the bedrock of continental defence and given the large financial contributions that both governments will make, it is critical to ensure that we see a return on investment by utilizing, and strengthening, critical supply chain capabilities. The United States and Canadian governments should launch a public industry consultation component to NORAD modernization whereby American and Canadian companies contribute their views and inform the government of their relevant capabilities. This work with the United States should include a binational NORAD technology road-mapping exercise to better position industry to meet the capability requirements of a modernized NORAD.

There is also significant potential as it relates to critical minerals. In the 100 day supply chain reviews released this past June, the DoD report identified over 20 critical mineral products where Canada can play a role meeting American defence needs. The United States Government should work with the Government of Canada to explore how to adjust their procurement policies to require critical mineral inputs, when possible, to be sourced from within North America. Where inputs are not sourced from within North America, strict certification requirements should be required to ensure critical minerals are not produced with forced labour as a pre-condition for securing government contracts. These measures will bolster demand for North American sourced critical minerals, which in turn will enhance the resiliency of critical mineral supply chains on the continent.

There is also a need to ensure Canada and the United States have a modernized framework for our unique defence industrial relationship that responds to the needs of the current security environment. To deliver this, the two governments should develop a strategic statement of intent, in consultation with industry, that includes reviewing the effectiveness of the DPSA and the DDSA, with a view to strengthening these foundational arrangements.

Outside of these bilateral arrangements, the DoD should also commit to working with industry under the NTIB framework to ensure there are forums for providing regular input that identify a discrete list of priorities where action can be taken to strengthen the continental defence industrial base.

Cutting across all the aforementioned areas should also be the inclusion of facilitating exchanges in emerging and disruptive technologies to ensure continued interoperability and advanced military capabilities in the current, and future, security environment.

Question 5 – What can the government do differently to successfully implement industrial base cybersecurity processes or protocols, attract skilled labor, implement standards, and incentivize the adoption of manufacturing technology?

The Canadian defence sector is closely tracking developments related to DoD's Cybersecurity Maturity Model Certification (CMMC) given the critical importance of it for doing business with the DoD. However, Canadian firms need non-discriminatory access to services offered to American firms under the auspices of the existing CMMC Accreditation Body. If possible, Canadian firms should be allowed to offer these services by undergoing the same requirements as American firms. This would serve two purposes. It would enable the DoD continued access to high-quality Canadian products that benefit the DoD's cybersecurity objectives. Additionally, it would reinforce efforts in Canada to have CMMC adopted by reference in Canada, which in turn would create benefits for continental cybersecurity and the protection of critical infrastructure.

The United States government has already taken important strides to secure the defense supply chain. This includes Executive Order 14017 and Executive Order 14028. In a digitally connected world, where our supply chains are more interdependent and vulnerable to cyber attacks than ever before, more attention needs to be placed on safeguarding the defense software supply chain.

The DoD could undertake several actions in this regard:

- **Adopt a Secure Software Development Life Cycle approach to mitigate software supply chain risk**. It is critical that DoD align its procurement policies with secure software development practices that consider security throughout the lifecycle of software from design, development, production, maintenance, and decommissioning. Adopting an approach in line with NIST's draft Secure Software Development Framework will help DoD mitigate the risk of software vulnerabilities in its platforms. This is critical because NIST's National Vulnerability Database, and the threat landscape writ large, are constantly evolving as new vulnerabilities and exposure information come to light. The DOD should employ software and software security measures that are capable of monitoring changes to Common Vulnerabilities and Exposures (CVEs) associated with the embedded software in military assets throughout their lifecycle, which could last 20-30 years. To facilitate this, it is essential that the DoD consider a software update mechanism for long-term in-field products. With type approval requirements often costly and time-consuming, there is a risk that in-field platforms could go years without an update. It is essential the DoD consider options to facilitate software updates and security patches in a way that strengthens the security posture of platforms that are in the mid- or end-of their lifecycles.

- **Leverage third party professional service teams and subject matter experts to undertake risk assessments and perform penetration tests.** Given that military systems can be deployed in contexts with intermittent or no connectivity to the internet, it is essential that technical experts who understand the limitations of hardware and software routinely audit systems for CVEs, Common Weaknesses Enumeration (CWE) and the software bill of materials. Given the need for a lifecycle approach, a continuous monitoring of supply chain security and platform security is essential. The use of independent third parties can ensure that assessments are undertaken in a transparent manner and according to industry best-practice.

- **Protect defense IT and Operational Technology (OT) systems with AI-driven endpoint security tools that can prevent malware from deploying**. Defense systems have evolved into sophisticated, multi-layered digital software systems that contain millions of lines of code and connect to thousands of devices and external networks via a variety of classified and unclassified communication technologies. As the complexity and scale of software in defense systems grow, so does the attack surface. A cyberattack that exploits software vulnerabilities could have devastating national security consequences. To prevent such attacks, DoD should adopt AI/ML based anomaly detection and cybersecurity tools that have been independently proven to prevent malware from executing. This means moving away from signature-based tools and adopting next generation AI/ML driven cybersecurity tools that have been developed through long-term training on massive and relevant data sets to dynamically predict and prevent cyber breaches. This could be combined with other methods such as a Zero Trust Architecture and Unified Endpoint Security tools that provide a platform approach to prevent, detect and respond to cyber threats and attacks 24x7.

Thank you for the consideration of the Canadian Chamber's inputs. We would be glad to provide further information for this review process.

Sincerely,

Mark Agnew
Senior Vice President, Policy and Government Relations
Canadian Chamber of Commerce
magnew@chamber.ca