The Definition, Measurement, and Institutionalization of Transparency in National Security

Government of Canada
Gouvernement du Canada

Canada

The National Security Transparency Advisory Group (NS-TAG) is an independent, arms-length committee that is supported financially and in-kind by the Government of Canada. The opinions and views expressed in this document are strictly those of the NS-TAG members collectively, and should not be considered as the official view of the Government of Canada.

Cat. No: PS9-21/2021E-PDF
ISBN: 978-0-660-39315-5

Table of Contents

Members of the NS-TAG at the time this report was written:

Michèle Audette, Senior Advisor for Reconciliation and Indigenous Education and Assistant to the Academic and Student Affairs Vice-Rector, Université Laval.

William Baker, Chair of Immigration, Refugees and Citizenship Canada's Departmental Audit Committee, Former Deputy Minister of Public Safety Canada

Khadija Cajee, Co-Founder, No Fly List Kids

Mary Francoli, Director, Arthur Kroeger College of Public Affairs, and Associate Dean, Faculty of Public Affairs

Harpreet Jhinjar, Expert in Community Policing and Public Engagement

Thomas Juneau (non-governmental co-chair), Associate Professor, University of Ottawa's Graduate School of Public and International Affairs

Myles Kirvan, Former Associate Deputy Minister of Public Safety Canada, former Deputy Minister of Justice and Deputy Attorney General of Canada

Justin Mohammed, Human Rights Law and Policy Campaigner, Amnesty International Canada

Bessma Momani, Professor of Political Science at the University of Waterloo, Senior Fellow at the Centre for International Governance and Innovation

Dominic Rochon (government co-chair), Senior Assistant Deputy Minister, National and Cyber Security Branch, Public Safety Canada

Jeffrey Roy, Professor, School of Public Administration at Dalhousie University's Faculty of Management

Executive Summary

The National Security Transparency Advisory Group (NS-TAG) was created in 2019 as an independent and external body. Our role is to advise the Deputy Minister of Public Safety Canada, and the rest of the national security and intelligence community, on steps to infuse transparency into Canada's national security policies, programs, and activities in a manner that will increase democratic accountability and public awareness, engagement, and access to national security and related intelligence information.

In our first report, published in December 2020, we offered a survey of the state of transparency in Canada's national security community, and highlighted areas for future improvement.

In this second report, we lay out general principles related to the definition, measurement, and institutionalization of transparency in the national security and intelligence community. For greater transparency to be sustainable, it must be institutionalized and routinized; structures and processes must be put in place to define, measure and then 'hardwire' transparency into the national security community's everyday work.

To do so, we recommend that individual departments and agencies with national security functions should:

- Develop and release a clear statement in which they express their commitment to greater transparency;
- Develop and release metrics to measure and evaluate the implementation of their transparency commitment;
- Institutionalize a range of initiatives to support their efforts to enhance transparency;
- Develop a common understanding around the purpose of community engagement and its importance in enhancing transparency and building trust, and invest more resources to better train and equip personnel with less experience with community engagement.

1. Introduction

Government transparency is foundational to the rights of citizens in democratic countries. A range of national and international legal instruments enshrine fundamental human rights such as freedom of the press, freedom of assembly and freedom to participate in public life. A lack of transparency impedes the realization of these rights and, invariably, the health of a democracy. In the absence of transparency, it is difficult to hold government to account, there is risk of government abuse and corruption, and public trust in government erodes. On the other hand, the social impacts of transparency are wide reaching and can touch on health, education and the economy. Additionally, in light of the COVID-19 pandemic, new concerns about transparency and its impact on the work of the national security community have emerged. We briefly address these at the end of this report.

Promoting transparency in the world of national security, which has historically been marred by a culture of secrecy, is complex. As we noted in our first report, despite recent improvements, the national security community in Canada does not have a strong record in meeting the highest standards of transparency. This has a negative impact on the confidence of citizens in national security institutions.

Through virtual meetings, the NS-TAG consulted extensively and meaningfully in preparing this report. We heard that the lack of transparency in national security is felt across many sectors. Journalists noted that they struggle to provide reliable information on national security. Many citizens mistrust national security institutions and, as noted above, are unable to benefit from their democratic rights to their fullest extent. The work of the national security community also suffers as it struggles to effectively engage with citizens. Weakened democratic health invariably results from a poorer flow of competing ideas.

"About half (49%) of Canadians agree that publicly available Government information on national security is more trustworthy than information found elsewhere."

Source: Library and Archives Canada – Public Opinion Research Report 072-20

Openness, transparency and civic engagement have become the basis of an international advocacy movement. The Open Government Partnership, an initiative founded in 2011 to promote accountability, transparency and inclusive government and of which Canada is a member, has grown from eight member countries to 78, in addition to a growing number of local governments. Non-governmental organizations such as Transparency International have been reporting on transparency for even longer. The International Budget Partnership, Publish What You Pay and the Open Contracting Partnership, to name a few, are among the many organizations that now work to promote transparency in various sectors.

Defining, measuring and institutionalizing transparency call for a basic understanding of not only why transparency matters, but also of the structural and cultural determinants of systemic reforms that can lead to improved institutional accountability and better performance. With respect to defining transparency, it is important to acknowledge varying approaches to articulating the concept in general terms, as well as in more applied contexts specific to agency mandates. While we see value in articulating a broad set of principles for the national security community, it is equally imperative to transform these principles into specific measurable outcomes across the community in ways that are relevant to both individual agencies and government as a whole.

Measurement is equally essential: research and experience confirm that what gets measured matters in determining decisions and tracking impacts. Moreover, recent government reforms tied to open government and results-based management underscore the importance of providing clear indicators of performance goals. In a realm as complex as national security, it is important that reporting include quantitative and qualitative benchmarks, along with the regular holding of consultations with stakeholders and the public. Measurement must be viewed not as a singular linear exercise but as an enabler of learning, adjustment and continual improvement. Accordingly, measurement is an essential foundation for shared accountability and public engagement by grounding dialogue in indicators of success and failure, not only to better assess past performance, but also to prepare for emerging and increasingly complex challenges.

An emphasis on consultation and engagement is essential to institutionalize transparency in meaningful ways, and requires cultural and structural reforms to the governance of national security. Cultural change in any large organization takes effort and time, and this is especially relevant to national security where secrecy has been a hallmark of individual action and organizational leadership. The essence of the NS-TAG is to support the creation of a shared understanding for organizational cultural change, as well as specific policy and governance reforms that can help steer the process of institutionalizing transparency in pursuit of strengthened accountability and greater innovation.

2. Definition

> **We recommend that every department and agency with national security functions develop and release a clear statement in which they express their commitment to greater transparency.**

This statement should represent a commitment to transparency, an articulation of the department or agency's interpretation of what transparency means, why it is important, and how it will be measured and implemented. The commitment should be specific and provide a foundation for further reporting and accountability. In drafting this commitment, departments and agencies can use the government's National Security Transparency Commitment as a foundation, while adapting it to their particular circumstances.[1]

Departmental transparency statements should be made public. They should be hosted, in an easily accessible manner, preferably on existing departmental webpages dedicated to transparency (where they could be bundled with specific initiatives and documentation such as mandate letters, departmental reports and proactive disclosure).[2] By publicizing this statement, these organizations can establish the parameters for performance reporting and create a public expectation that they will pursue this commitment to transparency. We also encourage organizations to commit to review, and revise as necessary, their definition of transparency as they gather experience.

There are many definitions of transparency. At its most fundamental level, it can be defined as "official business conducted in such a way that substantive and procedural information is available to, and broadly understandable by, people and groups in society, subject to reasonable limits protecting security and privacy".[3]

Yet beyond this general definition, there are different types of transparency. It can be interpreted expansively, for example, or it can focus on the type of information to be released, or more on the processes governing these releases.

When defined narrowly and passively, transparency simply corresponds to the release of requested information. Demand-driven tools such as access to information requests, moreover, are principally used by a limited segment of society, such as journalists, academics and non-governmental organizations.

[1] Canada, Public Safety Canada, *National Security Transparency Commitment*, December 22 2020. https://www.canada.ca/en/services/defence/nationalsecurity/national-security-transparency-commitment.html.
[2] Ibid. List of individual department and agency transparency webpages.
[3] Michael Johnston. "Good Governance: Rule of Law, Transparency, and Accountability", Colgate University, 2002. https://etico.iiep.unesco.org/sites/default/files/unpan010193.pdf.

A broader and more dynamic interpretation, one that the NS-TAG supports, also emphasizes bolstering citizen engagement and government responsiveness. Similarly, an expansive conception of transparency does not only describe what information is released (and why and how), but also what information cannot be released (not only its quantity and quality, but also based on what authorities and as a result of which process, with the availability of meaningful and rapid review to challenge omissions and redactions). It is, in this sense, essential to be ‘transparent about transparency’, as one of our invited speakers argued. Moreover, an essential pillar of a dynamic transparency strategy also promotes citizens’ ability to access information and supports their understanding of processes to do so, what can be labeled as latent transparency.[4]

“One in three (32%) Canadians agree that they know where to find Government information about national security issues and threats, although four in ten (41%) disagree.”

Source: Library and Archives Canada – Public Opinion Research Report 072-20

We recommend that departments and agencies with national security functions adopt a proactive definition of transparency, as opposed to a narrow, reactive and passive one. Departments and agencies should seek to engage stakeholders within and outside government in a dialogue to identify the scope of such an outward, expansive and dynamic definition of transparency. Such a dialogue would also serve as a basis for ongoing efforts to establish and refine measurement and to foster institutionalization and adaptation over time.

3. Measurement and Reporting

> **We recommend that each department and agency with national security functions develop relevant metrics to measure and evaluate the implementation of this transparency commitment.**

We recognize that measuring transparency can be challenging, and that it is labour-intensive. Nevertheless, we believe that it is essential. Without a clear process to measure transparency, it is difficult to assess whether commitments to become more transparent have been fulfilled. Indeed, the act of measuring transparency is itself a step toward transparency.

In this context, the NS-TAG believes that departments and agencies with national security functions should operationalize their definition of transparency and explain how they plan to measure and track their progress. This implies that they should also put in

[4] Stephan G. Grimmelikhuijsen et. al., “Latent Transparency and Trust in Government: Unexpected Findings From Two Survey Experiments”, Government Information Quarterly, 2020, Vol. 37, no. 4. https://www.sciencedirect.com/science/article/abs/pii/S0740624X20302768.

place the mechanisms to collect, analyze and then disseminate the results. Both the metrics and the regular reporting based on those metrics should be easily accessible to the public, possibly alongside the transparency statement on their website. We recommend, moreover, that departments and agencies should include a discussion of their transparency measurement and reporting efforts in their annual reports tabled in Parliament (the Departmental Plan, tabled annually and which provides parliamentarians and Canadians with a high-level summary of plans and priorities, and the Departmental Results Report, which accounts for results achieved against expectations set out in the Departmental Plan).

National security departments and agencies should develop specific indicators to measure progress toward achieving greater transparency. These should be relevant to the mandate of each specific agency, though some indicators could also be common across the community. The National Security Transparency Secretariat in Public Safety Canada can help coordinate this process, along with the interdepartmental working groups charged with the implementation of the National Security Transparency Commitment. Without prejudging the outcome, we can envision indicators such as:

- the proactive disclosure (where appropriate) of policies, operating parameters and activities;
- data about complaints and investigations, and specific outcomes from resolved disputes or litigation;
- disaggregated data on diversity, including on race, in individual departments and agencies;
- official documents for public access without necessitating Access to Information procedures;
- public outreach activities;
- the disaggregated budgetary allocations of national security organizations;
- information about cybersecurity threat assessments and potential privacy breaches;
- open data holdings and data-sharing policies and activities;
- qualitative and quantitative information on the use of emerging technologies (notably Artificial Intelligence systems) for national security purposes; and
- declassification of historical information and documents.

Again, we emphasize that in measuring their performance on these metrics, departments and agencies should consult widely: by definition, efforts at the level of measurement should be transparent. Consultations with stakeholders on the measurement of departmental performance, in particular, should be institutionalized. Even if consultations are labour-intensive, they are essential.

We also recommend that departments and agencies with national security functions consider developing a system to measure the transparency of their community engagement. In doing so, it is important not to limit this measurement to the number of outreach events or of training programs. Instead, the effectiveness of these initiatives should be carefully determined to measure quality over quantity. The benefits of these initiatives are difficult to measure in the short term. However, they can produce tangible benefits over the long term as trust and partnerships grow with communities and stakeholders.

4. Institutionalization

> **We recommend that departments and agencies with national security functions should institutionalize transparency initiatives.**

Here again, we offer general principles as well as specific proposals that could guide this ’hardwiring’ of transparency. It should be noted that the Government of Canada’s National Security Transparency Commitment already provides positive suggestions. For example, Principle 1 on “information transparency” calls on institutions to “examine their holdings and release summary information that demonstrates what they do and the scale of those efforts”. Principle 2 calls on departments and agencies to support Canadians in accessing national security information to the “maximum extent possible without compromising the national interest, the effectiveness of operations, or the safety or security of an individual.”

Institutionalizing transparency requires cultural change: mindsets that have traditionally privileged the hoarding of information as the default posture must evolve. The institutionalization of transparency also needs to be championed from the top. The national security community’s leadership must commit to transparency to motivate staff engagement and to increase trust among the rest of their organization. In this context, we recommend that the public service consider including a transparency commitment in the performance agreement for each deputy minister or head of agency in the national security community. Every department should also name a transparency champion at a senior level who would coordinate and promote efforts to better hardwire transparency from within.

Transparency is not just about releasing information. It is also about direct engagement with the public, including during the policy-making process, in line with Principle 6 of the National Security Transparency Commitment. There is, as such, a need for regular interaction, dialogue and consultation with civil society, media, academia and

“Two in three (66%) Canadians feel it is important that Canada’s national security departments and agencies reach out to various organizations, experts, groups or communities, external to Government, to obtain their views on national security policies, programs and issues.”

Source: Library and Archives Canada – Public Opinion Research Report 072-20 businesses. The national security community must build sustainable partnerships to achieve this, not merely organize occasional, ad hoc exchanges with a narrow subset of the population. For example, the CSIS Director recently gave a public speech in which he highlighted the need for CSIS' legal authorities to evolve;[5] any such changes to the mandate and authorities of CSIS should be predicated on transparent and meaningful consultation.

National security and intelligence personnel often do not have the necessary tools to implement initiatives to enhance transparency. As such, we recommend that the community adopt a greater commitment to training on transparency. Individual courses on transparency are necessary, but it is also essential to integrate transparency across personnel training, not just as part of separate modules. Personnel should, in particular, learn the skills necessary to write with a clearer and more concise style when documents are for public consumption. More broadly, institutional culture should better encourage open and honest communication with the public.

We also observe that one of the key impediments to greater transparency in the national security community is the widespread tendency to overclassify information.[6] This is largely explained by an imbalance of incentives, which steers national security personnel, more often than not, to err on the side of caution.[7] That is, the penalties for underclassification can be significant, while there are few, if any, for overclassification. There is, moreover, rarely a need to justify decisions to classify information at a higher level than necessary. The benefits of overclassification, as a result, are internal while the costs are externalized. Reducing overclassification, we believe, would be an essential step toward greater transparency and accountability. We therefore recommend that the national security and intelligence community consider making it harder to overclassify information. This could be accomplished by, for example, taking steps to lessen the fear of underclassifying information, adopting an explicit reference in performance management frameworks, and conducting spot audits or reviews of the appropriateness of classification levels.

[5] Canada, Canadian Security Intelligence Service, "Remarks by Director David Vigneault to the Centre for International Governance Innovation", February 09 2021. https://www.canada.ca/en/security-intelligence-service/news/2021/02/remarks-by-director-david-vigneault-to-the-centre-for-international-governance-innovation.html.

[6] This is an issue we briefly raised in our first report. Canada, National Security Transparency Advisory Group, *Initial Report: What We Heard in Our First Year,* December 08 2020. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2020-nstag-irwwh/index-en.aspx.

[7] Elizabeth Goitein and David Shapiro, "Reducing Overclassification through Accountability," Brennan Center for Justice, 2011.
https://www.brennancenter.org/sites/default/files/legacy/Justice/LNS/Brennan_Overclassification_Final.pdf.

Institutionalizing Transparency Through Community Engagement

Community engagement initiatives are essential anchors to institutionalize and implement greater transparency. At the centre of this responsibility is the national security community's willingness to build its own capacity for engaging with Indigenous, racialized, marginalized and other minority communities. As such, we recommend that the community improve its capacity to practice meaningful engagement.

The current level and understanding of community engagement among the national security community varies significantly. There is a need to break silos and develop a more cohesive community engagement strategy. To do this effectively, national security institutions can benefit from identifying their blind spots and establishing a stronger common understanding of community engagement.

Inconsistent messaging on engagement from different national security agencies creates confusion and mistrust in communities. This further impedes the efforts made toward improving transparency. While the level of community engagement is different for each agency depending on its mandate, it is important to acknowledge that the communities they engage with are often the same. It is for this reason that we recommend a more coherent understanding of the purpose of community engagement and its importance in improving transparency and building trust. This starts with building each department and agency's internal capacity to strengthen community engagement practices and learning how to effectively implement them.

We also note that many national security departments and agencies have limited experience with community engagement. Consequently, they are insufficiently equipped to perform effective community engagement. We therefore recommend that these departments and agencies provide more resources to their units responsible for interacting with relevant communities as an essential step towards institutionalizing efforts to improve transparency.

Building such institutions is an essential step, but so is assuring visibility around these efforts. Communicating effectively is an important part of carrying this responsibility. We therefore recommend that national security institutions develop practical strategies to better communicate their efforts not only with the general public, but also by reaching out to the communities with which the lack of transparency contributes to mistrust.

For example, CSIS and CSE are now active on social media to promote and discuss their reports. This is an effective way of engaging with the public. The *CSIS Public Report 2019*, for example, is important for racialized and marginalized communities because it refers to the importance of terminology when discussing threats to national security. Such reports help ensure that language does not unintentionally or unfairly stigmatize a given community. It is important that reports like this one reach the communities that were affected by previous stigmatizing language. Communicating such new initiatives in an effective and transparent manner is an opportunity to demonstrate a commitment to the affected communities.

5. COVID-19 and National Security Governance: Implications for Transparency

The COVID-19 pandemic has had significant impacts on national security; we believe that it is important for the NS-TAG to briefly address these challenges here. As new threats and challenges have emerged, the governance of national security must evolve. Indeed, within any ‘new normal’ taking shape, learning and adaptation are essential. With respect to transparency, there are three areas that stand out as especially relevant to the NS-TAG’s efforts: shifting boundaries of national security policies and heightened complexity; cybersecurity and data privacy; and the evolution of openness and oversight.

5.1 Shifting Boundaries and Heightened Complexity

Important debates have emerged within and outside government about the degree to which the implications of the pandemic should be viewed as elements within a shifting mosaic of national security threats, actors and policies, or whether they represent a new overarching paradigm going forward.[8] What seems clear is that as governments seek to foster holistic pandemic responses, horizontal coordination, information and data sharing, and collaboration within and across governments and other sectors become more essential.

The pandemic has had an impact on a range of critical matters such as health intelligence, security of supply chains and border management. Moreover, one of the key themes in the first year of our work has been to encourage a better articulation of the parameters and functioning of the national security community to Canadians. As such, we suggest that understanding how and why the governance of national security is changing is a crucial element of transparency and accountability.

5.2 Cybersecurity and Data Privacy

COVID-19 has accelerated the pre-existing trend of digitization across society. As a result, building secure and resilient infrastructure within and outside the public sector is a critical concern. CSE reports, for example, that the Government of Canada alone is the subject of more than 1.6 billion malicious threats every day. As more Canadians make use of digital service channels, and as more pandemic-related data sources are gathered, analyzed and shared (from mobile applications for contact alerts to the

[8] See for examples:
1. Wesley Wark, “Pandemic Gives Security and Intelligence Community an Urgent New Mission”, Policy Options, April 14 2020. https://policyoptions.irpp.org/magazines/april-2020/pandemic-gives-security-and-intelligence-community-an-urgent-new-mission/.
2. Thomas Juneau and Leah West, “Canada Can Improve Its Multi-Agency Approach to Global Threats”, Policy Options, May 15 2020. https://policyoptions.irpp.org/magazines/may-2020/canada-can-improve-its-multi-agency-approach-to-global-threats/.

emergence of vaccine passports), cybersecurity and data privacy become more closely intertwined with national security.

The pandemic has also brought about a host of new online threats, ranging from misinformation to more targeted conspiracy theories meant to seed domestic unrest and instability, as well as 'dark web' markets for vaccines and other medical supplies. From a transparency perspective, exposing and better explaining such threats can contribute to societal learning and resilience, improving public trust and government capacity for innovation.

Regarding data privacy, the emergence of vaccine passports in many countries raises both new and familiar questions in terms of openness and trust. The State of New York's fledgling and controversial partnership with IBM to deploy blockchain technologies for its own digitized vaccine passport is a case in point, while the UK has undertaken a broad review of the operational and privacy implications of such passports. Whether and how such data sources and mechanisms are used within the national security apparatus further underscores the importance of openness and transparency.

5.3 Oversight and Openness

As has been reported by Canadian media, the pandemic has affected the efforts of new oversight bodies. The National Security and Intelligence Review Agency (NSIRA), for example, has acknowledged facing delays and obstacles.[9] Similarly, the National Security and Intelligence Committee of Parliamentarians (NSICOP) has also faced new hurdles arising from COVID-19.[10]

Such challenges are not unexpected. Given the unprecedented scope of the public health crisis, new oversight bodies may struggle to create organizational systems and recruit skilled workers, while departments and agencies face distractions and potential delays in meeting their nonetheless important oversight obligations. At the same time, we are encouraged that NSIRA intends to broaden its focus to include considerations of the pandemic – committing, for example, to exploring how "the Government of Canada collects intelligence on medical issues or in relation to the health of Canadians."[11]

From the NS-TAG's vantage point, there is an additional risk that if backlogged oversight demands are prioritized over more proactive forms of openness, the necessary impetus for our own proposed reforms might be neglected. As COVID-19 recasts government priorities and operations, it is essential that new and existing oversight and review bodies are equipped to ensure accountability. At the same time,

[9] Catharine Tunney, "National Security Watchdog Says the Pandemic is Slowing its Work", CBC News, March 03 2021. https://www.cbc.ca/news/politics/nsira-staffing-1.5933157.

[10] Canada, National Security and Intelligence Committee of Parliamentarians (NSICOP), *Annual Report 2020,* December 18 2020. https://www.nsicop-cpsnr.ca/reports/rp-2021-04-12-ar/annual_report_2020_public_en.pdf.

[11] Canada, National Security Intelligence Review Agency (NSIRA), *2019 Annual Report*, 2019, p.33. https://nsira-ossnr.ca/wp-content/uploads/2020/12/AR-NSIRA-Eng-Final.pdf (p.33).

political and senior managerial commitments toward embracing transparency as a basis for deeper and more systemic change are equally vital.

Annex A: Defining, Measuring and Institutionalizing National Security Transparency – Sample of Relevant Work from Around the World12

The tables below provide examples of work related or relevant to transparency in national security. There are examples from a national security context as well as other areas where transparency was considered in the organization's initiatives. Please note that this is not an exhaustive list. For instance, countries listed below may have other transparency-related initiatives. The purpose of the information is to serve as a starting point for looking at transparency in national security. It is based on publicly available resources across a few jurisdictions, with supporting examples from international organizations and academic groups.

For the purposes of material to include in this chart, "Transparency" concerned policies, programs, mechanisms or activities that proactively disclose information to citizens, residents or stakeholders. Reactive disclosure systems – such as access to information mechanisms – were covered in annex 5.1 of the NS-TAG first report published in December 2020.

The material is presented as follows:

- Source;
- Scope (what was covered, what was it about, what was done);
- How transparency was defined (or a term closely related to transparency such as accountability, integrity and trust);
- What indicators, measures, parameters, etc. were used or suggested;
- Elements relevant to institutionalizing or hardwiring transparency (or related concept) or on the cultural change process;
- Observations on the material.

Important: This annex and the information contained within was last verified on May 3rd, 2021, and is subject to change in the future. This document will not be updated.

[12] The annexes to this report were written by the National Security Transparency Commitment Secretariat in Public Safety Canada.

A. Canada

Source	Scope	Definition of Transparency	Forms of Measurement	Elements Relevant to Institutionalizing/Hardwiring Transparency	Observations
Government of Canada – National Security Transparency Commitment (NSTC)	The NSTC is about integrating Canada's democratic values into national security activities. Enabling democratic accountability without providing information that could compromise Canada's security or the safety of Canadians. Citizens must know *what* the Government does to protect national security, *how* the government does it, and *why* such work is important.	Six principles of national security transparency are outlined under three action areas: - Information transparency - Executive transparency - Policy transparency	- Work is underway to develop appropriate performance indicators to measure implementation and success. - Public opinion research was conducted to measure, inter alia: the public's level of knowledge on national security issues and threats; knowledge of national security organizations activities; perceptions regarding information from the government on national security; the importance of transparency on various national security topics or challenges, and; the importance of public engagement methods. - Subsequent public opinion research could envision measuring public satisfaction on steps taken to foster dialogue and engage with the public on national security issues, on transparency efforts and initiatives, or the level of agreement on whether the government is transparent with the public on national security issues.	The creation of the NS-TAG (National Security Transparency Advisory Group) serves to advise the DM of PSEPC and the Government of Canada's national security community on how to implement the Commitment. This will be accomplished by advising on the following: - Infusing transparency into Canada's national security apparatus; - Increase public awareness, engagement and access to national security and related intelligence information; - Promoting transparency while ensuring the safety and security of Canadians.	The NSTC is a non legislated initiative, unlike oversight or review mechanisms. The six principles of national security transparency, which are conceptualized under three action areas, target proactively sharing information with the public, explaining decisions and legal considerations, and engaging with the Canadian public and stakeholders.
Canada's 2018-2020 National Action Plan on Open Government	This action plan stems from Canada's commitment to open government as part of the Open Government Partnership. The plan features commitments related to transparency in various realms, including financial and corporate transparency, access to information, digital	N/A	The action plan contains a host of commitments and milestones across the 10 commitments outlined in the report. In terms of measurement, the following questions are used to guide and track the progress of each respective department in regard to achieving transparency:	The existence of commitments at the beginning of each topic serves as a means to institutionalize transparency writ large. An example of this is the "Financial transparency and accountability" section, where commitments are outlined to "improve the transparency of the Government's spending and open contracting" in order to	This example displays the Government of Canada's efforts as part of the Open Government partnership. On a national level, Canada promotes transparency as an important aspect of government. The guiding commitments provide a foundational framework with which transparency initiatives can be analyzed and measured.

	government and services, etc.[13]		What will we do? How we will know we succeeded? What is our deadline?	create an easier understanding of Canada's federal budgets[14]: - Make government budget and spending information easier to find and understand; - Publish an analysis of gender-based impacts for all Budget measures; - Ensure Canadians have access to open data on Government of Canada procurement; - Explore adoption of common contracting data standards across Canada[15].	
Government of Canada - International Approach to Transparency	This source is a guidance note that outlines the Government's approach to encouraging transparency and open dialogue in international assistance.	Transparency is referred to as an environment in which information on the objectives, frameworks, rationale and accountability terms of government policies and programs is provided to the public in a comprehensible, accessible and timely manner.[16]	N/A	N/A	It is mentioned that transparency and open dialogue lead to better policies and services, promote public-sector integrity and help to secure the trust of citizens in public institutions.
Department of Justice – Technical Engagement	The Department of Justice source is a report on a technical engagement with experts about the future of the *Privacy Act,* which is Canada's federal public sector privacy law.	Notes that while transparency is fundamental, it cannot ensure accountability. Accountability is defined as "the acceptance of responsibility (for personal information protection)"[17].	N/A	N/A	While this definition is in the context of privacy, it is a good starting point for a definition of 'transparency' and related matters.
Natural Resources Canada - ESTMA	The Extractive Sector Transparency Measures Act (ESTMA) is an act that requires businesses to publicly report certain payments they	N/A	N/A	*Extractive Sector Transparency Measures Act* (ESTMA) from National Resources Canada was developed through engagement with provinces and territories, civil society, industry and Indigenous representatives.	The ESTMA highlights the importance of stakeholder engagement to build trust in not only government institutions, but

[13] Canada, *Canada's 2018-2020 National Action Plan on Open Government,* 2018. https://www.opengovpartnership.org/wp-content/uploads/2019/01/Canada_Action-Plan_2018-2020_EN.pdf.

[14] Ibid, p.18.

[15] Ibid.

[16] Canada, Global Affairs Canada, *Canada's Approach to Transparency and Open Dialogue in Canadian International Assistance*, 2019. https://www.international.gc.ca/world-monde/assets/pdfs/issues_development-enjeux_developpement/priorities-priorites/FIAP_Guidance3-ENG.pdf.

[17] Canada, Office of the Information and Privacy Commissioner of Alberta et. al., *Getting Accountability Right with a Privacy Management Program*, April 17 2012, p.1. https://www.priv.gc.ca/media/2102/gl_acc_201204_e.pdf.

	make to all levels of government in Canada.[18]				the legislation and initiatives that hold them to account. Having consistent engagement with stakeholders is portrayed as key to achieving transparency and accountability.

B. United States

Source	Scope	Definition of Transparency	Forms of Measurement	Elements Relevant to Institutionalizing/Hardwiring Transparency	Observations
Government Information Quarterly	This report examines the role that transparency plays in enhancing public trust in government, particularly the concept of “latent transparency”. The findings of the report found that the widely held belief of transparency’s positive effects on citizen trust requires a more critical examination.	The concept of transparency was broken down into two different definitions: **Latent transparency**: Defined as the awareness of the right to access government information. The potential of being able to access government information without necessarily intending to or actually accessing the information. **Manifest transparency**: When citizens gain access to actual government documents, data or information. Most literature has focused on this type of transparency.	N/A	Unit inspections (U.S military). Incentivizing the declassification of information by evaluating intelligence units against individual agents, and then rating those units using checklist criteria. E.g. If the transparency team has any classified documents, the team would be judged as a unit on how we adhere to ATIP rules. It makes us all accountable for realizing this goal.	The concept of unit inspections is an example of hardwiring transparency. It places the responsibility of upholding transparency on every team member rather than one person. This can result in a greater commitment to transparency.
What is Transparency?	The importance of public access to government information and the role it plays in a healthy democracy is discussed.	“Transparency .. relates to inputs, outputs and outcomes of decisions”.[19]	A transparent policy is deemed effective when the public acts on the information that the policy provides.	N/A	This source emphasizes the importance of a framework when looking to make transparency actionable. In this example, the “input-output-

[18] Canada, Natural Resources Canada, “Extractive Sector Transparency Measures Act (ESTMA) FAQs”, 2021. https://www.nrcan.gc.ca/mining-materials/estma/18802.
[19] Carolyn Ball, “What Is Transparency?”, Public Integrity 11(4), December 08 2014, p. 293–308. https://doi.org/10.2753/pin1099-9922110400.

	The report offers recommendations that seek to balance these perspectives while ensuring that transparency and accountability remain paramount.		E.g. When an education agency provides information on the quality of schools via performance measurement, and parents choose their child's school based upon this information, the policy is said to be effective. Example: **Input**: An education agency provides information on the quality of schools. **Output**: The education agency creates performance measurement statistics of the schools. **Outcome**: Parents choose schools based upon this information.		outcome" framework provides a base for how transparency could be measured. This framework may be helpful to the discussion of national security and transparency.
Office of the Director of National Intelligence (ODNI) – IC Transparency Implementation Plan	In February 2015, the Director of National Intelligence published the Principles of Intelligence Transparency for the Intelligence Community (IC). The goal of this report is to facilitate intelligence community decisions on making information publicly available while maintaining national security.[20]	N/A	N/A	The IC has put a lot of effort into enhancing transparency in their organizations. Some initiatives of note include: - The ODNI established "IC on the Record" as a repository for declassified documents, official statements, speeches, and testimony. "IC on the Record" has published over 5,000 pages of officially released documents.[21] - The IC publicly supported the passage of the USA FREEDOM Act, which includes additional transparency requirements that the IC will implement.[22] - The IC prepares and publishes two annual statistical reports that highlight the use of key surveillance authorities.[23]	IC on the Record is a tangible example of an activity that aims to enhance transparency and better inform the public.
National Security Agency (NSA) - Report on the Activities of the	The purpose of this report is to inform stakeholders about the NSA's commitment to protecting civil liberties and	N/A	In this report, there are tables that outline the types of reviews, outreach programs and engagement meetings the Office	A full-time Civil Liberties and Privacy Officer was named along with a support office. This office focuses on key civil liberties, privacy and transparency issues, namely those	The existence of an office that oversees transparency in the NSA, along with a report that outlines their activities may be

[20] United States of America, Office of the Director of National Intelligence, *IC Transparency Implementation Plan,* October 27 2015. https://icontherecord.tumblr.com/transparency/implementation-plan-2015.

[21] Ibid.

[22] Ibid.

[23] United States of America, Office of the Director of National Intelligence, "ODNI Releases Annual Intelligence Report Regarding Use of National Security Authorities", April 30 2020. https://www.dni.gov/index.php/newsroom/press-releases/item/2111-odni-releases-annual-intelligence-community-transparency-report..

National Security Agency Civil Liberties & Privacy Officer	privacy. Additionally, it also provides additional transparency about the activities of the Agency.[24]		has held. This serves as a measure to show the public that maintaining civil liberties, addressing privacy concerns and ensuring transparency is paramount in everything the NSA does.	surrounding the capabilities used to conduct NSA activities.	helpful in promoting transparency in national security organizations. Additionally, the existence of a report that tracks the efficiency of the NSA Civil Liberties Privacy Office in delivering its mandate reinforces the importance of being as transparent as possible with the general public.
Transparency at the Department of Homeland Security (DHS)	This page highlights the ongoing transparency initiatives at the Department of Homeland Security (DHS).	N/A	N/A	- In terms of hardwiring transparency, the DHS has outlined several initiatives it is taking to promote or maintain transparency in its department. Some examples include: - A National Cybersecurity Awareness Campaign, which seeks to be transparent and share messaging, resources and recommendations with the public.[25] - Outlining their Declassification of Information policy, in which they are transparent about their document management process.	The DHS Transparency page has a number of initiatives that look to promote transparency in its organization. The explanations given for their respective initiatives help to contextualize how transparency exists in their various spheres of activity.

C. United Kingdom

Source	Scope	Definition of Transparency	Forms of Measurement	Elements Relevant to Institutionalizing/Hardwiring Transparency	Observations
Institute for Government	This report touches upon the importance of accountability in government. Recommendations presented aim to improve accountability across government.	Accountability is defined as a relationship between those responsible for something, and those who have a role in passing judgement on how well that	N/A	Having rigorous complaints and investigation processes that engage high levels of public trust.	Looking at these sources, the literature notes that accountability cannot exist without transparency. Throughout these assessments, there appears to be a trend of having frameworks in place that seek to frame transparency in a tangible manner.

[24] United States of America, Central Security Agency and National Security Agency, *Report on the Activities of the National Security Agency Civil Liberties & Privacy Officer,* 2018, p. 3-4. https://www.nsa.gov/Portals/70/20190910-nsa-civil-liberties-privacy-officer-report.pdf

[25] United States of America, Department of Homeland Security, *Transparency at the Department of Homeland Security,* April 13 2021. https://www.dhs.gov/transparency.

		responsibility has been discharged.[26]			

D. Australia

Source	Scope	Definition of Transparency	Forms of Measurement	Elements Relevant to Institutionalizing/Hardwiring Transparency	Observations
Australian Institute of Company Directors	This report provides detailed descriptions of governance to help not-for-profit boards and directors achieve good governance.	Accountability is defined as existing in a relationship between two parties where one has expectations of the other, and the other party is obliged to provide information about how they have met these expectations.[27] Two components of accountability are discussed: **Answerability** – Providing information and justification for how one's actions align with expectations. **Enforcement** – Being subject to, and accepting the consequences of, failing to meet these expectations. Transparency is defined in this report as organizations that enable others to see and understand how they operate in an honest way. To achieve transparency,	N/A	N/A	The Institute discusses the components of accountability. Due to the fact that accountability involves multiple parties, the source communicates that it is important to clearly define who is accountable to *whom* and *how*. This also allows for a transparent process, as stakeholders are able to understand clearly defined accountability mechanisms.

[26] Benoit Guerin et. al., "Accountability in Modern Government: Recommendations for Change", Institute for Government, April 2018, p.3 https://www.instituteforgovernment.org.uk/sites/default/files/publications/Accountability_modern_government_WEB.pdf

[27] Australian Institute of Company Directors, "Not-for-Profit Governance Principles, Second Edition", January 2019. https://aicd.companydirectors.com.au/-/media/cd2/resources/director-resources/not-for-profit-resources/nfp-principles/pdf/06911-4-adv-nfp-governance-principles-report-a4-v11.ashx.

		an organization must provide information about its activities and governance to stakeholders that is accurate, complete and made available in a timely way. This does not mean all information should be publicly available, as there are certain types of information that must be protected.			
Opening Government: Transparency and Engagement in the Information Age	This source discusses open government, namely transparency and engagement in the information age. It looks at using information to achieve better accountability, building trust through civic engagement, transparency and data management.	N/A	N/A	In 2010, the Australian Government provided three key principles as support for openness and transparency: **Informing**: Strengthening citizen's rights of access to information, establishing a pro-disclosure culture across Australian government agencies, making government information more accessible and usable. **Engaging**: Collaborating with citizens on policy and service delivery to enhance the processes of government and improve the outcomes sought. **Participating**: Making government more consultative and participative.	This framework conceptualizes transparency. It is portrayed as key to hardwiring and measuring transparency, as it also allows the government to be held to account by its citizens.
Australia's International Cyber Engagement Strategy	This document discusses Australia's cyber engagement strategy. Clear goals are outlined to achieve a stable and peaceful online environment.	N/A	N/A	Australia released a host of documents that sought to display a willingness to be transparent to the public. They include the following documents: - 2016 Cyber Security Strategy - 2016 Defence White Paper - the forthcoming Foreign Policy White Paper "Other examples include cyber policy dialogues, sharing the country's national cyber governance structures, and outlining Australia's position on how international law applies to state conduct in cyberspace".[28]	What is of note from this source is the ability to be detailed and precise in how to achieve a specific goal. Australia has outlined specific steps they will take in order to achieve their objectives. When it comes to transparency, measures they have taken in order to provide insight into their activities are listed. They also acknowledge the need for secrecy, and where necessary theystate that they do not discuss specifics.

[28] Commonwealth of Australia, Department of Foreign Affairs and Trade, *Australia's International Cyber Engagement Strategy*, October 2017. https://www.internationalcybertech.gov.au/sites/default/files/2020-11/The%20Strategy.pdf.

E. New Zealand

Source	Scope	Definition of Transparency	Forms of Measurement	Elements Relevant to Institutionalizing/Hardwiring Transparency	Observations
Transparency Reporting Summary Report	This report discusses the value of transparency reporting as a part of upholding the privacy rights of individuals. Namely, looking at law enforcement agencies and how they use their powers to ask agencies for the personal information that they hold.	N/A	N/A	The concept of "transparency reporting". In this context, "transparency reporting is public reporting by companies that hold personal information requested by and disclosed about the information requested by and disclosed to government agencies, usually for law enforcement or national security purposes. The content of transparency reporting may differ between different companies and jurisdictions but the aim is usually the same; to be transparent about what happens with personal information in order to promote accountability and to maintain customers' trust".[29]	The concept of transparency reporting is relevant to the national security realm. The benefits that transparency reporting provides in this context include prompting agencies to ensure that they use their powers in a justifiable way, giving consumers insight into the actions of the companies use of public data and encouraging best practices for handling requests.
2020 New Zealand Security Intelligence Service (NZSIS) Annual Report	The NZSIS Annual Report "details the work the NZSIS has undertaken over the past year to meet the security and intelligence priorities set by Government, and outlines the agency's contribution to the ongoing wellbeing and security of New Zealand."[30]	N/A	Information requests are used as a form of measurement for transparency, namely the amount that is completed per year. The New Zealand Security Intelligence Service tracks this as a way to show that they are committed to being as transparent as possible with the public.	N/A	N/A
New Zealand Intelligence and Security Bill 2016	The NZ Parliament created the New Zealand Intelligence and Security Bill 2016, which was designed to update the legislative framework and improve the transparency of New Zealand's intelligence and security agencies.	N/A	N/A	The New Zealand Security Intelligence Service believes that having robust compliance processes is key to maintaining the trust of the public. As such, compliance frameworks are run (through a series of audits and reviews) to ensure that staff are compliant with New Zealand law. This is also important in installing and maintaining a culture of self reporting compliance incidents.[31]	A notable takeaway from the New Zealand Intelligence and Security Bill is that it standardizes the expectations of transparency for all national security agencies. This makes for a clearer understanding across agencies in terms of accountability to the public.
Accountability and Public Governance in New Zealand	This paper provides insight relating to accountability and public governance. Various definitions of accountability were	It is acknowledged that accountability has many definitions. The definitions have	N/A	N/A	The definitions of accountability help to explain the term.

[29] New Zealand, Office of the Privacy Commissioner, *Transparency Reporting Summary Report*, 2017. https://www.privacy.org.nz/assets/Files/Reports/Transparency-Reporting-Cover-Report-for-public-release-Oct-2017.pdf.

[30] New Zealand, New Zealand Security Intelligence Service, *Annual Reports*, October 30 2017. https://www.nzsis.govt.nz/resources/annual-reports/https://www.nzsis.govt.nz/resources/annual-reports/.

[31] New Zealand, New Zealand Security Intelligence Service, *2020 Annual Report*, 2020 p. 49-50. https://www.nzsis.govt.nz/resources/annual-reports/.

	discussed as well as the way it manifests itself in different contexts.	established that accountability involves the following: “A relationship where an individual/agency is held to answer for performance that involves some delegation to act.”[32] A framework where there is an actor (a government agency) and a forum (the public), where the actor has an obligation to explain their conduct, and the forum can pose questions, pass judgement and impose penalties on the actor.[33]			Elements of these definitions could be helpful in discussions on implementing transparency across national security departments.

F. International Organizations, Think-Tanks, Academic Research and Other Jurisdictions

Source	Scope	Definition of Transparency	Forms of Measurement	Elements Relevant to Institutionalizing/Hardwiring Transparency	Observations
Measuring Local Government Transparency - Portugal	This paper developed a municipal transparency index (MTI) based on information available on the websites of local government officials.[34]	Defined transparency as “the publicity of all the acts of government and its representatives to provide civil society with relevant information in a complete, timely, and easily accessible manner.”[35]	The role of information and communication technology (ICT) in improving transparency and accountability on website transparency was gauged by 25 items divided into 6 categories[36]:	N/A	This can serve as a guide when measuring transparency across NS departments. Based on this source, it appears that this group created their own transparency measures because existing/available

[32] Rodney Dormer and Sarah Ward, “Accountability and Public Governance in New Zealand”, 2018, p.7. https://researcharchive.vuw.ac.nz/xmlui/bitstream/handle/10063/7002/paper.pdf?sequence=1.

[33] Ibid, p. 8

“A Municipal Transparency Index (MTI) was based on a participatory method to determine the dimensions and indicators of transparency, to select the metrics and to compute their weights. This stakeholder-based method avoids the reliance on purely legal/formal indicators and produces an index that can be employed as a benchmarking tool. In addition, an index based on stakeholders’ opinions constitutes a form of collaboration to improve transparency and accountability that is believed to increase social capital and foster a culture of inclusiveness and diversity in local communities that facilitates participation”. Nuno Ferreira da Cruz et. al., “Measuring Local Government Transparency”, Public Management Review, 18:6, 2015, p. 866-893.

[35] Ibid.

[36] Ibid.

			- Ownership and content update (website updates) - Contact information - Information about the internal organization - Specific contents including laws, reports and publications - Explanations and instructions to citizens - Security and privacy statements These are examples of indicators that were developed when evaluating transparency on municipal government websites.		sources failed to adequately define and measure transparency. They suggest using stakeholder participation to help produce these transparency indicators. The collaboration underlines the transparency of the process and helps build public confidence in these forms of measurement.
NATO: Building Integrity in Operations	The purpose of this handbook is to raise awareness of the risks and impact of corruption associated with a military mission. Additionally, this report strives to act as a tool to support integrity efforts including good governance, transparency, accountability and integrity across NATO operations.	Transparency is defined as "a situation where business and financial activities are done in an open way without secrets, so that people can trust that they are fair and honest".[37]	N/A	N/A	In this definition of transparency, "activities are done in an open way without secrets". While this can be antithetical to the nature of some national security work, it insists that it is important to be transparent about why certain information cannot be made public.
Building Integrity and Reducing Corruption in Defence Compendium	This compendium discusses integrity in the defence sector. It discusses best practices for integrity building, as well as the role of government and other important stakeholders in implementing integrity building programs.	Accountability was defined as holders of public office being responsible to the public for their decisions and actions, as well as subject to scrutiny.[38] Integrity is defined in two ways. In a technical sense, it means that a system is fully functional and intact. In a moral sense, integrity refers to the consistency of actions, values, principles and outcomes.[39]	N/A	N/A	These definitions shed light on the fact that maintaining integrity is not only an organizational goal, but also has a moral element as well. This speaks to the importance of culture change when attempting to embed transparency in organizations.

[37] North Atlantic Treaty Organization, *Building Integrity in Operations Handbook,* 2020, p.42. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/6/pdf/200608-bi-handbook.PDF.

[38] North Atlantic Treaty Organization, *Building Integrity and Reducing Corruption in Defence: A Compendium of Best Practices*, 2010, p. 165. https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/20120607_BI_Compendium_EN.pdf.

[39] Ibid, p. 166.

Ministry of Justice – (Italy)	This source discusses Italy's 2016 Open Government partnership commitment to improve transparency in its penitentiary system.	N/A	N/A	To improve transparency in its prison system, the Italian Ministry of Justice began disclosing the "transparency sheets" of its 190 penitentiary institutions on a new portal. Each transparency sheet includes information on the following: - The institution's structure - Prison capacity - Physical characteristics - Policies around work, visitation, and other aspects of prison life.	The transparency sheet looks to be a central register of sorts. This could serve as a model for the NS-TAG to build upon. An example would be our national security institutions updating the public on certain initiatives they are working on.
The Transparency and Accountability Initiative (India)	This source provides concrete examples of balancing the need for transparency with the public, while acknowledging the importance of secrecy in national security departments.	N/A	N/A	Recommends that states should establish independent and adequately resourced bodies that are able to review the decisions of security sector agencies when it comes to withholding information.[40] An example cited is India's Right to Information Act, 2005. This Act applies to a wide range of India's national security apparatus; it allows for national security agencies to be exempted from the law, however Parliament can debate any exclusion and force the government to withdraw it.	The example of India's Right to Information Act is used to show that these two principles can co-exist, rather than be at odds with each other.
Transparency International – CPI Perceptions Index FAQ	This source is a primer on the Corruption Perceptions Index (CPI) index. It answers commonly asked questions about the metric and goes into detail about its limitations.	The CPI is assembled by Transparency International, which is a leading non-profit organization that works to combat global corruption.[41] The specific components of corruption the CPI measures include ability of governments to enforce effective integrity mechanisms in the public sector, legal protections for journalists, whistleblowers, investigators; and access	N/A	The CPI is generally regarded as a "valuable governance indicator". It should be noted that while "researchers from academic, civil society and governments have made advances in terms of objective corruption measurement", to date there is no objective standard.[42]	Outside of the CPI, existing literature notes that transparency is difficult to measure. There are common principles surrounding transparency in general, however the term is measured according to a specific industry/company's environment. Common principles may be helpful in developing metrics for measuring transparency in the national security environment.

[40] Transparency and Accountability Initiative, *National Security Transparency and Accountability*, 2011, p. 2. http://www.transparency-initiative.org/archive/wp-content/uploads/2011/09/14-National-security1.pdf.

[41]Transparency International, "Corruption Perceptions Index 2020: Frequently Asked Questions", 2020. https://images.transparencycdn.org/images/2020_CPI_FAQs_ENv2.pdf.

[42] Ibid.

		of civil society to information on public affairs.			
Open Government: Beyond Static Measures	This source suggests new indicators that can be used to assess the openness of government. It argued that existing indicators are binary in nature; focusing on the presence of key laws/institutions, or on the public's perceptions of government performance.[43]	N/A	The Open Government report "introduces new indicators which the author suggests should be added alongside existing measures of government openness. These existing indicators include: the presence of key laws and institutions, and citizens' perceptions of government performance". New indicators are proposed in this piece, which are intended to compliment the aforementioned methods. They are grouped as follows: - Indicators relating to law on Access to information and documents, - Ombudsman/Information Commissioner Institutions, - Supreme Audit institutions, and - Consultation policies. For purposes of this research, the indicators relating to consultation policies are most relevant. An example of this framework in action is as follows: **Suggested indicator**: Public bodies are required to consult with citizens or other stakeholders in decision making. **Sub-indicators:** a) Does the scope of the policy cover all organizations and institutions delivering services to the public? b) Are public bodies required to publish an official response at the end of a consultation exercise?	N/A	The indicators of consultation policies and the questions asked are highlighted as important to note. Frameworks help to take abstract ideas (e.g. transparency) and turn them into actionable items (e.g. creating standards with input from all national security entities that will institutionalize transparency long term).

[43] Karin Gavelin et. al., "Open Government: Beyond Static Measures", Involve for the OECD, 2009. https://www.oecd.org/mwg-internal/de5fs23hu73ds/progress?id=uMz1_4vF5Hiy0xi1w3XzxoADmd8R4hYUacioeNlV9O8.

			Follow-On Question to sub-indicator a): If no: what organizations and institutions are exempt from the law?[44]		
University of Amsterdam	This source discusses surveillance by intelligence services from the perspective of oversight and transparency. Ten standards are provided as practical guidance for the policy arena surrounding the issue of transparency in national security.	N/A	N/A	There are a few relevant recommendations that would be helpful to hardwiring transparency. **Standard 8**: Intelligence services and their oversight bodies should provide layered transparency. Example: a) All stakeholders should be informed (individual, oversight bodies, civil society). b) Adequate level of openness about intelligence services prior to and after the fact. c) Information about what will remain secret under all circumstances should be provided. **Standard 9**: Oversight bodies, civil society and individuals should be able to receive and access information about surveillance. **Standard 10**: Companies and other private legal entities should be able to publish aggregate information on surveillance orders they receive.	The standards discussed here display how intricate transparency can be embedded in organizations. Transparency goes beyond a definition; actionable items work to achieve the overarching goal of transparency in national security.
GUARD//INT Research Project	The GUARD//INT initiative is a European research project that examines surveillance, intelligence and oversight. The main goal of this project is to build empirical and conceptual tools to better understand the limits and potential of intelligence oversight mechanisms.[45]	N/A	N/A	This website is a publicly accessible and open-source archive that holds legal documents, oversight reports, court decisions and regulatory frameworks. It currently has information on France, Germany and the UK.	This project is an example of an open access repository that is transparent. It compiles documents from various countries into one spot, which is very accessible to the public.

[44] Ibid, p. 4.

[45] GUARD//INT Surveillance Oversight Database. 2021. https://guardint.org/

Annex B: NS-TAG Meeting Highlights, October 2020 – April 2021

Regular Meeting – October 7, 2020, Virtual

Theme/Topic: "Transparency by Design: Definition, Evaluation and Institutionalization of National Security Transparency – Part One: Open Government"

Highlights:

- Discussion with guests on the concept of open government: metrics considerations; institutionalization and change; the scope and end goal of transparency and the drivers behind current Government of Canada efforts; and fundamental questions that should be addressed when attempting to achieve "transparency by design."
- Internal discussion on the completion and publication of the NS-TAG first report.

The full summary is available online.

Regular Meeting – November 4, 2020, Virtual

Theme/Topic: "Transparency by Design: Definition, Evaluation and Institutionalization of National Security Transparency – Part Two: The United States' Experience"

Highlights:

- The discussion with guests focused on the work being done at the United States' Office of Civil Liberties, Privacy and Transparency, within the Office of the Director of National Intelligence. Members and guests discussed the fundamental goals of transparency and why it is important, both for national security institutions and for the public, and how to approach it as a good business practice. They also shared considerations for institutionalizing and measuring transparency, and outlined a number of transparency initiatives led by the Office that had widespread implications across the United States' national security and intelligence community.
- Discussion and adoption of amendments to the NS-TAG's Terms of Reference. Members re-appointed the non-governmental co-chair for a second one-year term.
- Update and discussion on the production and release of the NS-TAG's first report, including on raising public awareness on the report.

The full summary is available online.

Special Meeting – December 14, 2020, Virtual

Theme/Topic: Discussion with the Director of the Canadian Security Intelligence Service

Highlights:

- The NS-TAG welcomed the Director of the Canadian Security Intelligence Service (CSIS) and the Deputy Director of Policy and Strategic Partnerships. Opening remarks and responses to members' questions covered a number of topics including: community engagement, diversity and inclusion in the workplace, new terminology for violent extremism, datasets, and review and accountability.

The full summary is available online.

Regular Meeting – January 20, 2021, Virtual

Theme/Topic: "Transparency by Design: Definition, Evaluation and Institutionalization of National Security Transparency – Part Three"

Highlights:

- The discussion session with guests focused on how to build transparency in organizations, how to improve access to information, and the relationship between accountability, integrity and transparency.
- Members discussed outreach activities they conducted following the publication of the Group's initial report in late 2020. This included two outreach video sessions on January 14, interviews with social media, and written media publications.
- The Group also discussed programming for upcoming meetings and when the Group will move to the next theme.

The full summary is available online.

Regular Meeting – February 17, 2021, Virtual

Theme/Topic: "Transparency by Design: Definition, Evaluation and Institutionalization of National Security Transparency – Part Four"

Highlights:

- The discussion session with guests focused on: access to information, the duty of candor, digital technologies and data, culture change and challenges related to measurement and key indicators, as well as some of the areas where transparency could be improved.
- Members discussed the approach to their second report and its outline.

The full summary is available online.

Regular Meeting – March 17, 2021, Virtual

Theme/Topic: "Transparency by Design: Definition, Evaluation and Institutionalization of National Security Transparency – Part Five"

Highlights:

- The discussion with guests was centered on the Communications Security Establishment's – including the Canadian Centre for Cyber Security – mission, key principles, and transformation in recent years. In particular, members discussed the progress CSE has made in terms of transparency, including several examples of concrete outreach and engagement initiatives they have put in place.
- The Transparency Secretariat provided an update on the National Security Transparency Commitment's implementation across departments and agencies and presented the preliminary results of recent public opinion research on national security transparency and information sharing, the final report of which will be made public.
- Members discussed the current draft of their second report and members' respective involvement in writing the next draft.

The full summary is available online.

Regular Meeting – April 21, 2021, Virtual

Theme/Topic: "Transparency by Design: Definition, Evaluation and Institutionalization of National Security Transparency – Part Six"

Highlights:

- To conclude discussions on the current theme, members and guests exchanged views on: overclassification and why it happens, measures to prevent the overclassification of documents, the importance of accountability and culture change, selected European projects on digital rights, surveillance and democracy, and challenges and limits of transparency.
- Internal discussion on the current draft of the Group's second report and the timeline for publication.

The full summary is available online.