Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Security Intelligence
Review Committee

Comité de surveillance des activités
de renseignement de sécurité

Office of the Chairman

Bureau du président

**TOP SECRET // CEO**

File No.: 2800-229

January 17, 2018

The Honourable Ralph Goodale, P.C.
Minister of Public Safety and Emergency Preparedness
269 Laurier Avenue West
Ottawa, Ontario K1A 0P8

Dear Mr. Goodale,

**Re: SIRC Review of CSIS's Response to the Federal Court Decision (Section 54 SIRC Study — 2017-10)**

This letter summarizes the first of two reports of the Security Intelligence Review Committee (SIRC) to evaluate the response of the Canadian Security Intelligence Service (CSIS) to the Federal Court decision of October 4, 2016. In its decision, the Federal Court found that while CSIS may collect non-threat-related information incidentally, its mandate does not allow it to retain data (including metadata) in bulk without assessment.

The full details of the first part of the review, related to non-warranted bulk datasets, are provided in Annex A. SIRC's assessment of CSIS's response to the decision in relation to warranted bulk datasets will be reported separately in March 2018.

In assessing the decision's implications for the collection and retention of bulk datasets acquired without a warrant, SIRC was mindful of the significant amendments to CSIS's collection authorities proposed by Bill C-59. However, if the *CSIS Act* remains unchanged, SIRC is concerned that the continued collection, retention, and exploitation of these datasets risks exceeding CSIS's lawful authority. This concern heightens when assessed against the conclusion of the *en banc* decision on the scope and limitations of section 12 of the *CSIS Act*. SIRC advises that, at a minimum, CSIS should seek your direction as to how to proceed with respect to mitigating legal risk until uncertainty regarding a potential new regime under Bill C-59 is resolved.

ATIP version
dated: JUN 0 8 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

Additionally, **SIRC recommends that:**

1. **CSIS continue to prioritize the implementation of a robust process for assessing the privacy impacts and legal risk associated with its datasets, particularly with respect to Canadians;**
2. **CSIS develop a system for assessing the utility of individual datasets, and that decisions regarding the continued retention of datasets should be informed by those assessments;**
3. **CSIS implement as soon as practicable a data control system in its operational database that can account for the provenance and access controls on each piece of reported data; and**
4. **CSIS develop a strategic approach to data collection and analysis across the organization, including with respect to data governance, performance measurement, and the integration of data analysis with investigations.**

Moreover, it is SIRC's view that operational utility is a key element of any assessment of the collection and retention of bulk datasets, whether with respect to the threshold of "strictly necessary," as required under the current wording of the *CSIS Act*, or the lower retention threshold of "likely to assist" proposed in Bill C-59. SIRC's report on bulk datasets assesses the operational outcomes achieved from the exploitation of the datasets and the management of the datasets, including how CSIS dealt with the legal risk emanating from the *en banc* decision.

Overall, SIRC has seen that CSIS does not currently have a system in place to assess the utility of its dataset holdings and thus was not able to clearly demonstrate to SIRC the utility of these datasets in terms of lead generation or the advancement of investigations. CSIS needs to grapple with the challenges raised by "Big Data" analytics programs with respect to privacy, governance, and measurement. It is lagging its primary foreign and domestic partners in this respect, a fact that CSIS acknowledges. By contrast, SIRC has observed a practice of CSIS collecting and retaining bulk personal datasets without a satisfactory assessment of the contents and utility of the data itself.

SIRC acknowledges CSIS's efforts to institute changes to its bulk data acquisition processes in response to SIRC's review on Data Management and Exploitation (2015-02). However, SIRC is not satisfied that the datasets have been properly assessed with respect to legal risk, including the implications of the *en banc* decision with respect to the collection and retention of non-threat- and third-party-related information.

In at least one case, SIRC assesses that CSIS has collected records with a Canadian nexus since 2010

ATIP version
JUN 0 8 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

CSIS nevertheless continues to collect this data. As the activity has been assessed as more likely than not to violate the Charter, SIRC believes that the continued collection of this dataset without a warrant is unreasonable.

Regarding the new powers proposed by C-59, SIRC finds that CSIS's data analysis function is not yet ready to operate in compliance with the requirements of this regime. However, SIRC acknowledges that work is underway at CSIS to prepare for the requirements of the new dataset regime. If the *CSIS Act* is amended to lower the legal thresholds for collection and retention of this type of data, SIRC suggests that ministerial direction should be provided, as it is for other operational areas.

Sincerely,

Pierre Blais

Pierre Blais, P.C.
Chair

c.c.:

David Vigneault, Director of CSIS

DG/

ATIP version
dated: JUN 0 8 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

## ANNEX A

1. Introduction

### Purpose and scope of the review

In October 2016, the Federal Court issued an *en banc* decision that highlighted limitations on the mandate of the Canadian Security Intelligence Service (CSIS). The Federal Court found that the third-party, non-threat-related metadata retained by CSIS had been retained illegally. SIRC believes that the decision's findings have implications for both warranted and non-warranted data collection, in particular, by the Operational Data Analysis Centre (ODAC) and encompassing all of CSIS's collection and retention practices and demanding a broad response from CSIS.

Following the decision, the Minister of Public Safety and Emergency Preparedness asked the Security Intelligence Review Committee (SIRC), under section 54 of the *CSIS Act*, if SIRC could prepare a special report on CSIS's response to this decision. SIRC accepted the request. Because of the reach of the *en banc* decision with respect to CSIS operations, SIRC will prepare two reports to fulfill the request. In this report, SIRC will assess the retention and management of non-warranted bulk personal datasets. In a March 2018 report, SIRC will assess CSIS's ongoing efforts to identify and destroy non-threat-related data collected under warrant.

In its decision, the Court indicated that the limitation imposed by "strictly necessary" in section 12 of the *CSIS Act,* read in the context of the definition of threats to the security of Canada in section 2, "shows that legitimate activities ... are specifically excluded from the ambit of the Service."[1] As a result, the Court concluded that "incidental collection of non-target and non-threat related information does not form part of what is 'strictly necessary' to collect."[2]

This conclusion led SIRC to assess the retention and management of non-warranted bulk personal datasets through the lens of operational utility, even with the possibility of change in CSIS's legislative authorities. It is SIRC's view that utility is a key element of any assessment of the collection and retention of datasets, whether that assessment is of the "strictly necessary" threshold required under the current *Act,* or the "likely to assist" threshold envisioned by Bill C-59.

This approach will allow the Minister to assess not only how CSIS is managing the legal risk of collecting, retaining and exploiting these datasets following the *en banc* decision, but also the operational utility achieved by the program since its inception in 2006. The review does not cover CSIS's exploitation of its warranted metadata. However, SIRC's assessment is that, based on the cases reviewed, the datasets derived from warranted metadata provided demonstrable value to investigations.

[1] Decision in *Re X* (2016), p. 94, para. 183.

[2] Decision in *Re X* (2016), p. 94, para. 186.

ATIP version
JUN 0 8 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

This review covers the entire period of ODAC's operation, from 2006 to 2017.

the review was limited to activities that fall within the scope of the decision — activities performed in support of investigations into threats to the security of Canada that involved datasets collected under the authority of section 12.

Among Canada's close allies, all are engaged in bulk collection and exploitation activities. In the US and the UK, as well as other jurisdictions, the utility in bulk collection for intelligence purposes has been extensively evaluated and discussed publicly. Reviews of this question in the UK and US in particular reached divergent conclusions on the question of utility. This lack of consensus illustrates the important point that utility of bulk collection is heavily dependent on the nature of the datasets, the use to which they are put, as well as the threat environment.

2. Methodology

### Assessment of utility

To evaluate the outcomes of the data exploitation program with respect to utility, SIRC asked CSIS for a range of statistics regarding the use of non-warranted datasets, as well as examples of the value brought to investigations by these datasets. CSIS was not able to deliver statistics relating to use or utility of datasets.

Absent a detailed profile of the use of the datasets, SIRC looked at similar evaluations done elsewhere, including David Anderson, whose methodology was based on an analysis of case studies. Similarly, SIRC approached the question of utility by evaluating case studies illustrating the best outcomes across operational areas and datasets, including warranted metadata and bulk datasets acquired without a warrant. Some were identified by CSIS as representing good examples of operational utility,[3] and others were chosen by SIRC. Thirty-three cases were studied in detail. The selection of cases was not intended to be statistically representative; rather, cases were chosen in order to highlight the best results of the program, as well as to represent the diversity of data sources and activities. SIRC evaluated the outcomes of the cases against operational objectives, as discussed below. Throughout the review, SIRC consulted CSIS for additional details and insight to ensure the full context was taken into account.

Evaluating the utility of any intelligence activity is complex, as it is generally an ongoing process to which a wide variety of sources and methods may contribute. In evaluating the selected cases, SIRC looked at the results in the full investigative context, in order to understand how the course of the investigation might have been affected without the data exploitation output.

The assessment of utility in each case was informed by the framework developed by SIRC and discussed below. This framework was shared with CSIS for general comment.

[3] Included among these are the cases that CSIS highlighted as examples of the operational utility of warranted metadata before the *en banc* sitting of the Federal Court.

ATIP version
JUN 0 8 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

The framework was also shared with the operational branches associated with each case, along with a list of general and specific questions that they were asked to complete. These written answers, presented in a standard format, assisted SIRC in its evaluation of the utility of each case and facilitated comparison across cases. The best outcomes associated with each case were selected.

### Framework for assessment against operational objectives

Data exploitation is used primarily for two functions within CSIS: 1) lead generation and analysis and 2) enrichment of information on subjects of interest. The evaluation of utility in this review follows the framework laid out in Table 1.

Lead generation is difficult to measure. Since a lead often starts as an insignificant seed of information, it is easy to conceive of virtually any type of information generating a lead, defined as a piece of information that generates further inquiries, which may or may not be productive. In order to come to concrete conclusions regarding utility, SIRC examined cases in which leads stemming from datasets or data exploitation were followed or leads from other sources were triaged using bulk datasets, as well as the outcomes of the intelligence processes.

The second function, enriching target information, is more straightforward. When an individual comes to CSIS's attention, operational personnel attempt to put together as much information as possible as quickly as possible, in order to understand if the activities of the individual pose a threat to the security of Canada.

| **Overall outcome** | **Lead generation** | **Enrichment of information on target** |
|---|---|---|
| Some impact on investigation | Subject of interest identified (or ruled out) | Basic information on target identified (e.g., additional selectors) |
| Significant impact on investigation | New target identified | Important information on target identified |
| Major impact on investigation | New high-priority target identified (e.g., identification of a person of interest who poses an active threat to Canadians) | Critical information on target identified (e.g., indicators that led to the discovery of an active threat to Canadians) |

**Table 1. Utility framework**

ATIP version
dated: JUN 0 8 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

SIRC's assessment of the impact on investigations of ODAC's data exploitation activities was informed by assessments from CSIS operational personnel, as well consideration of the incremental utility added to the existing intelligence picture. SIRC assessed the incremental utility achieved by considering three sources of intelligence: 1) that derived from traditional intelligence sources or activities (e.g., warranted intercepts and human sources), 2) that derived from analysis of historical warranted metadata, and 3) that derived from non-warranted bulk personal datasets. To understand the process and outcomes, SIRC reviewed operational reports and received written and oral briefings from analytic areas, regional operational desks, and operational branches at headquarters. In total, responses were received from all operational areas[4] and all six regions.

SIRC considered an intelligence product to have a *major impact* on the investigation if it resulted in the discovery of new activities that represent a threat to the security of Canada; a *significant impact* if it resulted in additional insight into activities that pose a threat to the security of Canada, and *some impact* if additional information (e.g., selectors) was gained but did not provide additional insights into such activities. In general, CSIS's assessments with respect to the impact on investigations concurred with SIRC's.

With respect to proportionality, SIRC remained mindful of the need for collection of this type to be balanced against alternate means of accomplishing the intelligence objective, as well as the potential for intruding on the privacy rights of substantial numbers of people, the great majority of whom have no association with a threat to national security.

**Overall management of the program**

To fully understand the use and stewardship of the datasets, SIRC examined the detailed workings of the program, from strategic objectives to the activities and technical systems employed. SIRC reviewed corporate documentation on the rationale for collection and assessment with respect to privacy interests engaged and legal risk for all datasets whose ingestion had been approved by July 2017. SIRC also examined the contents of the datasets through direct access to data repositories. Given the lack of statistics on the use of datasets, SIRC searched the operational database to produce a rough count of uses of individual datasets. With respect to legal risk, SIRC examined the evaluation process for the datasets in the context of the *en banc* decision, as well as what legal advice was sought and decisions were made based on this advice.

3. Assessment of utility

Consistent with previous studies,[5] SIRC found that information on capabilities and intent of subjects of investigation invariably came from reporting from traditional sources,

[4]

[5] For discussion of the comparative value of different sources of intelligence in counterterrorism investigations, see P. Bergen, D. Sterman, E. Schneider, B. and Cahall, *Do NSA's Bulk Surveillance Programs Stop Terrorists?*, New America Foundation, 2014; and E. Dahl, *Intelligence and Surprise Attack*, Georgetown University Press, 2013.

ATIP version
JUN 0 8 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

including warranted data (including content), human sources,[6] and foreign and domestic partners (based on similar sources). These sources also generated the majority of high-quality leads and served to corroborate or rule out conclusions arrived at based on data exploitation alone. This is a consequence of the low information content of metadata and other datasets, which lack the context provided by more robust sources of information, such as human sources and the content of communications. However, SIRC acknowledges that reporting on the content of communications is limited by the ability of human analysts to process the data, and that the use of data analytics could improve the efficiency of processing this information.

Bulk personal datasets

To identify cases from these datasets in which value was obtained, SIRC searched the operational database for cases in which these datasets were used.[7] SIRC also relied on successful cases of data exploitation identified by CSIS itself. Of the datasets surveyed, the only ones with an exploitable Canadian nexus that generated a significant number of hits were Of the datasets without an exploitable Canadian nexus, only [8] generated a large number of hits, while a few of the others (e.g., generated one or two.

SIRC could find no references to the remaining datasets in the operational database. Although an imperfect measure, inclusion in operational reporting was the best available indicator of use of the datasets.

SIRC reviewed in detail 20 cases in which bulk personal datasets were exploited. In addition, SIRC discussed the utility of certain specific datasets more broadly with operational desks at headquarters. SIRC was able to confirm for only one dataset that results with a significant impact on an investigation had been obtained. In all cases but one, SIRC's assessment agreed with the information provided in writing by CSIS.

### *Category One: Datasets with no exploitable Canadian nexus*

Datasets with no exploitable Canadian nexus are collected in the hopes of quickly attributing real-world identities based on selectors. SIRC reviewed five cases in which such datasets were used and also participated in more general discussions with CSIS regarding some datasets. With one exception, CSIS was not able to demonstrate that these datasets provide significant value in the Canadian security intelligence context.

One type of non-warranted dataset stood out in terms of adding significant value to an investigation. Several datasets from contain indicators that can reliably be linked

[6] Here, the term human sources includes tips and casual interviews, in addition to directed human sources.

[7] For the purposes of evaluating utility, datasets containing data already assessed to be threat-related by a domestic partner were not examined.

[8] As it is referred to in the operational database as the results could not be disaggregated.

ATIP version
JUN 0 8 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

In combination with other sources of intelligence, these datasets provided clear investigative benefit in terms of generating leads This dataset has been used on a regular basis for this purpose, No cases that significantly advanced investigations were identified by CSIS from the bulk of .

The other datasets examined generally yielded minor enrichments of intelligence that had come up in the course of investigations. These results could be said to increase situational awareness in terms of CSIS's but there was no clear evidence of a concrete operational impact beyond this.

As noted, in all but one of the cases discussed above, SIRC's assessment that there was no significant impact on the investigations in question is reflected in CSIS's written answers. In the disputed case, CSIS indicated that the intelligence provided insight SIRC assessed that given what was known the additional information did not significantly advance the investigation.

***Category Two: Datasets with an exploitable Canadian nexus***

The dataset was queried on a regular basis in order to identify a Canadian nexus to or to find information relevant to In the cases in which leads were generated, no discernible impact on investigations was achieved. In cases where the dataset was queried some information was generated (e.g., ); however, it was not clear that there was a significant impact to the investigation beyond what was available from other sources.

Datasets relating to also have a potentially exploitable Canadian nexus, , although the majority of the data appears to relate to CSIS has used a variety of techniques to exploit these datasets, SIRC reviewed 10 cases covering the full spectrum of analytical activity. In all of these cases, the leads did not find good uptake with operational desks and did not lead to any discernible operational result.

SIRC also reviewed the results of While these were pilot projects they illustrate a potential use for non-threat-related datasets with a strong Canadian nexus. Anonymized versions of the dataset were used for statistical investigations, and leads were also generated. These were investigated, but did not lead to any significant investigative outcome. SIRC also notes that these pilots illustrate how access to relevant datasets can be secured without the bulk ingestion of data by CSIS.

ATIP version
dated: JUN 0 8 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

While datasets with an exploitable Canadian nexus are prized by CSIS due to the possibility of generating leads, there was no evidence that the nexus to threats is strong enough for them to deliver significant utility in terms of lead generation. This issue was exacerbated by poor data quality.

This issue was encountered in the review of the cases discussed above. For example, in one case, CSIS headquarters indicated that a lead generation activity using the dataset had identified However, a review of relevant operational reports revealed that further investigation by the region had discovered that this was a case of mistaken identification.[10]

4. Findings with respect to the management of the datasets

### Assessment of the datasets

In response to SIRC's review of Data Management and Exploitation (2015-02), CSIS promulgated a new policy and procedure governing the collection and management of datasets in August 2016.[12] This policy defined a new category of "discoverable datasets," along with procedures to follow for identification, collection, and exploitation. Discoverable datasets are defined as those in which "the majority of the information contained may not, in and of itself, be directly or immediately indicative of threat-related behaviour, or directly linked to an individual target." In plain language, these are datasets containing records of generally legitimate activities, some fraction of which may relate to threats.

CSIS's policy was developed

CSIS, by virtue of its decision to continue ingesting bulk datasets, chose to accept this risk. In SIRC's view, this legal risk

[10]

[12] CSIS policy documents *Governing Policy: Conduct of Operations* (305-12-1) and *Governing Procedure: Collection and Management of Discoverable Datasets*

ATIP version
dated: JUN 0 8 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

likely reached the level of "high" once the Federal Court delineated a "strictly necessary" test that defines "strictly necessary" in terms of information that is directly related to a specific target.

The procedure that CSIS developed
provided that each dataset is to be evaluated against operational objectives and potential privacy interests of the dataset, including the presence of Canadians, in order to determine if collection is "strictly necessary" and to identify potential risk with respect to the *Canadian Charter of Rights and Freedoms*.

SIRC reviewed a list of discoverable datasets
From the standpoint of utility, the bulk personal datasets fall into two categories: those with an exploitable Canadian nexus, and those without. While any or all of the datasets may have Canadian content, only some are expected to have recognizably Canadian identifying information

In reviewing a list of the approved dataset authorization forms, SIRC found a number of problems with the process. First, the question of whether the intelligence gained from the dataset could be acquired through a smaller subset of the data is not satisfactorily addressed. Most of the forms discuss only whether it is feasible to *acquire* a smaller subset at the point of collection, rather than whether a smaller subset could be *retained* and exploited in order to satisfy the same intelligence objectives. In most cases, the acquisition and retention of a bulk dataset pertaining to a given country is justified based on intelligence objectives relating to the presence of terrorist groups in that country or region.

Second, indicated "unable to identify" whether the dataset contained data on Canadians. SIRC acknowledges that it can be a challenge to identify the precise number of Canadians contained in any given dataset. However, it is important to properly assess which datasets contain information on Canadians in order to characterize the privacy interests engaged. SIRC was, through a quick search, able to identify fields indicating a nexus to Canada in a number of these datasets flagged as "unable to identify."

Third, the assessment of privacy considerations in the majority of the authorization forms is inconsistent and, in most cases, minimal. Most indicate that there are no privacy considerations,

SIRC understands that the dataset regime proposed in Bill C-59 was likely drafted to respond to the *en banc* decision. It is concerning, however, that in the intermediate term, SIRC has seen no evidence that CSIS has, in any way, changed its policies and procedures with respect to the collection of discoverable datasets in the wake of a Federal Court decision that clearly had implications for this practice. In the context of the *en banc* decision, therefore, SIRC finds that CSIS has not adequately addressed the privacy interests and legal risk involved in the collection of bulk datasets, including with respect

ATIP version
JUN 0 8 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

to the volume of Canadian information contained in them. As a consequence, CSIS is running a substantial risk of having datasets that contain sensitive information about Canadians that are not subject to proper protections and that may not have been collected under the proper legal authority.

SIRC examined the case of in particular detail, as it represents an important illustration of the process failures on a number of levels. The dataset contains records

CSIS's assessment of under the new process[15] indicates

The assessment does not include evidence concerning the value of the non-threat-related data.

CSIS's authorization form to collect however, indicates that it was "unable to identify" whether the dataset contains information on Canadians. In SIRC's view, CSIS's assessment that it was "unable to identify" if the dataset contains information on Canadians is a significant error. Though it is not possible to extrapolate a trend from one instance, the obvious likelihood that this dataset contains data on Canadians leaves SIRC concerned about the rigour with which the other datasets housed in ODAC have been and will be assessed.

SIRC is also concerned with CSIS's management of legal risks related to the dataset. Despite the large volume of data CSIS did not request a formal legal risk assessment from the Department of Justice regarding the collection of the dataset until November 2016, more than six years after it began collecting the data. Although the dataset had been

[14] This is based on data provided by CSIS at a meeting to discuss the dataset.

[15] This assessment is documented in the Data Authorization Form for

ATIP version
JUN 0 8 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

subject to legal risk considerations as part of the ingestion process, the Department of Justice submitted its formal legal risk assessment in February 2017.[16]

[17]

The fact that CSIS did not seek a legal risk assessment until 2016 is of concern to SIRC. CSIS has, rightly, pointed out that it was not required to seek a legal risk assessment until the Minister of Public Safety and Emergency Preparedness issued the current Ministerial Direction on Operations and Accountability in July 2015. Irrespective of this fact, the dataset constitutes the continuous and extended collection of information

SIRC saw that further consideration was requested among senior management regarding the legality of the collection, in part as a result of the *en banc* decision. However, CSIS ultimately decided to continue with the collection.[18] In a briefing with SIRC, CSIS officials cited a number of factors that entered into the decision,

In SIRC's view, this process is symptomatic of CSIS's failure to grapple with the risk surrounding the legality of the collection of non-warranted bulk datasets in the wake of the *en banc* decision and to provide adequate high-level direction regarding their collection. This resulted in significant confusion regarding the role of different groups at CSIS, as well as the grounds on which to make the decision. Overall, in light of the legal risks associated with bulk collection, both with respect to section 12 of the *CSIS Act*, as well as the Charter in this case, SIRC believes that the continued collection of this dataset without a warrant is unreasonable. The *en banc* decision was not appealed. If uncertainties persisted about the scope of the decision, an application for a warrant would have eliminated any doubt on the lawfulness of this collection activity. While SIRC has not conducted a full review of the datasets in ODAC holdings, other datasets contain other types of data that may present similar Charter risks.

[16] See Legal Risk Assessment in

[17]

[18]

ATIP version
dated: JUN 0 8 2019

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

## Management of the data analysis function

The challenges outlined above with respect to ODAC's assessment of datasets and utility should be situated within the context of broader issues concerning the management of ODAC. ODAC was created in 2006 in order to allow CSIS to take full advantage of data that it was already collecting (e.g., through warranted collection) using modern data exploitation technologies. However, ODAC encountered significant challenges in reaching its trajectory laid out in 2005. Reviews by consultants in 2007 and 2009 identified a number of issues that were preventing ODAC from reaching its desired end state. They made a number of recommendations, including with respect to data quality and quantity, technical capabilities, measurement of utility, [19]

A new roadmap for ODAC was released in 2010 to chart a new path forward, largely with respect to new capabilities Some of these technical improvements have been implemented. However, SIRC found that recommendations with respect to business processes and governance, reporting, and performance measurement structures were not satisfactorily addressed.

Despite these issues, in 2011, the Data Acquisition Program was initiated to add to the warranted metadata in ODAC's holdings through the acquisition of bulk datasets. In fact, ODAC assigned priority to acquiring datasets,

In recent years, some technical improvements have been introduced.

[19] The 2007 Report and 2009 report, Data Exploitation Task Force I and II, and Data Exploitation Working Group (DEWG) reports from

ATIP version
JUN 0 8 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

However, the privacy implications, which have yet to be assessed, may be significant.

SIRC found that significant issues still exist with respect to business processes, governance, and performance measurement. For example, the value provided by data exploitation activities was limited by [20] More problematic is the fact that CSIS does not have a system for tracking the operational outcomes achieved by the program, nor is it able to track the use or propagation of data within its systems. This was highlighted when CSIS encountered a number of challenges delivering the statistics SIRC requested regarding the use of non-warranted datasets, as well as examples of the value brought to investigations by these datasets.

A new method of logging access was implemented in the spring of 2017, CSIS has not put in place any system to measure the utility of activities or datasets, nor has there been an internal audit or evaluation. Thus, precise tracking of use of and utility from data sources was not possible.

This is in contrast to the United Kingdom, where there is a developed process to support decision-making around the retention of datasets. This process involves periodic "retention reviews" that require the intelligence agencies to supply specific information on how often the dataset has been used, as well as examples of specific operations that benefited from information contained in the dataset. Domestically, the use of scenario based targeting by the Canada Border Services Agency, which involves collecting personal information on travelers, is monitored and evaluated on an ongoing basis for effectiveness, among other things.[21] Overall, **SIRC found that the implementation of ODAC was such that it did not achieve its strategic objectives.**

5. Recommendations

SIRC has seen substantial effort by CSIS following the SIRC review of Data Management and Exploitation (2015-02) to improve CSIS's management and assessment processes with respect to bulk datasets. ODAC encountered a number of challenges, including the lack of a final legal opinion, in its efforts to assess the volume of data that had been collected in the previous years. However, in evaluating CSIS's efforts in this regard, SIRC concluded that CSIS has not grappled with the impact of the *en banc* decision on this type of collection. In this context, **SIRC found that CSIS's assessment and management of**

[20] One encouraging sign is the implementation of a pilot project in the regions, This appears to be a step in the right direction,

[21] *Canada Border Services Agency — Scenario Based Targeting of Travelers — National Security,* Office of the Privacy Commissioner, 2017.

ATIP version
JUN 0 8 2019
dated:

Document released under the Access to Information Act / Document divulgué en vertu de la Loi sur l'accès à l'information

**the non-warranted datasets with respect to privacy interests and legal risk are not satisfactory.**

**As a result, SIRC finds that there is a substantial risk that CSIS has exceeded its legislative authorities in the collection and retention of non-threat related information on individuals not suspected of constituting a threat to national security, both with respect to section 12 of the *CSIS Act* and the Charter.** This risk is more apparent in the context of the *en banc* decision. SIRC is of the view that, at a minimum, CSIS should seek direction from the Minister as to how to proceed with respect to mitigating legal risk until uncertainty regarding a potential new regime under Bill C-59 is resolved.

SIRC concludes that the management of the data collection and analysis function has been plagued with significant issues since the inception of ODAC in 2006. ODAC did not achieve its initial objective to bring modern technologies and techniques to bear on threat-related data, yet moved to acquire additional datasets. At the same time, **SIRC found that ODAC was never able to measure the operational value of its products or the datasets. Moreover, with few exceptions, CSIS was not able to demonstrate that these datasets deliver significant utility in terms of lead generation or provide significant value in the Canadian security intelligence context.**

If the new regime proposed by Bill C-59 becomes law, SIRC is concerned the threshold of "likely to assist" will allow for the collection and retention of more datasets than under the current wording of the *CSIS Act* before a fully functioning system is in place with respect to data governance, performance measurement, and the integration of data analysis with investigations.

Anticipating such a dataset regime, **SIRC recommends that:**

1. **CSIS continue to prioritize the implementation of a robust process for assessing the privacy impacts and legal risk associated with its datasets, particularly with respect to Canadians;**
2. **CSIS develop a system for assessing the utility of individual datasets, and that decisions regarding the continued retention of datasets should be informed by those assessments;**
3. **CSIS implement as soon as practicable a data control system in its operational database that can account for the provenance and access controls on each piece of reported data; and**
4. **CSIS develop a strategic approach to data collection and analysis across the organization, including with respect to data governance, performance measurement, and the integration of data analysis with investigations.**

ATIP version
dated: JUN 0 8 2019