Public Comment Submission from the Canadian Association of Defence and Security Industries

Re: Cybersecurity Maturity Model Certification Program
Docket number DoD–2023–OS–0063
Regulatory Identifier Number (RIN) 0790–AL49

February 24, 2024

These comments are submitted by the Canadian Association of Defence and Security Industries (CADSI), which represents over 700 defence, cyber and security companies that comprise the Canadian defence industrial base (DIB). Given the integrated Canada-U.S. defence industrial base, the majority of these companies will be impacted by the final Rule on the Cybersecurity Maturity Model Certification (CMMC) Program. We look forward to working with the U.S. Department of Defense (DoD) and the Government of Canada (GC) to ensure that CMMC does not become a barrier to bilateral defence trade.

An Integrated Bilateral Defence Industrial Base

Canada and the United States share a deep and longstanding bilateral defence relationship that spans the full spectrum of cooperation, from shared defence of the continent to combined operations and exercises around the globe; commitments to collective objectives through NORAD, NATO, and the Five-Eyes; and intelligence sharing. Canada has long been a trusted defence and security partner of the U.S. and is explicitly recognized by the U.S. as an essential partner in the shared national security of North America.

Canada-U.S. DIB cooperation ensures our security of supply, helps avoid the duplication of efforts, increases interoperability, and provides surge production capacity – all which in turn contribute to our respective and collective national security. In times of war and national emergencies, Canada has repeatedly been a secure and trusted source of supply and surge capacity. Canada-U.S. supply chain cooperation, security and resiliency is paramount so that our integrated industrial base can continue to thrive to the benefit of our workers on both sides of the border. For this reason, CADSI supports in principle the objectives of CMMC to increase the cybersecurity and resiliency of the DIB.

Our industrial supply chains in North America are deeply integrated, efficient and long-standing. Canadian firms supply the U.S. with crucial, niche systems and technologies that support broader U.S. objectives. Since the Canadian (DIB)is heavily U.S.-owned, the profits and technology benefits from these companies create jobs and spread innovation on both sides of the border. In 2020, 49% of all Canadian defence exports, and 72.5% of cybersecurity industry exports, went to U.S. The defence sector's close integration helps us compete together on the global stage, but the incoming CMMC requirements will impact Canadian firms more than those of any other country.

Recommendations

One unique impact of CMMC is that Canadian firms will possess data that is CUI, FCI, Canadian Controlled Goods Program, and ITAR data. Each of these information designations have overlapping regulatory, policy and security requirements that can cause complications or contradictions for their effective handling in a secure and compliant manner, particularly when that data is stored, accessed or manipulated in the cloud. Some questions on how best to remain compliant or impediments to the

300-251 Laurier Avenue West
Ottawa, ON K1P 5J6
defenceandsecurity.ca
T: +1 613.235.5337
F: +1 613.235.0784
cadsi@defenceandsecurity.ca

data's practical use may arise over time and CADSI would welcome the opportunity to continue to work with DoD, CMMC AB, GC and Canadian industry to resolve in a timely fashion any unintended consequences that impede the integrated DIB.

It is in the spirit of this longstanding relationship and historical integration that CADSI submits the following comments and recommendations.

- DoD officials have said to Canadian industry that, in principle, Canadian firms as members of an integrated DIB should be able to complete the assessment process at all levels and thereby come into compliance; and, as CMMC is implemented in practice, we urge DoD to continue to work with GC and Canadian industry to remove or mitigate any barriers, roadblocks or impediments that uniquely or disparately impact Canadian firms seeking to comply.
    - The U.S. should ensure that any U.S. citizenship requirements include Canadians in lists of eligibly entities in the CMMC CyberAB Marketplace, across all disciplines including becoming CMMC Third Party Assessor Organizations (C3PA0s). Canadian firms wish to undergo the process (at level 2) to become C3PA0s in order to accredit Canadian defence contractors, regardless of the GC proceeding with its own equivalent cybersecurity standard.

- Recognizing the shared threat landscape that Canadian and U.S. defence firms face, CADSI supports the notion of increasing our collective cybersecurity posture and is supporting the Canadian government in its efforts to implement the Canadian Program for Cyber Security Certification (CP-CSC), a Canadian program nearly identical to CMMC.
    - We thank the U.S. for the cooperation to date and encourage both countries to continue to work toward mutual recognition and reciprocity between CMMC and CP-CSC.

- Security as a Service: Many small and medium enterprises (SMEs) on both sides of the border will need to rely on Cloud Service Providers (CSPs) and managed service providers to implement proper cybersecurity requirements in a cost-effective manner.
    - Given that Canada does not have a GovCloud or FedRAMP equivalent program, the U.S. and Canada should work together to advise on how Canadian companies that hold CUI, FCI, Controlled Goods and ITAR information can do so in the cloud effectively, and whether that data must reside in accredited U.S.-based CSPs or whether Canadian-based CSPs can be properly accredited to hold such data, assuming the appropriate export controls have been secured.

- The Standards Council of Canada is an internationally accredited, peer reviewed body that could act as a sister accreditation body to that of the CyberAB.
    - Given the hundreds of thousands of U.S. companies who will need to be CMMC certified, the U.S. should consider granting accreditation body standing to the Standards Council of Canda, which could then act as surge capacity and grant U.S. CMMC accreditations to Canadian-based C3PA0s, in addition to Canadian CP-CSC accreditations.

Our defence relationship and integrated supply chains are essential for the stability and security of both of our nations and Canada looks forward to continued cooperation as a secure and reliable trading partner for the U.S.

Thank you for the opportunity to comment on the incoming CMMC program.

300-251 Laurier Avenue West
Ottawa, ON K1P 5J6
defenceandsecurity.ca

T: +1 613.235.5337
F: +1 613.235.0784
cadsi@defenceandsecurity.ca