TRIPLE HELIX

Nine Actionable Decisions for the Prime Minister to Best Posture Defence

by VAdm (Ret'd) Ron Lloyd

August 2025

POLICY PERSPECTIVE

NINE ACTIONABLE DECISIONS FOR THE PRIME MINISTER TO BEST POSTURE DEFENCE

by VAdm (ret'd) Ron Lloyd

August 2025

Prepared for Triple Helix
Suite 200, 8 York Street, Ottawa, ON K1N 5S6 Canada
www.cgai.ca/triple_helix

ISBN: 978-1-77397-351-7

In light of the fact that Canada's previous relationship with the United States is over, Prime Minister Carney has made several recent announcements that aim to set the foundation for Canada's success strategically. The new EU-Canada Strategic Partnership of the Future and the EU-Canada Security and Defence Partnership announcements are arguably cornerstones of that foundation. Canada's commitment to meet the NATO defence spending target of 5% of annual GDP by 2035 is wind in these sails.

Cutting horizontally across these announcements are leveraging modern digital technologies, improving Canada's defence posture and improving government procurement broadly and defence procurement specifically. Whereas these announcements provide a spirit of optimism about resolving longstanding issues in Defence, such as digital and procurement, our history portends otherwise.

In the last 20 years, there has been a war, three much heralded Defence Policy updates, and a pandemic. And yet, Canadian Defence continues to fall behind our allies, partners and adversaries. The reason for this is quite simple: A flawed "small p" policy foundation. Whereas a "capital P" policy articulates a government's intent, such as meeting NATO's 5% spending target, "small p" policies are hundreds of non-legislative instruments, such as policies, directives, guidelines, Information Technology Security Guidance (ITSGs), and tools within which departments must deliver their mandates to realize the capital P Policy objectives.

In this paper, I will identify nine actionable decisions that will best enable the realization of the "capital P" policy outcomes articulated by the Prime Minister. All the decisions will directly affect Defence, with some accruing benefits across all government departments and agencies. I use the term "actionable" because the decisions do not require legislation and the compelling evidence that once the decisions are implemented, they immediately begin to mitigate real-world risks. These real-world risks include a lack of defence interoperability with allies and partners, poor posturing of the Canadian Armed Forces (CAF) to prevail in conflict, and the inability to provide modern digital services to the CAF or Canadian citizens.

Will there be risks associated with implementing the decisions and transitioning from the status quo "small p" policy paradigm? Of course, but they will not be real-world risks. Rather, they will be policy, process, transition and implementation risks. As the Prime Minister acknowledges in his mandate letter, "We must meet a series of unprecedented challenges with both a disciplined focus on core priorities and new approaches to governing." The following nine decisions are recommended in that spirit.

Decision #1 – Wait to announce any organizational changes affecting Defence until the policy foundation has been amended to enable a form follows function outcome.

If you want it bad, you will get it bad. Building new structures on a flawed foundation is not what right looks like. The successful organization changes that I have been associated with are those where form follows function. I have witnessed too many organizational changes occurring without an understanding of the root cause that warranted the change or were viewed as politically expedient solutions.

Based on my experience in Defence, any organizational changes, whether internal or external, will require significant leadership and staff engagement in addition to a restructuring of associated authorities, responsibilities and accountabilities (ARAs). The effort and time required should not be underestimated. This is not to say that organizational changes won't eventually be required. However, as appealing as it may be to embark upon organization changes to demonstrate government action, doing so in advance of understanding the implications of a number of related announcements may be premature.

I would suggest that other than CAF specific organizational change, broader Defence organizational change in advance of understanding the implications of a new Defence Enterprise Readiness Platform (ERP), leveraging modern digital tools such as agentic AI, and understanding the new ARAs associated with a reset of the "small p" policy paradigm, will posture Defence for today when we need to be posturing Defence for tomorrow.

Organizational change on the scale of standing up a defence procurement agency affecting multiple departments accrues even greater real-world risk. Many of the "small p" policies that adversely impact defence procurement are not within the ARAs of the departments likely to be implicated. As such, there is a high probability that once the new organization is stood up, the intended outcomes envisioned by the government will still not be realized. A rearranging of the deck chairs on the Titanic if you will. The scope and scale of the changes required to deliver better defence procurement outcomes can only be fully appreciated in the context of the following decisions.

Decision #2 – Adopt a new security classification framework of official (official sensitive), secret and top secret.

40 years ago, Canada adopted a new security classification framework that was, and remains, unique amongst all our allies and partners. Whereas other nations assess the level of injury associated with the compromise of personal information, such as personal appraisals and tax information, as less than the compromise of classified information that is in the national interest, such as troop movements that could result in life-or-death implications, Canada did not. The unintended consequences of this framework are that Canada's physical and digital security baselines are excessive and not aligned with our allies and partners.

This is not to say that personal information should not be appropriately secured, as it must be in accordance with legislation. However, the level of security needs to be proportional to the level of injury associated with the compromise and treated accordingly. Just like all our allies and partners do. As much as there are those that would like to believe that overclassifying information is a good thing, it is not.

Overclassification in government leads to excessive security clearance requirements, significant additional security costs, reinforces a culture of risk aversion, undermines the overall security posture and adversely affects interoperability with our allies. Overclassification has become so problematic in the public service that in 2023 the Chief Information Officer for the Government of Canada put out a directive to all departments that citizen data should not be classified secret.

Adopting a new security classification framework of official (official sensitive), secret and top secret will enable the government to recalibrate risk tolerance in the public service, and the following advantages will also accrue:

a) a tangible reorientation to NATO as the UK has the same framework,

b) savings in hundreds of millions of dollars if not billions by government and industry when secret is appropriately applied,

c) improved interoperability and integration with our partners and allies,

d) greater transparency of government data for Canadians, and

e) an improved national and cyber security posture for Canada.

As the security classification framework informs almost all processes in modern government, changing it is the necessary first step to reset the public service risk management culture.

Decision #3 – Direct the amendment of the thousands of affected small "p policies" to reflect the PM's intent of focusing on results and not process and to recalibrate the risk tolerance of the public service.

Once the security classification framework has been amended there will be a requirement to amend the hundreds of "small p" policies horizontally across central agencies and the thousands of "small p" policies vertically across all government departments and agencies. The opportunities to enable a more permissive/risk tolerant government posture are as significant as the level of effort that will be required to implement the changes associated with a new security classification framework.

Of the many "small p" policies that need to be amended or rescinded two are worthy of specific mention. Just as the security classification framework informs almost all modern government

processes so too does risk management and digital security. The Harmonized Threat and Risk Assessment (TRA) Methodology (2007) is out of date and fosters a culture of overclassification and risk avoidance. As such, it should be rescinded immediately as it is assessed that other policies provide sufficient direction and guidance to departments and agencies.

With respect to digital security, today, there is a patchwork of policies, guidelines, directives, ITSGs, Information Technology Security Professional (ITSPs), and playbooks that Defence, as well as all government departments, must take into consideration when establishing their cyber security postures. It is not helpful that many of the documents are outdated and do not reflect modern best practices or technologies. To further exacerbate the situation, the documents are promulgated by different central agencies which introduces a complicated web of overlapping and confusing ARAs.

In order to address this shortcoming, the Canadian Centre for Cyber Security should be directed to consolidate the plethora of digital security "small p" policies into a single document. The consolidation of digital security direction will make it easier for departments to understand and implement the recommended digital security baselines. In addition, it will also better enable annual amendments to Canada's cyber security posture based on the ever-changing cyber landscape, a best practice used by several of our allies and partners.

Most importantly, this consolidation would enable the rescinding of IT security risk management: A lifecycle approach ITSG-33 (2012). As the principal document that enables compliance with "the overall risk management strategy and objectives established by TBS, assurance that all aspects of IT security are addressed in an efficient manner, and predictability and cost-effectiveness with regards to IT security risk management" it is problematic for several reasons. First, the digital security baselines directed, and the risk management processes are excessive because of Canada's unique security classification framework and TRA-1. Secondly, ITSG-33 does not reference cloud, artificial intelligence, data centric security and zero trust because it was issued over a decade ago. If you want to understand why departments are failing to leverage modern digital best practices read ITSG-33.

Decision #4 – Empower Defence Digitally by removing their dependency on SSC as directed in Order in Council 2015-1071.

Success in the battlespace of the 21st Century will be determined by a military's ability to leverage modern digital technologies at speed and scale. The Canadian Armed Forces continues to fall behind our allies, partners and adversaries which jeopardizes our credibility within the alliance. It is unrealistic for the Deputy Minister of Defence and the Chief of the Defence Staff to be responsible for mitigating national defence and security risks when they do not control the digital levers required to be successful.

A decade ago, when Order in Council 2015-1071 defined what services Shared Services Canada was to provide departments in accordance with *the Shared Services Canada Act*, I am sure that it

made sense. However, as technology has so rapidly evolved and we find ourselves in a vastly different digital world characterized by cloud, zero trust, data centric security, artificial intelligence, and quantum, this Order is undermining Defence's ability to exploit these technologies at pace and scale.

Having served as the first Chief Data Officer for Defence while concurrently commanding the Royal Canadian Navy, I was provided remarkable insights into the CAF's dependencies on SSC. Six years later, currently serving commanders characterize the CAF's inability to keep pace with our allies and partners as jeopardizing our interoperability, credibility and ability to contribute meaningfully to operations. I am convinced that the CAF's dependencies on SSC undermines the CAF's digital readiness and ultimately the combat readiness of the force. In the geostrategic environment in which we expect the CAF to fight tonight, be day one interoperable with allies and partners, and prevail over our adversaries, they need to be digitally agile. They are not.

Decision #5 – Direct an independent third party to conduct an end-to end mapping of the "as is" defence procurement process from the tactical (departmental) to the strategic (central agencies). Once mapped, direct options to be developed to reduce the procurement approval timelines by 50% and 75% and provide them to the Prime Minister.

In my experience, the level of and types of risk an executive is prepared to accept is seldom truly appreciated by their subordinate leaders and their respective staffs regardless of how much it is communicated. The only way to truly understand the risks associated with streamlining a process, training requirements, or citizen centric service requirements across multiple empowered stakeholders is to direct an end-to-end mapping of the "as is" process. The end-to-end mapping that I am referring to is not simply Defence or PSPC, but it implicates all processes from the tactical to the strategic.

Whereas one would expect Treasury Board to have a strategic role in identifying procurement issues and to ensure departments are spending in accordance with government's intended objectives they do far more than that. For example, Treasury Board directs the use of the Project Complexity and Risk Assessment tool to be used by departments for procurement. Unfortunately, the way the tool has been designed it codifies almost all digital procurements as evolutionary or transformational requiring additional governance and approvals. Do we truly understand the implications of all of these TB directed requirements?

The approval process within Treasury Board itself could also be further streamlined. Similarly, why must a department seek expenditure authority, if they have the resources required to sign a contract that has already been approved by Cabinet and Treasury Board? It is unrealistic to believe that you can exponentially increase defence procurement throughput if Treasury Board does not change their internal processes.

Closely linked to Treasury Board approval is the requirement to seek policy coverage through a memorandum to cabinet for defence procurements. Since 2017, almost all Defence procurements are directed in Defence Policy. For those that are not, all deputy heads are to submit an investment plan for the upcoming five years, including a list of planned and approved projects and programmes of $2.5 million or greater. If Defence procurements are already articulated in Policy and TBS approves departmental investment plans, should that not represent sufficient government oversight? If there is doubt with respect to whether a project requires policy coverage, I would suggest that it should be a conversation between the President of Treasury Board, the Minister of the Department, and if required, the Prime Minister.

Defence also has numerous internal processes that would need to be mapped. The Procurement Administration Manual and the Project Approval Directive, both internal documents to Defence, as well as additional processes such as the Independent Review Panel for Defence Acquisition (IRPDA) are very process intensive. Suffice it to say that with increased delegated authorities, less central agency directed process, and less central agency involvement there are significant opportunities to amend internal defence "small p" policies while still ensuring proper oversight of taxpayer dollars.

PSPC will also be implicated because of their extensive involvement in defence procurement. In addition, as Defence may still wish to procure services through SSC, they should also be included in the "as is" mapping.

Once the "as is" process is mapped, I believe that there will be significant opportunities to streamline the process by at least half. The options to identify a 75% reduction may not be realizable but at least it will enable a conversation with government on how much and what types of risk they are prepared to assume. The reason for briefing the options to the Prime Minister is because of the overlapping ARAs shared between ministers which often result in impasses which are intractable for staff to resolve. For something as wickedly complex as Defence Procurement this should be step one.

In today's world, the nations that operate at the speed of trust are more likely to prevail in crisis or conflict. Individuals operate at the speed of trust. Process does not. If we are to realize the PM's vision of delivering results, our elected ministers and most senior executives in government need to be empowered to do so. Currently they are not. The mapping of the "as is" defence procurement process and the identification of a 50% and 75% reduction in timelines would invariably enable the delegation of the appropriate ARAs to achieve the PM's intended outcomes.

Decision #6 – With a comprehensive understanding of the modernized policy foundation make the organizational changes required.

Canada has been talking about fixing defence and government procurement for decades. Waiting approximately one year to ensure a solid "small p" policy foundation is put in place upon which to build new structures, if required, will be time exceptionally well spent.

Decision #7– Direct Defence to decentralize ADM HR Civ and ADM IE and re-empower the service, institutional and operational commanders.

As the departmental lead for the Deficit Reduction Action Plan (DRAP), I was in the room when the DRAP recommendations were considered by Defence leadership prior to recommending them to government. I can attest to the fact that the economies of centralization that were envisioned when the decisions were made were not realized. I can say this authoritatively having had to live with implications of these decisions as the Commander of the RCN. The centralization of these authorities may have made sense in a time of austerity, but they will not serve Defence well, if they ever did, in a time of growing the Defence enterprise.

Decision #8 – Direct the development of an integrated implementation plan that will ensure the appropriate sequencing and phasing of the aforementioned decisions and implement a governance structure that reports progress to the Prime Minister monthly.

You get what you inspect, not what you expect. As much as I have every confidence in the leadership of the departments implicated in the decisions, the complexity of implementing one of decisions, let alone all of them, in an environment of overlapping ARAs should not be underestimated. Couple this complexity with the fact that all of the executives have important day jobs which often results in the tyranny of the urgent trumping the important and the probability of success is further reduced.

To ensure government success a rigorous adherence to Plan, Execute, Measure and Adjust (PEMA) will be critical. The phasing and sequencing of these decisions will need to be articulated in a comprehensive and integrated implementation plan. As the plan is implemented many "small p" policy barriers and obstacles to its realization will be identified and need to be resolved. In order to maintain momentum, it will be critical to ensure that there is a governance body sufficiently empowered to address these challenges in a timely manner. As the plan is adjusted it needs to continue to be aligned with the government's intent and not the status quo. PEMA will underpin the realization of this once in a generation opportunity articulated by the PM.

Decision #9 – Accept the transition risk.

I am always amazed at how the characterization of transition, policy and implementation risk to a better posture precludes an organization's transition and perpetuates the status quo. It must be remembered that there are two sides to the risk management coin. On the one side risk identification and mitigation and on the other side leveraging innovation and opportunity. The government is placing a big bet that innovation and opportunity will be the vehicle by which Canada will emerge from this crisis. Unfortunately, the current "small p" policy paradigm will

contextualize this big bet as too risky. I lived this construct while serving and witness it firsthand working in industry today.

I am confident that the current crisis will generate some success in the short term. These successes will be a result of leveraging exceptional means to bypass processes or to over pressurize the system. Neither of which will be sustainable in the long term to accomplish the breadth and depth of the current government's mandate. I would suggest that these short-term successes will be false positives, just like those heralded during the Afghanistan War and the Pandemic. It is unrealistic to expect otherwise. The status quo "small p" policy paradigm is a powerful thing and will continue to remain a significant obstruction to realizing the government's meaningful outcomes.

As the PM noted in his mandate letter "Canada's challenges are not small, but we can more than meet them with vigour and a constructive approach. That is how Canadians have built the best country in the world. That is how we will build it to be even better." These nine actionable decisions are provided for the government's consideration in the spirit of a constructive approach to addressing our nation's defence and security challenges.

About the Author

Vice-Admiral (Ret'd) *Ron Lloyd was the 35th Commander of the Royal Canadian Navy from 2016-2019. During that time, he was also "double hatted" as the acting Vice Chief of the Defence Staff for almost half a year and as the first Chief Data Officer for the Department of National Defence and Canadian Armed Forces for a full year.*

During his 38-year career in the RCN, he was privileged to have commanded HMCS CHARLOTTETOWN, HMCS ALGONQUIN, the PACIFIC Fleet and the ATLANTIC fleet. He has extensive operational experience having deployed on numerous occasions globally.

Lloyd has over a decade of experience at National Defence Headquarters having also served as the Deputy Commander of the RCN, the Chief of Force Development for the Canadian Armed Forces, the Director General of Force Development for the RCN and Executive Assistant to the Commander of the RCN.

Lloyd holds a Bachelor of Arts in Military and Strategic Studies from Royal Roads Military College (1985) and a Master of Arts in War Studies from the Royal Military College (2004). He is a graduate of both the Command and Staff Course and the National Security Studies Course at the Canadian Forces College in Toronto. He has also attended the HARVARD Kennedy School, Executive Education, Senior Executives in National and International Security.

Today, as Principal of Leadmark Ventures, he shares his experience in leadership, strategic planning and digital transformation with organizations committed to providing innovative solutions that enhance public sector performance in defence and non- defence related activities.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.