CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Canada's Security Classification Framework: The Biggest Impediment to Realizing Our Digital Ambition

by Ron Lloyd

June 2024

POLICY PERSPECTIVE

CANADA'S SECURITY CLASSIFICATION FRAMEWORK: THE BIGGEST IMPEDIMENT TO REALIZING OUR DIGITAL AMBITION

by Ron Lloyd

June 2024

CANADIAN GLOBAL AFFAIRS INSTITUTE
INSTITUT CANADIEN DES AFFAIRES MONDIALES

Prepared for the Canadian Global Affairs Institute
Suite 2720, 700 – 9th Avenue SW., Calgary, AB T2P 3V4
www.cgai.ca

ISBN: 978-1-77397-304-3

Canada's Security Classification Framework: The Biggest Impediment to Realizing Our Digital Ambition

In 2022, the Government of Canada, under the leadership of the Chief Information Officer of Canada, published Digital Ambition 2022.[1] The document outlines a vision for the government of Canada to leverage modern digital technologies to transition the nation's digital enterprise to 21st century standards. In 2023, an update was provided that noted that while progress had been made, "there is much more work to be done". Despite the best efforts and tremendous commitment of leadership, this vision will be a challenge to realize because of the security classification framework that Canada adopted over 40 years ago.

In the 1980s, when the classification framework was adopted, the only considerations for the security of digital data were physical. The classification of the data dictated whether the floppy disk, hard disk, laptop or USB was to be locked in a filing cabinet with a lock, a filing cabinet with a locking bar and lock, or a special filing cabinet with a Sargent and Greenleaf lock. Although it could be argued that the security classification framework made sense when it was originally implemented, the unfortunate reality is that it has become the biggest impediment to realizing Canada's Digital Ambition. Furthermore, the framework is responsible for the culture of over classification that permeates the public service and Defence, it precludes leveraging affordable industry standard security technologies that Canadians use every day, and it drives up the costs of providing digital services to Canadians. The current framework also adversely impacts procurement, the contract security program, and interoperability with our allies and partners. Suffice it to say that it is no longer fit for purpose, if it ever was.

Ensuring the safeguarding of personal data is exceptionally important in both the private and public sector. It is important, not only from the perspective of the individuals affected, but equally so, from an organization's reputational risk perspective. In all instances, the compromise of personal information is a lose/lose situation. In Canada, the legislation that determines the framework for how private-sector organizations collect, use, and disclose personal information in the course of for-profit commercial activities across Canada and the personal information of employees of federally regulated businesses is the Personal Information Protection and Electronic Documents Act (PIPEDA).[2] In the act personal information includes age, name, ID numbers, income, ethnic origin, blood type, evaluations, social status, employee files, loan records, medical records, opinions and credit records. For businesses subject to the act they must follow the 10 fair information principles to protect personal information. The relevant principle for the purposes of this paper is principle 7 – Safeguards. In accordance with PIPEDA, businesses are responsible to protect personal information "in a way that is appropriate to how sensitive it is" and "regardless of how it is stored, protect it against loss, theft or any unauthorized access, disclosure, copying, use or modification."[3] The act does not specify particular safeguards but places the onus on organizations to ensure personal information is adequately protected as technologies evolve and new risks emerge. The private sector continues to leverage modern and innovative digital

[1] https://www.canada.ca/en/government/system/digital-government/government-canada-digital-operations-strategic-plans/canada-digital-ambition.html#toc1
[2] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#
[3] https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/principles/p_safeguards/

solutions to provide better security, improved services, higher customer satisfaction, and more intuitive and convenient features while concurrently ensuring personal information is protected regardless of the type of device, the application or how the information is transmitted.

The challenge for government is that because of the security classification framework, they are significantly constrained in how they treat personal information. For example, if a Canadian citizen were to upload personal information that is not commonly found in the public domain to a digital application and then provide it to the Canadian government, that information would be given a security classification of Protected B. In accordance with government policy, the level of injury associated with the compromise of Protected B information is the same as that for the compromise of secret information. It is difficult to believe that personal information that Canadians share digitally in the private sector, if compromised, would have the same level of injury to the nation as the compromise of our nation's most closely held secrets. However, once that same information is provided to the Government of Canada that is how it is treated. The fact that none of our closest partners and allies have the same level of injury for two different security classifications substantiates the belief that the level of injury is considerably different. The implications in the 80s and early 90s weren't significant because everything was stored in a filing cabinet. Fast forward to today, because of the artificially high level of injury associated with Protected B information, it must be transmitted digitally using government infrastructure and with additional encryption. If the information needs to be communicated outside of government mailing and faxing are also permissible, just as it was in the 80s.

To understand how Canada got out of step with our allies, partners and industry we need to examine Canada's security classification framework. In so doing, it will also become evident that all that is required to address the issue are Treasury Board policy amendments. As easy as the solution is, there would still be a requirement for significant internal and external stakeholder engagement as well as a great deal of education and change management required before, during and after the adoption of a new security classification framework.

Security Classification Framework

In Canada, the current data classification framework is defined by the Directive on Security Management, Appendix J – Standard on Security Classification. Although the directive was updated in July 2019, the current classification framework was implemented in the 1980s. The current classification framework consists of two types of information: Classified information in the national interest and Protected information outside of the national interest. The greater the level of injury due to the unauthorized disclosure of the data, the higher the classification. All nations, other than Canada, recognize that the level of injury for the loss of classified information that is in the national interest, results in a greater level of injury than information that is not in the national interest. Further exacerbating the situation is that it assigns the same level of injury for two different security classifications. In Canada the level of injury is the same for Top Secret/Protected C, Secret/Protected B, and Confidential/Protected A as shown in figure 1.

Figure 1: Level of Injury from the Directive on Security Management - Appendix J: Standard on Security Categorization[4]

Level of injury	Classified information (National Interest*)	Protected information (Outside the National Interest*)
Grave injury	Top Secret	Protected C
Serious injury	Secret	Protected B
Limited or Moderate Injury	Confidential	Protected A

Examples of classified secret information in Canada are the tactics, techniques and procedures (TTPs) used by the Canadian Armed Forces to deal with military threats, intelligence on adversary capabilities, and foreign intelligence operations. Examples of Protected B information in Canada are personal records such as personnel evaluation reports, medical information and administrative reports. To put this in perspective, based on Canada's security classification framework the compromise of the disposition and readiness of our forces in Latvia and their associated plans and TTPs would result in the same level of injury to the nation than the compromise of personal or administrative data. This problem was recognized early after adoption of the new classification framework and the issue was "clarified" in the 290 page Harmonized Threat and Risk Assessment Methodology (TRA-1) policy document released in 1997 by the CSE/RCMP. The TRA-1 provides a more nuanced view as shown in figure 2.

Figure 2: The comparative injury level table found in TRA-1[5]

Comparative Injury Levels	Classified information	Protected information
Very High	Top Secret	--
High	Secret	Protected C
Medium	Confidential	Protected B
Low	(Restricted)	Protected A
Very Low	Unclassified	

[4] Directive on Security Management - Appendix J: Standard on Security Categorization- Canada.ca
[5] Microsoft Word - 2007-HTRAM-Eng-Word2002-classroom-1023.doc (cyber.gc.ca)

As a result of the TRA guidance and it informing security training since 1997, despite the higher level policy indicating Secret and Protected B having the same level of injury, the culture of the public service is more closely aligned with the level of injury of Confidential and Protected B being the same. The unfortunate reality is that there should not be the same level of injury for two different security classifications and there should be a clear delineation between the level of injury for the disclosure of classified information in the national interest of the nation and other data holdings. The uniqueness of Canada's security classification framework is evident when compared to our closest allies and partners in figure 3.

Figure 3: A comparison of the classification frameworks of Canada, U.K., Australia, and the U.S.

<table>
<tr><td colspan="2">Canada

Implemented – 1980s

Updated – 2019</td><td>U.K.

Implemented – 2014

Updated - 2023</td><td>Australia

Implemented – 2018

Updated – 2023</td><td>U.S.

Implemented – 1953

Updated – 2009</td></tr>
<tr><td>Top Secret</td><td>Protected C</td><td>Top Secret</td><td>Top Secret</td><td>Top Secret</td></tr>
<tr><td>Secret</td><td>Protected B</td><td>Secret</td><td>Secret</td><td>Secret</td></tr>
<tr><td rowspan="3">Confidential</td><td rowspan="3">Protected A</td><td rowspan="3">Official

* 90 per cent of U.K. Public Sector business is Official

* Official Sensitive is not a separate classification but a marking that can be used to denote information that if released would result in moderate damage

* For Public Release is a handling instruction that can be applied to Official</td><td>Protected</td><td>Confidential-

see note</td></tr>
<tr><td>Official

* Official Sensitive is a subset of Official</td><td rowspan="2">*The U.S. classification framework only applies to national security data. In some instances, departments will use handling requirements such as For Official Use Only for non-classified data</td></tr>
<tr><td>Unofficial</td></tr>
</table>

Note: The Office of the Director of National Intelligence indicated in 2017 that "Based on this analysis conducted of CONFIDENTIAL level protection, the decision was made to remove CONFIDENTIAL entirely from the Guide"[6]

In 2009, the U.S. reaffirmed that their classification framework only applies to the most important information of the nation, that which affects its national security. As stated in Executive Order 13526, information shall not be considered for classification unless it pertains to one or more of the following:

a. military plans, weapons systems, or operations;

b. foreign government information;

c. intelligence activities (including covert action), intelligence sources or methods, or cryptology;

d. foreign relations or foreign activities of the United States, including confidential sources;

e. scientific, technological, or economic matters relating to the national security;

f. United States Government programs for safeguarding nuclear materials or facilities;

g. Vulnerabilities or capabilities of systems, installations, infrastructure, projects, plans, or protection services relating to the national security; or

h. The development, production, or use of weapons of mass destruction.[7]

The executive order also recognizes the adverse implications associated with the over classification of information. The executive order stipulates that if there is "significant doubt about the need to classify information, it shall not be classified" and similarly, "if there is significant doubt about the appropriate level of classification, it shall be classified at the lower level."[8]

Whereas the U.S. only classifies national security data, the Australians and U.K. prefer to ensure standardization across all data holdings and ministries. The U.K. implemented their new classification system in 2014 replacing the existing Government Protective Marking Scheme which had been in place for decades. The cabinet office noted that "although the core requirements of protecting information have not changed, many of the supporting processes were developed for a paper-based system and are now complex, poorly understood and unsuited to the modern workplace."[9] In an effort to avoid over classification, the U.K. also explicitly notes that 90 per cent of all their data holdings should be classified at the lowest classification. The Australians followed the U.K. very shortly thereafter and implemented a new classification framework in 2018. The Australian framework is very much a hybrid of the U.K. and U.S. model. In keeping

[6] ODNI FY2017 FCGR.pdf pg. 5.
[7] CFR-2010-title3-vol1-eo13526.pdf (govinfo.gov) pg. 300
[8] CFR-2010-title3-vol1-eo13526.pdf (govinfo.gov) pg. 298-299.
[9] Introducing the Government Security Classifications Core briefing for 3rd Party Suppliers, Cabinet Office, October, 2013

with the U.S. construct, they have three classified security classifications. However, in keeping with the U.K. construct, they also recognize that "all other information from business operations and services requires a routine level of protection and is treated as OFFICIAL. Information that does not form part of official duty is treated as UNOFFICIAL."[10]

Whereas other nations caution about the implications of overclassifying data, for the last 40 years Canada has systemically overclassified personal information with an institutionalized belief that the loss of Protected B is at least as injurious as the loss of confidential information if not secret. The reasons nations caution about over classification is because of the adverse consequences which include:

- preventing important information from getting to a decision maker in a timely fashion.
- it accrues significant physical and IT costs for its long-term storage.
- the volume becomes challenging to protect adequately.
- it desensitizes an individual's understanding of what is actually classified information.
- it brings the overall security posture into disrepute or at least undermines it.
- if procedures are not applied properly, it requires an increased demand for security clearances,
- it may unnecessarily limit public access to government information including the historical record, and
- it leads to, or reinforces, a culture of risk aversion.[11]

If Canada is truly committed to avoiding these outcomes, which arguably many have already materialized, and realize its Digital Ambition then there is a pressing requirement to amend its security classification framework. Of the models examined and based on the advancements of commercial encryption and other methods of securing data, the U.K. model would be recommended. Rather than being a directive, the following classification framework should be incorporated into the main body of the Policy on Government Security: Top Secret, Secret, and Official. The handling instructions, not to be confused with classification, of Official - For Public Release and Official-Sensitive, for more sensitive information, are also recommended to be incorporated into the policy.

Further exacerbating the over classification culture in Canada is a very simplistic characterization of what level of injury corresponds to an appropriate security classification. In Canadian strategic policy there is very little amplification of the level of injury. For example, serious injury as it pertains to Secret is "unauthorized disclosure could reasonably be expected to cause serious injury

[10] PSPF policy 8: Sensitive and classified information (protectivesecurity.gov.au) pg. 4
[11] Classification-Review-Report.pdf (igis.govt.nz)

to the national interest". Serious injury as it pertains to Protected B "is unauthorized disclosure could reasonably be expected to cause serious injury outside the national interest, for example loss of reputation or competitive advantage".[12] Based on this limited guidance, the risk of a wide variance in interpretation of the term(s) serious, loss of reputation or competitive advantage is significant. In an effort to ensure alignment horizontally across departments, the only document that was identified that attempted to define the level of injury with any specificity was once again, TRA-1. The level of injury associated with each security classification in TRA-1 is at figure 4.

Figure 4: Expanded Injury Table from TRA-1 with Secret highlighted for comparative purposes to the Australian tool used to assess the level of injury for Secret.[13]

Level of Injury	Injury to People		Financial Impact
	Physical	Psychological	
Very High (Top Secret)	1. Widespread loss of life	1. Widespread Psychological Trauma 2. Potential Civil Unrest	>$1B+
High (Secret Protected C)	1. Potential Loss of Life for Some 2. Permanent Disability for Some 3. Serious Illness or Injury for Many 4. Serious Physical Hardship for Many	1. Serious Embarrassment for Many 2. Serious Doubts/Uncertainty for Many 3. Widespread Public Suspicion 4. Alienation of Large Groups	>$10M+
Medium (Confidential Protected B)	1. Serious Illness/Injury to Some 2. Serious Discomfort for Many 3. Minor Pain for Many	1. Serious Embarrassment for Some 2. Serious Doubts/Uncertainty for Some 3. Serious Inconvenience for Many 4. Minor Embarrassment for Many 5. Minor Doubts/Uncertainty for Many	>$100k+

[12] Directive on Security Management - Appendix J: Standard on Security Categorization- Canada.ca
[13] Microsoft Word - 2007-HTRAM-Eng-Word2002-classroom-1023.doc (cyber.gc.ca) pg. B4-1.

Low (Protected A)	1. Serious Discomfort for Some 2. Minor Pain for Some 3. Minor Discomfort for Many	1. Serious Inconvenience for Some 2. Minor Embarrassment for Some 3. Minor Doubts/Uncertainty for Some 4. Minor Inconvenience for Many	>$1k+
Very Low (Unclassified)	1. Negligible 2. Minor Discomfort for Some	1. Negligible 2. Minor Inconvenience for Some	<$1k

Note: Although the threshold between "some" and "many" remains open to interpretation, one thousand people may be a useful demarcation.

Although the document has not been updated in over a quarter of a century, the link to the document is found on the Canadian Center for Cyber Security website stating that it "is a set of tools designed to address all assets, employees, and services at risk."[14] It is understood that TRA-1 has been superseded from a physical security perspective, however, it has been confirmed with Treasury Board of Canada Secretariat (TBS) that this document is still relevant in the digital security domain. This is reinforced by the fact that it is used as a reference for the document IT Security Risk Management: A Lifecycle Approach (ITSG 33, CSE, 2012 updated in 2015) which supports the guidance on the security categorization of cloud-based services (CSE, 2020).

By comparison the Australian and U.K. policies provide detailed guidance to departments/ministries to help them better define the level of injury/business impact to ensure the most appropriate classification of data is selected. Whereas the level of detail for the Australian tool is far more detailed, both tools provide very similar levels of injury for Secret and Official. For example, the level of injury for secret in both nations includes; directly threaten an individual's life, serious damage to the delivery of current military operations, and serious damage to security or intelligence operations. As evidenced in figure 5, the Australian policy is far more comprehensive than the level of injury defined for Secret/Protected B in Canada.

[14] Harmonized TRA Methodology (TRA-1) - Canadian Centre for Cyber Security

Figure 5: Australian Business Impact Level Tool for Secret[15]

Secret	
Extreme Business Impact	
Very valuable, important and sensitive information. Compromise of SECRET information would be expected to cause serious damage to the national interest, organisations or individuals.	
Potential impact on individuals from compromise of information	
Dignity or safety of an individual (or those associated with the individual)	Serious damage is discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly threaten or lead to the loss of life of an individual or small group.
Potential impact on organisations from compromise of the information	
Entity operations, capability and service delivery	Serious damage to entity operations is: a. a severe degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform any of its functions. b. directly threatening the internal stability of Australia.
Entity assets and finances, eg. operating budget	Not applicable. Impacts on an entity or organisation at this scale (greater than $10 billion) are considered a matter of national interest.
Legal compliance, eg. information compromise would cause noncompliance with legislation, commercial confidentiality or legal professional privilege	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.
Aggregated Data	A significant aggregated holding of sensitive or classified information that, if compromised, would

[15] PSPF policy 8: Sensitive and classified information (protectivesecurity.gov.au) pg. 7 – 8.

	cause serious damage to the national interest, organisations or individuals.
Potential impact on government or the national interest from compromise of the information	
Policies and legislation	Serious damage to the national interest is: a. a severe degradation in development or operation of multiple major policies to an extent and duration that the policies can no longer be delivered.
Australian economy	Serious damage to the national interest is: a. undermining the financial viability of an Australian industry sector (multiple major organisations in the same sector) b. long-term damage to the Australian economy to an estimated total in excess of $20 billion.
National infrastructure	Serious damage to the national interest is shutting down or substantially disrupting significant national infrastructure
International Relations	Serious damage to the national interest is: a. severely disadvantaging Australia in major international negotiations or strategy b. directly threatening internal stability of friendly countries, leading to widespread instability c. raising international tension or severely disrupting diplomatic relations resulting in formal protest or sanction.
Crime prevention, defence or intelligence operations	Serious damage to the national interest is major long-term impairment to the ability to investigate or prosecute serious organised crime affecting the operational effectiveness, security or intelligence capability of Australian or allied forces.

The differences between the Canadian and our allies' characterization of what constitutes secret are stark. Although it is recognized that the TRA-1 table is almost 20 years out of date, the challenge for departments is that TRA-1 also denotes that "where the injuries to people (either physical or psychological) and the financial impact arising from a single compromise to one asset

differ, record the highest value".[16] As the financial impact for the equivalent of Secret is any risk assessed in value of greater than $10 Million, but less than $1 Billion, it is not hard to understand how many activities are characterized as high risk in Canada.

In light of the shortcomings of the existing construct, it is recommended Canada codify the level of injury/business impact for each security categorization across multiple business lines. It is also recommended that they are more closely aligned with our closest allies and partners, particularly for secret. Once again, this information should be incorporated into the Policy on Government Security. It would also be worth considering rescinding the Harmonized Threat and Risk Assessment Methodology (TRA-1) and if a requirement still exists for such a document, redevelop it after amending the classification and business impact frameworks.

Aggregation of Data

Another consideration that is closely aligned with the classification of data is the concept of data aggregation. In both the U.K. and Australia the aggregation of data is dealt with in government policy and in the U.S. by the National Institute of Standards and Technology. In all three countries, the aggregation of data applies to aggregating data from multiple data sources. In the United States, it is important to remember that only national security data is classified and therefore the aggregation of all other data sets would not warrant being classified. In Australia, the policy articulates that a compilation of information "may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components."[17] Note the use of the term "may" and "significant" as the decision is not automatic. In determining whether to increase the classification other options are to be considered such as additional access or security controls.[18] In the U.K., they have recently provided greater clarity from their 2018 posture which stated "Aggregated data sets should be considered to be within the same classification level: however where the impact of compromise or loss has increased as a result of aggregation, these aggregated data sets must be carefully and tightly controlled."[19] The subtle difference in the articulated 2023 posture is that "Aggregating data will not usually affect the classification of the component information, but a new piece of data or set of data, formed as a result of associations, may need to be classified at a higher level."[20]

In Canada, the only reference to the aggregation of data at a policy level is a June 2023 Security Policy Implementation Notice (SPIN). Up until the release of the SPIN, the only reference to the aggregation of data was found in TRA-1. Specifically, it states "as the number of assets increases, the injuries arising from compromise may grow as well. For example, unauthorized disclosure of a single personnel file might be expected to cause some embarrassment to the individual and generate public anxiety regarding personal information. If all human resource records for a major

[16] Microsoft Word - 2007-HTRAM-Eng-Word2002-classroom-1023.doc (cyber.gc.ca) pg. B4-2.
[17] PSPF policy 8: Sensitive and classified information (protectivesecurity.gov.au) pg. 8.
[18] PSPF policy 8: Sensitive and classified information (protectivesecurity.gov.au) pg. 44.
[19] Government Security Classifications Version 1.1 May 2018 Cabinet Office pg. 31.
[20] Guidance 1.5: Considerations for Security Advisors.docx (publishing.service.gov.uk) pg. 23.

department were released inappropriately, however, the adverse effects could be significantly worse."[21] In keeping with the government's culture of avoiding policy risk, this guidance was translated into a more restrictive posture by a major department as follows: "A file containing one address may be protected A, while a file containing 10 000 addresses would be at least Protected B."[22]

The reality for public servants is that they have been led to believe that the aggregation of protected data will at some juncture cross the threshold of data being in the national interest. This is not possible based on the fact that they are two different types of information by definition. TRA-1 reinforces this fact. Unfortunately, as TRA-1 improperly characterized the level of injury of Protected C as being the equivalent of Secret, the culture has erroneously assumed that aggregated Protected B data should be classified as Secret based on "equivalency". To attempt to address this culture of over classification, the SPIN states that "The personal information of individuals that is used to deliver GC services and benefits should be categorized as no higher than Protected B." This SPIN is exceptionally helpful for clarifying personal information however, the current culture of over classification extends to all data holdings. It is therefore recommended that concurrent to amending the security classification framework, Canada defines data aggregation to reflect multiple data sets and recognizes that although there may be increased risk, the mechanism to mitigate the risk is through access and controls and not through increasing the classification of the data unless new data sets are created.

Regardless of whether the data is protected or classified, the focus should be less on the fact that data can be aggregated and more on who has access to the data. Technological advances in data security, access management, and architectures such as Zero Trust, mitigate the implications of data aggregated in a single system. The overly simplistic characterization that data should not be aggregated because of the belief that once you have the keys to the filing cabinet means that you can see everything in it, is not particularly helpful in realizing our digital ambition. Until these conversations are had, the culture will prevail particularly as it pertains to personal data.

As a result of personal data being confused with having similar risks to confidential or secret information, it has also had unintended consequences on Privacy Impact Assessments. Ensuring that personal data is properly safeguarded is extremely crucial and the Digital Ambition reinforces the importance of Canadians having trust in the ability of their government to protect their personal information and data. "Putting in place appropriate and rigorous privacy measures will assure Canadians that their personal information is protected while continuing the move toward more digital approaches in the delivery of government services."[23] This commitment is amply reinforced with the most recent amendments to the government's Policy on Privacy and the Directive on Privacy Practices that were completed in 2022. However, despite the requirement to review on an annual basis, the Directive on Privacy Impact Assessment has not been updated since 2010.[24]

[21] Microsoft Word - 2007-HTRAM-Eng-Word2002-classroom-1023.doc (cyber.gc.ca) pg. B-14.
[22] Working With Sensitive Information - Canada.ca
[23] Canada's Digital Ambition 2022 - Canada.ca
[24] Directive on Privacy Impact Assessment- Canada.ca

Personal information is clearly defined in the Privacy Act."[25] The act is also explicit about how government shall collect, retain, protect, access and dispose of personal information, which is very similar to the legislation of our Five Eyes Partners and the EU. However, unlike our Five Eyes Partners and the EU, the act does not require government to conduct a privacy impact assessment prior to collecting personal data. As a matter of fact, the act does not mention or refer to privacy impact assessment at all. However, policy requires this assessment be completed. The TBS Policy on Privacy Protection (Oct, 2022) articulates that heads of government institutions are to ensure that "when applicable, privacy impact assessments (PIAs) and multi-institutional PIAs are developed, maintained and published."[26] The Directive on Privacy Impact Assessment provides the explicit direction on the completion of PIAs.

As the PIA represents an important tool it is useful to compare it to our allies and closest partners. As indicated in figure 6, the U.K., Australia, U.S. and the EU have all updated their PIA guidance between 2016-18.

Figure 6: A comparison of Canada's PIA requirements to those of U.K., Australia, U.S. and the EU.

	Canada	**U.K.[27]**	**Australia[28]**	**U.S.[29]**	**EU[30]**
PIA direction last amended	2010	2018	2017	2016	2016
Flexibility to tailor PIA	Only after 6 sections of core PIA completed	Yes	Yes	Yes	Yes
Risk defined by probability and consequence	No	Yes	Yes	Yes	Yes
Flexibility with respect to risks considered	No	Yes	Yes	Yes	Yes
Flexibility to assign risk level	No	Yes	Yes	Yes	Yes
Recognizes advances in new digital technologies	No	Yes	Yes	Yes	Yes

[25] P-21.pdf (justice.gc.ca) Pg. 2-3 provides a complete list that would be considered personal identifiable information
[26] Policy on Privacy Protection- Canada.ca
[27] Data Protection Impact Assessments (DPIAs) | ICO
[28] Guide to undertaking privacy impact assessments | OAIC
[29] Review-Doc-2016--466-1.docx (whitehouse.gov)
[30] endorsement_of_wp29_documents_en_0.pdf (europa.eu) https://www.bing.com/search?q=20171013_wp248_rev_01_en_D7D5A266-FAE9-3CA1-65B7371E82EE1891_47711.pdf&cvid=27d8d5729c4a4d51b61beb859bdf8629&aqs=edge..69i57.7422j0j4&FORM=ANAB01&PC=U531 Data protection impact assessment Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, WP248 rev.01

It is also noteworthy that all of the other countries provide PIA templates for consideration by departments but that they are encouraged to tailor them accordingly to their requirements. The Canadian PIA only allows for departments to tailor their PIA once they have completed the core PIA which consists of the following six sections:

Section I – Overview and PIA Initiation

Section II – Risk Area Identification and Categorization

Section III – Analysis of Personal Information Elements for the Program or Activity

Section IV – Flow of Personal Information for the Program or Activity

Section V – Privacy Compliance Analysis

Section VI – Summary of Analysis and Recommendations

Section VII – Supplementary Documents List

Section VII – Formal Approval

As discussed previously, in accordance with the Government of Canada's risk management framework, deputy heads are responsible for the risk management of their departments. However, section II of the core PIA is very prescriptive, and it defines the level of risk being assumed by departments. Imagine the frustration of dedicated public servants trying to deliver modern digital services that are citizen centric, reflect citizen experiences and expectations and leverage software as a service only to come to understand that the initiative is high risk. I have taken the liberty of completing section II that would very closely approximate the risk associated with such initiatives. Color coding is used as a visual reference of risk where green represents low risk, yellow medium risk and red high risk.

Figure 7: Section II - Risk Area identification and Categorization[31]

a) Type of program or activity	**Risk scale**
- Program or activity that does NOT involve a decision about an identifiable individual	1
- Administration of program or activity and services	2
- Compliance or regulatory investigations and enforcement	3
- Criminal investigation and enforcement or national security	4

[31] Directive on Privacy Impact Assessment- Canada.ca

b) Type of personal information involved and context	
- Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	1
- Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	2
- Social Insurance Number, medical, financial or other sensitive personal information or the context surrounding the personal information is sensitive; personal information of minors or of legally incompetent individuals or involving a representative acting on behalf of the individual.	3
- Sensitive personal information, including detailed profiles, allegations or suspicions and bodily samples, or the context surrounding the personal information is particularly sensitive.	4
c) Program or activity partners and private sector involvement	
- Within the institution (among one or more programs within the same institution)	1
- With other government institutions	2
- With other institutions or a combination of federal, provincial or territorial, and municipal governments	3
- Private sector organizations, international organizations or foreign governments	4
d) Duration of the program or activity	
- One-time program or activity	1
- Short-term program or activity	2
- Long-term program or activity	3
e) Program population	
- The program's use of personal information for internal administrative purposes affects certain employees.	1
- The program's use of personal information for internal administrative purposes affects all employees.	2

- The program's use of personal information for external administrative purposes affects certain individuals.	3
- The program's use of personal information for external administrative purposes affects all individuals.	4
f) Technology and privacy	
- Does the new or substantially modified program or activity involve implementation of a new electronic system or the use of a new application or software, including collaborative software (or groupware), to support the program or activity in terms of the creation, collection or handling of personal information?	
- Does the new or substantially modified program or activity require any modifications to information technology (IT) legacy systems?	
Specific technological issues and privacy - Does the new or substantially modified program or activity involve implementation of new technologies or one or more of the following activities: • enhanced identification methods; • surveillance; • or automated personal information analysis, personal information matching and knowledge discovery techniques?	
A **YES** response indicates the potential for privacy concerns and risks, which will require consideration and, if necessary, mitigation.	
g) Personal information transmission	
- The personal information is used within a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled).	1
- The personal information is used in a system that has connections to at least one other system.	2
- The personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed.	3
- The personal information is transmitted using wireless technologies.	4

It is important to note the amount of red and yellow in the PIA and how this would be interpreted in a risk sensitive department. It is also known that departments layer on additional PIA

requirements such as a legal review. Convincing an executive to proceed with this high-risk initiative despite the fact that the technology is widely used and trusted by Canadians in other sectors would be a challenge. The mistaken belief that compromise or loss may be the equivalent to the level of injury associated with secret data misrepresents the impact in the risk management calculation. As the analysis of this article required a great deal of research leveraging Canadian government online resources, there were several processes that were observed that are still paper based and require a telephone. Looking at those processes through the lens of the PIA, it becomes clearer why they are not digital. In almost every respect, the PIA would characterize the transition from a 20-, 30- or 50-year-old legacy system as high risk from a privacy perspective. This obscures two facts:

- The first is that maintaining the status quo from a privacy and service delivery perspective very likely represents extremely high risk.
- The second is that the Digital Ambition represents moving to a lower risk posture leveraging modern digital solutions to enhance government's ability to better protect the privacy of their citizens data and to deliver secure services online or in the cloud.

Rather than the prescriptive model that Canada has adopted, other nations have implemented a principles-based framework for their privacy impact assessments. Although Canada speaks to some of these principles in outcomes and objectives, the PIA global best practice is to frame the government's commitment to privacy from a principle's perspective. The following principles are all common to the other nation's privacy frameworks and are assessed as being applicable to the Canadian context: Accountability, Authority, Minimization, Quality and Integrity, Purpose Specification and Use Limitation, Security, and Transparency. A principles perspective that recognizes the importance of privacy and respects the Authorities Responsibilities and Accountabilities (ARAs) of ministers and deputy heads would better enable the realization of the Digital Ambition. It is recommended that Canada Develop a principles approach to privacy and incorporate it into the Policy on Privacy Protection next policy refresh. It is also recommended that The Directive on Privacy Impact Assessment Appendix C – Core Privacy Impact Assessment be amended as follows:

- Transition appendix C to a "tool" for consideration by departments,
- Amend Section II – Risk Area Identification and Categorization from a simplistic and inflexible risk categorization framework, which does not keep pace with improved technologies, processes and procedures, to a broader framework that enables departments to leverage proper risk management strategies to characterize and define risks and to implement plans to mitigate them as required.

Benefits to Updating Canada's Security Classification and Privacy Framework

As new digital technologies have delivered ever increasing transformational capabilities, it is unfortunate that these technologies and their procurement have been made to "fit" within the current categorization framework and its associated simplistic level of injury. The unintended consequences of this "reverse engineering" have been the incremental institutionalization of inefficiencies, increased operation and maintenance costs, increased capital costs, a culture of over-classification of data, and increased human resource costs affecting hiring, training, and security clearances. Policy, not culture, drives the security classification framework, directs an elevated risk sensitivity/level of injury, and requires departments to proactively mitigate risk. The implications affect almost all government operations including procurement.

To mitigate procurement risk the Contract Security Program (CSP) has been implemented. Although, our allies and closest partners all have similar programs, their resources are dedicated to mitigating risks associated with contractors having access to classified national security information and assets which are projects that are Secret or Top Secret. Once again, Canada is unique requiring all contractors to have a government issued reliability/security clearance for access to non-classified information. For example, in Australia, "A security clearance is not required to access information that does not have a security classification, including Official or Official: Sensitive information. For this type of information, routine employment screening is sufficient."[32] Similarly, New Zealand takes a risk management approach for hiring contractors that do not require access to classified information.

As a result of Canada's CSP applying to all procurements, it drives up procurement costs, causes delays in procurement delivery, and once again directs resources to address inflated levels of injury. A key requirement of the CSP is ensuring that individuals are issued the appropriate security status/clearance. In the Standard on Security Screening (Oct, 2014) there are three standard screening criteria: reliability status, Secret clearance and Top Secret clearance, in addition to enhanced levels for reliability and Top Secret. Although the number of security status/clearances issued to non-public servants has increased significantly to approximately 750 000, and will continue to increase year over year, the overall representative percentage of clearances has remained relatively constant during the last decade. Approximately two-thirds are reliability, one-third Secret and less than two per cent Top Secret. Essentially there are approximately 490 000 reliability, 245 000 Secret and 15 000 Top Secret clearances issued to non-public servants. Therefore, approximately 75 000 status/security clearances require a renewal each year in addition to those that must be issued to support new procurements. The pressure that this has put on the CSP is significant as evidenced by the most recent CSP policy update that came into effect in May of 2022.[33]

The excessive security clearance requirements that extend into procurement also extend into the public service. If Canada were to adopt the same level of injury for Secret information as that of

[32] Security clearances – Overview | Sectors | Defence
[33] Upcoming changes to the Contract Security Program's security screening process: Phase 2 implementation - News and updates about contract security – Security requirements for contracting with the Government of Canada – Canada.ca (tpsgc-pwgsc.gc.ca)

our allies and closest partners, of 74 core and non-core public administration departments, 54 departments would not require access to Secret information, seven departments may require access and 13 departments would require access to Secret information. Of all the departments examined that required access to Secret information, none of them would require all employees to have a Secret security clearance. For example, the current requirement at TBS is for 100 per cent of their personnel to have a secret security clearance. With the adoption of a new security classification framework, only 20 per cent of the approximately 2750 personnel would require access to Secret information. Real cost savings would be realized in the following areas:

- reduction in Secret IT infrastructure (devices, desktop, and intranet),
- reduction in Secret data holdings,
- reduction in number of Secret security clearances,
- reduction in physical security infrastructure upgrades necessary to support Secret data holdings,
- reduction in the number of departmental organizations required to maintain Secret IM/IT infrastructure, and
- reduction in costs associated with procuring Secret cleared services such as cleaners, commissionaires, and maintenance contractors.

In addition, to the cost savings the following advantages would accrue:

- a security classification framework that better reflects 21st century digital realities to ensure not only the privacy and security of Canadian's data, but data that affects our national security,
- a classification framework that is less complex and provides more guidance will make it easier for public servants to follow and reduce the significant variance in the interpretation of the level of injury across the government that has led to a culture of over classification,
- it will enable an opportunity to ensure greater transparency of government data with Canadians and streamline Access to Information and Privacy (ATIP) requests,
- it is sufficiently significant that it will overcome the inertia of a minor amendment to policy and move the culture towards the digital-first mindset articulated in the Digital Ambition,
- it will facilitate more seamless exchange of information with our allies and partners, and

- currently it is often easier to get a Secret technology-related procurement under contract than it is to get a Protected B procurement under contract because there is no international equivalent of Protected B. Vendors with workforces that are increasingly globally distributed have difficulty clearing resources to align to Canada's protected information regime, being unable to rely on foreign equivalencies. This challenge would be alleviated in the new classification framework.

It is recognized that updating Canada's security classification framework represents a significant body of work as they affect almost all facets of government operations. As a result, there will be a requirement to update several other policies. As other policies are amended to reflect these changes, it would be logical to take the opportunity to align terminology across data, physical (RCMP - G1-026 Guide to the Application of Physical Security Zones), network (CSE - Baseline Security Requirement for Network Security Zones) and personnel security clearance (OCIO – Standard on Security Screening) policies. For example, today a public servant requires a reliability clearance to access Protected B data and below in a physical operations Zone on a network that is either an operations or restricted zone. In order to better harmonize and align policies to mitigate gaps and seams that could result, leveraging the same terminology and the same model, where possible, would be advantageous. For example, in a potential new policy construct a public servant would require an Official security clearance to access official data on IT in an official network zone located in a physical official zone. The beneficial effects of such a harmonization would be very significant in ensuring that the policy isn't simply words on a page, but rather a series of changes deliberately implemented in the culture and the business.

Therefore, it is crucial that the aforementioned recommendations be implemented in order to enable the Government of Canada to achieve their digital ambitions.

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.

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.