

Security classification: Secret
CCM Number:286425
Contact: Bruce Wallace, Digital Policy Branch, SITT, 343-291-3795
Originator: Thomas Dunne, SITT, Digital Branch
Action Required: For approval
For action by: March 11, 2016

**ADVICE TO THE ASSISTANT DEPUTY MINISTER**

c.c. Senior Assistant Deputy Minister

**2014-2015 Performance Measurement Report on the Lawful Access Initiative**

**Date for Action:** Public Safety Canada has requested approval from Lawful Access Partner ADMs the week of March 11, 2016

**SUMMARY**

- ISED has been a partner in the Lawful Access Initiative (LAI) since 2000.
- As a partner in the LAI, ISED approval (at the ADM level) is required for the LAI Performance Measurement Report (PMR).
- We recommend you indicate your approval by signing this briefing note.

**BACKGROUND**

In light of its responsibility for the *Personal Information Protection and Electronic Documents Act*, the *Telecommunications Act*, and the *Radiocommunication Act*, Innovation, Science, and Economic Development Canada's role in the LAI is to help balance law enforcement's need to maintain its lawful access capability to ensure public safety, while at the same time ensuring that any obligations stemming from the initiative will not hinder industry's competitiveness and will continue to protect the privacy of individuals.

As a member of our portfolio, the Competition Bureau has provided language for the PMR pertaining to their involvement in the LAI. Traditionally, the SITT ADM approves the PMR on behalf of both ISED and the Competition Bureau.

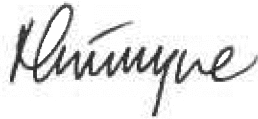
The LAI has received TBS approved funding since fiscal year 2000/01. LAI partners have worked collaboratively to prepare the annual progress reports which outline our collective efforts, expenditures, planned projects and priorities. ISED receives \$300,000 per year.

**CONSIDERATIONS**

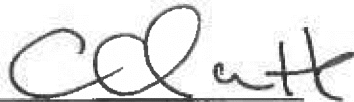
The PMR is attached with ISED input tabbed for your review. Your approval is requested prior to the submission of the PMR to Treasury Board. ADM approval from all partners is being sought the week of March 8, 2016.

**RECOMMENDATION**

I recommend that you approve the LAI PMR.



for Krista Campbell, Director General  
Digital Policy Branch, SITT

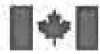


I approve

---

I do not approve

Attachment



Public Safety  
Canada

Sécurité publique  
Canada

SECRET//CC//CEO

BUILDING A SAFE AND RESILIENT CANADA



## Lawful Access Initiative

Performance Measurement Report  
2014-2015

DRAFT

Canada



## Table of Contents

<b>1. PROGRAM PROFILE .....</b>	<b>3</b>
1.1 INTRODUCTION .....	3
1.3 NEED FOR THE PROGRAM .....	5
1.4 ALIGNMENT WITH GOVERNMENT PRIORITIES .....	5
1.5 TARGET POPULATION(S) .....	6
1.6 STAKEHOLDERS .....	6
1.7 GOVERNANCE .....	6
1.8 RESOURCES .....	10
SUB-TOTAL .....	10
<b>2. LOGIC MODEL .....</b>	<b>11</b>
2.1 LOGIC MODEL DIAGRAM .....	11
<b>3. PERFORMANCE MEASUREMENT STRATEGY FRAMEWORK .....</b>	<b>12</b>
3.1 2014-2015 HIGHLIGHTS .....	12
3.1 PERFORMANCE RESULTS .....	24

DRAFT



## 1. Program Profile

### 1.1 Introduction

This document is the tenth Lawful Access Initiative (LAI) Performance Measurement Report (PMR), and covers the period beginning April 1, 2014, and ending March 31, 2015. It provides information on activities conducted by:

1. The Canadian Security Intelligence Service (CSIS);
2. The Communications Security Establishment (CSE);
3. The Department of Justice (DoJ);
4. Innovation, Science and Economic Development Canada (ISED);
5. The Public Prosecution Service of Canada (PPSC);
6. Public Safety Canada (PS); and
7. The Royal Canadian Mounted Police (RCMP).

These seven departments and agencies are known as the Lawful Access partners.

Assistant Deputy Ministers, or equivalents, responsible for the LAI from the participating federal government departments and agencies have all reviewed and endorsed this report. A copy of the report will be provided to the Minister of Public Safety and Emergency Preparedness, the Minister of Justice and the Minister of National Defence.

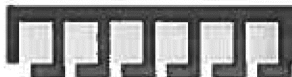
In the fall of 2013, PS led the LAI partners in an exercise to update the program's logic model as well as the performance indicators. The purpose of the exercise was to improve the utility of the PMR by using better indicators and making the results (the outcomes) of the LAI clearer. This streamlined report also reduces the reporting burden on the LAI partners while adhering more closely to current performance measurement standards.

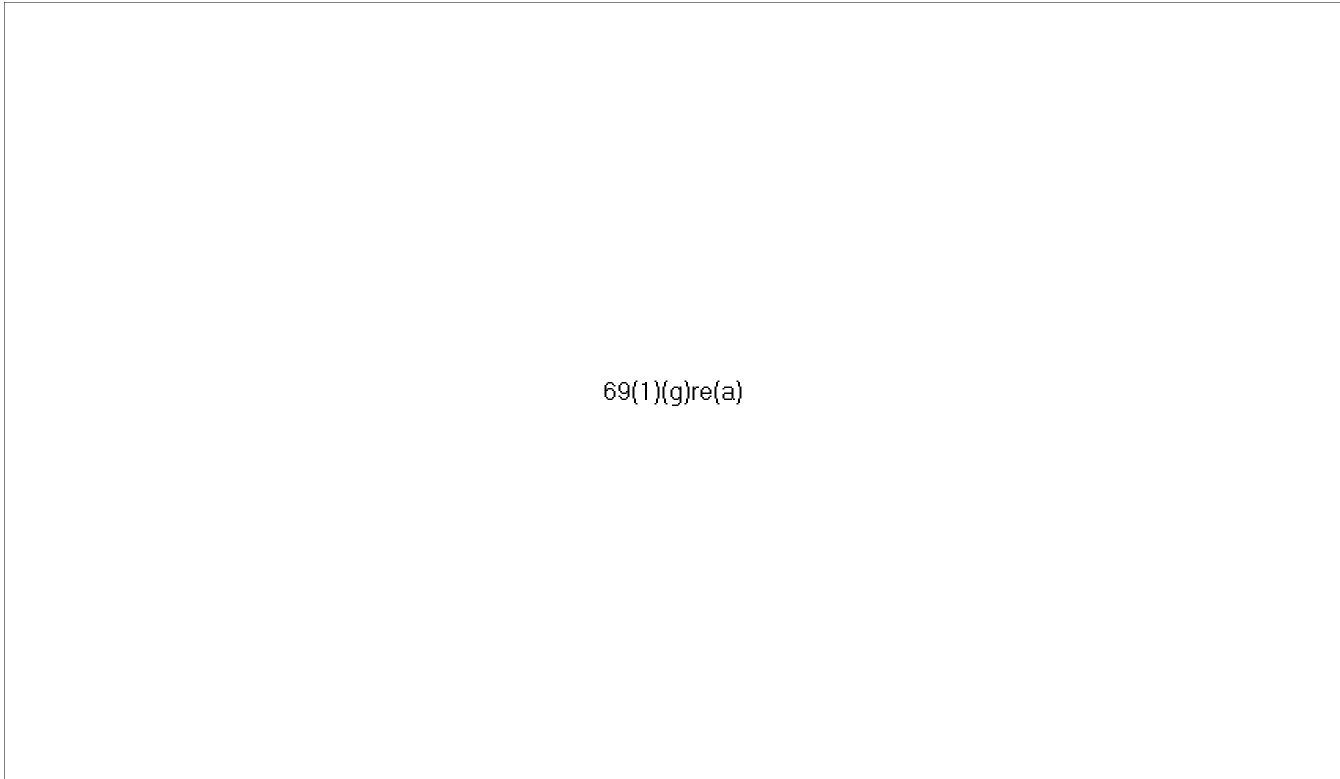
### 1.2 Background

#### *Lawful Access Funding*

In the 1990s, Canadian law enforcement and national security agencies recognized that their ability to lawfully access information and communications was eroding as a result of new technologies that enabled criminals and terrorists to evade the tools and techniques previously used by the police and CSIS to access information, a lack of funding and resources to explore and develop technological solutions to these challenges, and outdated legislation. It was agreed that corrective measures were needed.

69(1)(g)re(a)





69(1)(g)re(a)

The report is aimed at assessing the performance and value for money of the LAI and its funding envelope. It does not assess overall lawful access capabilities. It is important to note that many partners dedicate more resources to lawful access related activities than what they receive through the LAI in order to help address growing operational requirements, the increasing use of telecommunication services and rapid technical advancements. CSE, CSIS, DOJ, PPSC, and the RCMP reallocate significant funds from other sources to conduct activities that support or complement the LAI. This can include

15(1),16(1)(b)

15(1),16(1)(b)

15(1),16(1)(b)

or contributing to the development of lawful access related policies at international fora such as the United Nations. The PMR, however, only accounts for the activities conducted under the LAI.

Despite internal reallocations to fund activities to supplement the LAI, the overall resources dedicated to lawful access activities

15(1)

15(1)

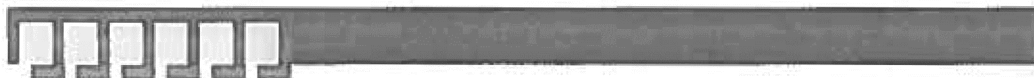
While the lawful access partners have made substantial progress over the years despite the LAI's limited funding envelope, with a general awareness of the environment,

15(1)

15(1)

15(1)

The LAI's funding levels, which were established in 2005, are simply no longer adequate to address today's operational requirements.



### 1.3 Need for the program

The term "lawful access" refers to the techniques used by law enforcement and national security agencies to lawfully intercept communications or obtain digital evidence and electronic data.

23

23

The implementation of judicial authorizations to intercept communications requires the development and management of

15(1).16(1)(b)

15(1).16(1)(b)

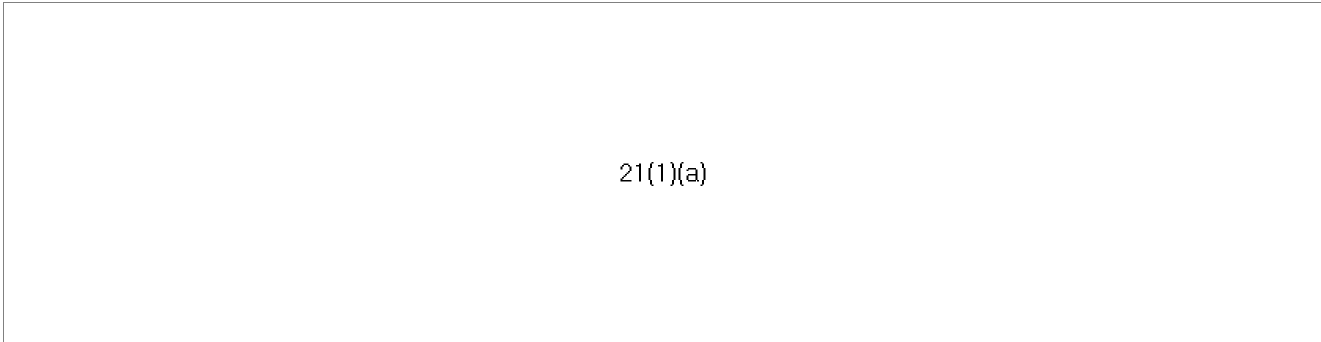
Lawful access supports the investigative and intelligence collection activities carried out by CSIS, the RCMP and other law enforcement agencies at the federal, provincial and municipal levels. It is a necessary tool in the investigation of threats to the security of Canada and Canadians, such as Internet child luring, drug trafficking, terrorism and organized crime.

### 1.4 Alignment with government priorities

The LAI is in line with the Government's priorities to protect Canada from a range of threats and its obligation to protect the national sovereignty and security of Canada. Furthermore, the 2015 Speech from the Throne acknowledged that Canada is fundamentally a safe and peaceful country, and the Government will continue to work to keep all Canadians safe, while at the same time protecting their cherished rights and freedoms.

In 2014-2015, the LAI remained consistent with Public Safety Canada's strategic outcome to "build a safe and resilient Canada". It also remained consistent with CSIS' strategic outcome, "Intelligence is used to protect the security and safety of Canada and its citizens", as the LAI funds the agency's ability to develop and maintain the means to collect and process intelligence.





21(1)(a)

**1.5 Target population(s)**

The program enhances the safety of Canadians and Canadian communities by giving law enforcement and intelligence agencies the tools they need to fulfill their mandates.

**1.6 Stakeholders**

LAI program stakeholders include: The Communications Security Establishment (CSE), the Canadian Security Intelligence Service (CSIS), The Department of Justice (DoJ), Innovation, Science, and Economic Development Canada (ISED), Public Prosecution Service of Canada (PPSC), Public Safety Canada (PS), and the Royal Canadian Mounted Police (RCMP).

**1.7 Governance**

***Canadian Security Intelligence Service***

CSIS uses a variety of collection and analysis methods to investigate individuals and groups whose activities are suspected of constituting a threat to national security. The role of CSIS with regard to the LAI is

15(1).16(1)(b)

15(1).16(1)(b) to ensure that Canada maintains effective capabilities for the collection and analysis of intelligence information. The lawful access initiative falls under Section 1.1 – Intelligence Program of the CSIS Program Activity Architecture (PAA).

***Communications Security Establishment***

As Canada’s national cryptologic agency, CSE possesses a unique ability to provide and protect information for the Government of Canada, including Canadian law enforcement and national security agencies. In response to broad Government of Canada and agency-specific intelligence priorities, CSE provides technical and operational assistance and services to other lawful access partners, as well as information from communications and non-communications signals obtained through the signals intelligence program. The lawful access initiative falls under section 273.64(1)(c) of the *National Defence Act* where CSE is mandated to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties.





21(1)(b)

***Public Prosecution Service of Canada***

The PPSC contributes to the LAI by providing legal advice and support to law enforcement agencies over the course of investigations and prosecutions involving lawful access issues. In addition to providing formal and informal training to investigators, the PPSC provides training to its wiretap agents at both the national and regional levels. Further, HQ counsel play a lead role in operational fora focused on litigation strategies and prosecutorial best practices in order to ensure that prosecutors have the required expertise to deal with the complex LA issues that regularly arise. Finally, the PPSC participates in policy development working groups with other LA partners in order to promote a common understanding of relevant legal issues, to support the implementation of consistent standards and practices, and to identify possible gaps in current legislation. The LAI falls under the Drug, *Criminal Code*, and terrorism prosecution program of the PPSC's program activity architecture.

***Public Safety Canada***

The role of PS with regard to the LAI is to provide leadership in the area of policy development and to coordinate interdepartmental initiatives to address the policy, legal and technical challenges experienced by the portfolio agencies and other lawful access partners. These initiatives require frequent meetings and consultations with partners and stakeholders, including provincial and municipal police services and their associations, federal and provincial privacy commissioners, privacy advocates, private sector companies and their associations, as well as international partners,

15(1).16(1)(c)	15(1).16(1)(c)	PS
----------------	----------------	----

coordinates the Performance Measurement Report on behalf of the lawful access partners. The lawful access initiative falls under Section 1.1 – National Security, Sub-Section 1.1.1 – National Security Leadership of Public Safety's program activity architecture.

***Royal Canadian Mounted Police***

The role of the RCMP with regard to the LAI focuses on the research and development of technical tools and expertise required for investigations, search and seizure, intelligence gathering, prevention, technical assistance and prosecution. The RCMP, along with CSIS and CSE, also engages in the research and development of technical solutions to address interception challenges resulting from emerging technologies and analysis of electronic data. The lawful access initiative falls under Section 1.1 Police Operations, sub-program 1.1.3 – Technical Services and Operational Support, sub-sub-program 1.1.3.1 – Technical Investigations of the RCMP's program activity architecture.



***Comprehensive Legal Review Committee***

21(1)(b)

In addition to the ITCC and the CLRC, each lawful access partner maintains comprehensive internal control and reporting processes. As well, the RCMP and CSIS follow the TBS' Enhanced Management Framework for projects. This includes developing and submitting formal Treasury Board submissions for project approval when necessary.

***Interdepartmental Technical Coordinating Committee***

The Assistant Deputy Minister Interdepartmental Technical Coordinating Committee (ITCC) is chaired by the Public Safety Senior Assistant Deputy Minister, National and Cyber Security Branch. The ITCC is intended to facilitate information exchange and to help ensure close coordinated collaboration between the RCMP, CSIS and CSE research and development efforts to maintain current lawful access capability. The ITCC meets as required to provide oversight and strategic direction, and to resolve conflicting priorities. Other departments, such as the Privy Council Office (Security and Intelligence), DoJ, PPSC, IC, and TBS are consulted, as required.

Much of the ITCC's mandate is accomplished through a number of policy, legislative, and technical working groups, along with various departmental bilaterals.



## 1.8 Resources

## Consolidated Funding for Lawful Access Initiative (FY 2014-2015)\*

(Thousands of dollars)

Department/ Agency	Lawful Access Initiative	2014-2015 Allocated and Ongoing Funding	2014-2015 Actuals
CSIS			
	15(1)		
	<b>SUB-TOTAL</b>		
CSE			
	15(1)		
DoJ			
	21(1)(b)		
	<b>SUB-TOTAL</b>	<b>\$1,477 (10.5 FTEs)</b>	<b>\$1,564 (8.95 FTEs)<sup>2</sup></b>
ISED	Policy Development	\$278 (3 FTEs)	\$278 (2 FTEs)
	Accommodation	\$22	\$22
	<b>SUB-TOTAL</b>	<b>\$300 (3 FTEs)</b>	<b>\$300 (2 FTEs)<sup>3</sup></b>
PPSC	Legal Advice and Prosecution	\$1,394 (11 FTEs)	\$30,418 (149 FTEs)
	Accommodation	\$123	\$3,041
	<b>SUB-TOTAL</b>	<b>\$1,517 (11 FTEs)</b>	<b>\$33,459 (149 FTEs)<sup>4</sup></b>
PS	Policy Coordination and Legislative Development	\$183 (2 FTEs)	\$203 (2 FTEs)
	Accommodation	\$17	\$17
	<b>SUB-TOTAL</b>	<b>\$200 (2 FTEs)</b>	<b>\$220 (2 FTEs)<sup>5</sup></b>
RCMP	Telecommunications Interception	\$5,345 (20 FTEs)	\$2,781 (20 FTEs)
	Processing and Analysis	\$1,926 (16 FTEs)	\$4,670 (16 FTEs)
	Entry and Alternate Techniques	\$5,356 (18 FTEs)	\$2,591 (18 FTEs)
	Field Support	\$1,378 (13 FTEs)	\$819 (10 FTEs)
	Accommodation	\$695	\$547
	<b>SUB-TOTAL</b>	<b>\$14,700 (67 FTEs)</b>	<b>\$11,408 (64 FTEs)<sup>6</sup></b>
<b>TOTAL</b>		<b>\$56,994 (239.5 FTEs)</b>	<b>\$85,355 (337.95 FTEs)</b>

<sup>1</sup> CSE continues to convert funding to support 15(1)

21(1)(b)

<sup>2</sup> IC reduced the number of FTEs it assigns to the Lawful Access Initiative as the funds allocated in 2005 were no longer sufficient to pay for the same number of staff in FY2012-2013.

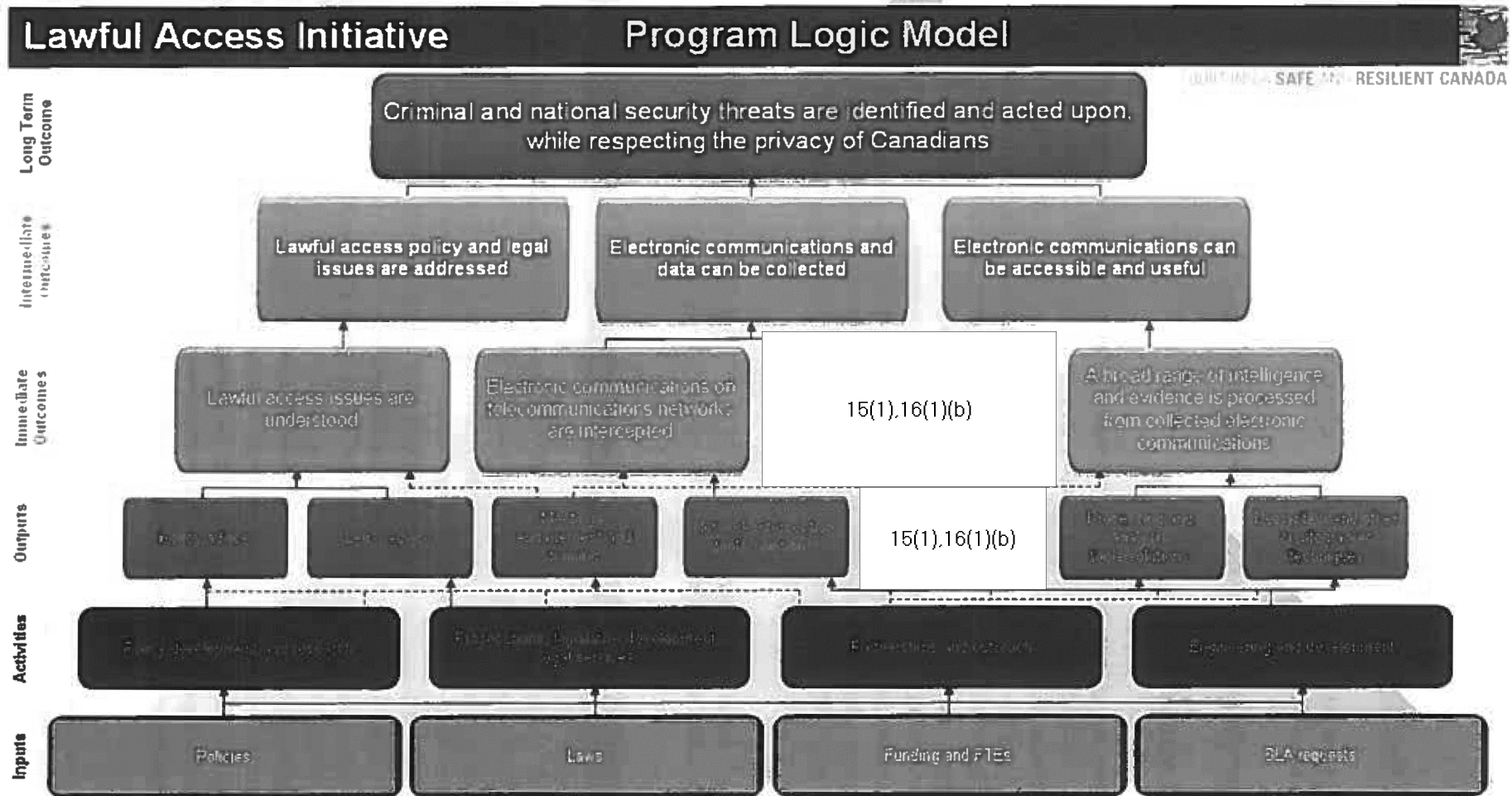
<sup>4</sup> PPSC's figures increased significantly as of 2012-2013 due to a change in methodology that the PPSC used to provide accounting of the resources allocated to lawful access prosecutions.

<sup>5</sup> PS internally reallocates funding to cover the salaries of FTEs as the Lawful Access Initiative funds allocated in 2005 are no longer sufficient to pay for the same number of employees.

<sup>6</sup> \$751K to be absorbed in the RCMP's operational budget.

## 2. Logic Model

### 2.1 Logic Model Diagram



## 2.2 Logic Model Narrative

For a full narrative on the logic model, please refer to the 2013-2014 Lawful Access Initiative Performance Measurement Report.

## 3. Performance Measurement Strategy Framework

### 3.1 2014-2015 Highlights

Currently, three out of four Canadians own smartphones, well above the rates in the United States and other developed markets.<sup>7</sup> The average consumer has affordable and easy access to more communications and computing power than ever before. Sophisticated encryption – which used to be well out of reach of the average person – is a standard out-of-the-box feature for many consumer devices (e.g. Apple's iPad and iPhone), offering several layers of security for minimal effort or expense. Indeed, many application developers have released popular apps with the sole purpose of ensuring encrypted communications between users. The average Internet user can also download free software to ensure they can traverse cyberspace anonymously. None of these innovations come packaged with complementary intelligence collection tools. Developing and maintaining the investigative capabilities needed for a 21<sup>st</sup> century environment continued to be an expensive and time-consuming task in 2014-2015.

The following is a narrative description of some key highlights from the 2014-2015 reporting year (Note: not all outcomes and outputs may be reflected here; only those with key highlights may be selected)

#### Output - Policy advice

- 52 briefings or reports were given to Director General Equivalents or lower on lawful access matters (2013-2014: 50). Significant topics included: 4 reports prepared for [redacted] 15(1).16(1)(c) [redacted] 15(1).16(1)(c) on legal, policy and technical challenges and experiences with respect to lawful interception; reports prepared for the Lawfully Authorized Electronic Surveillance Committee; [redacted] 15(1).16(1)(c) [redacted] 15(1).16(1)(c) statistical reports detailing the amount, type, and breakdown of interceptions across federal and provincial levels; info-bulletins to prosecutors on major bills or major court cases; Web-ex on bill C-13 and additional material to support bill C-13; the development of national precedents; and additional briefing material to support reports, documents or briefings submitted to senior management or Ministers ; briefing notes on Electronic Surveillance, forbearance, and obtaining subscriber figures; briefing material the transparency reporting guidelines; material prepared for the Canadian Association of Chiefs of Police meeting; and briefing material on internet blocking and internet governance**

<sup>7</sup> comScore, Inc. 2014. Canada Digital Future In Focus 2014: The 2013 Digital Year In Review & What it Means for the Year Ahead. [www.comScore.com](http://www.comScore.com).



15(1),23

23

**Output – Meetings, Engagement and Training**

- **207 meetings were held to develop or share technical and legal tools or skills (2013-2014: 242). These meetings were with either international or domestic partners, and non-government stakeholders. Significant meetings included: National Wiretap Experts Committee Face-to-face meetings and conference calls dealing with the *R. v. Spencer* decision; Coordinating Committee of Senior Officials Cybercrime Working Group conference calls and meetings; meetings with foreign partners; meetings with domestic partners to advance lawful access capabilities; meetings with telecommunications service providers to develop lawful access solutions, incorporating procedures/ security requirements and lawful access service contracts; Participation in the 15(1),16(1)(c) Participation in the Lawfully Authorized Electronic Surveillance (LAES) Committee; and meetings of the Tactical Analysis Team; meetings on safeguarding and enhancing lawful access, including topics such as the impact of the *Spencer* decision, impact of transparency reporting; and forbearance decisions; various interdepartmental meetings on *Spencer*; High-Tech Crime Sub-Group (G7 Roma-Lyons Group); Justice Cybersecurity Practice Group; attendance at Canadian Association of Chiefs of Police meetings for: eCrime Committee Meeting and the Tech Crime Committee; attendance at meetings with the Canadian Bar Association.**



- **95<sup>9</sup>** engagement and training sessions with stakeholders at the national and international level (2013-2014: 143). Significant engagement or training sessions included: a one-day wiretap session; school for Prosecutors level II; "Team Canada" quarterly training sessions (national); international sessions with international partners; and Intercept monitor training course; close access national level exchanges; presentations to international study groups on lawful access; mediation device training sessions to Communication Service Providers; conversion device training sessions to the RCMP and a CSP; human resources training session; training on bill C-13; *Spencer Working Group* meetings; and meeting with the United Kingdom Reviewer of Terrorism Legislation. .

Output - Network interception tools/solutions

- 

15(1),16(1)(b),16(1)(c)

Output - Entry and Alternative capture tools/solutions

- 

- 

- 

- 

15(1),16(1)(b),16(1)(c)

<sup>9</sup> A change in the number of engagements and training sessions could be explained by the exclusion of training courses (development) attended by personnel at the various departments and/or agencies. Only identified program level strategic national exchanges and sessions were included for 2014-2015.



**Output - Processing and analysis tool/solutions**

15(1),16(1)(b),16(1)(c)

**Output - Decryption and other cryptographic techniques**

15(1),16(1)(b),16(1)(c)

**- Immediate Outcome - Lawful access issues are understood<sup>41</sup>**

- **79 reports, documents or briefings were submitted to senior management (ADM equivalent and above) and Ministers in 2014-2015 (2013-2014: 24). Significant topics included: material to support Bill C-13 committee appearance; Memo to support meeting on intercept challenges;**

15(1),16(1)(b),16(1)(c)

<sup>41</sup> CSIS and the RCMP could not agree on a single result for this indicator because of their different targets and operational situations.





Memos to support policy and operational impacts of *R. v. Spencer*; Inquiry of Ministry, transparency reporting guidelines, cybercrime and cyber-bullying; lawful access funding.

**Immediate Outcome - Electronic communications on telecommunications networks are intercepted**

- 
- 
- 15(1).16(1)(b)
- 

**Immediate Outcome - Electronic communications and data that are inaccessible through network interception are captured**

- 
- 15(1).16(1)(b)

**Immediate Outcome - A broad range of intelligence and evidence is processed from collected electronic communications**

- 
- 15(1).16(1)(b)

15(1).16(1)(b)



- [Redacted]  
15(1),16(1)(b),16(1)(c)

**Intermediate Outcome - Electronic communications and data can be collected**

- [Redacted]
- [Redacted]  
15(1),16(1)(b),16(1)(c)
- [Redacted]

**Intermediate Outcome – Electronic communications can be accessible and useful**

- [Redacted]  
15(1),16(1)(b),16(1)(c)

**Intermediate Outcome - Lawful access policy and legal issues are addressed**

- **6<sup>14</sup> bills or major policy initiatives were introduced or implemented to address lawful access issues (2013-2014: 4). Significant achievements include:**

[Redacted]  
15(1),16(1)(b),16(1)(c)

<sup>14</sup> While many government departments and agencies worked on Bill C-51, for the purposes of this report, it was only counted once.

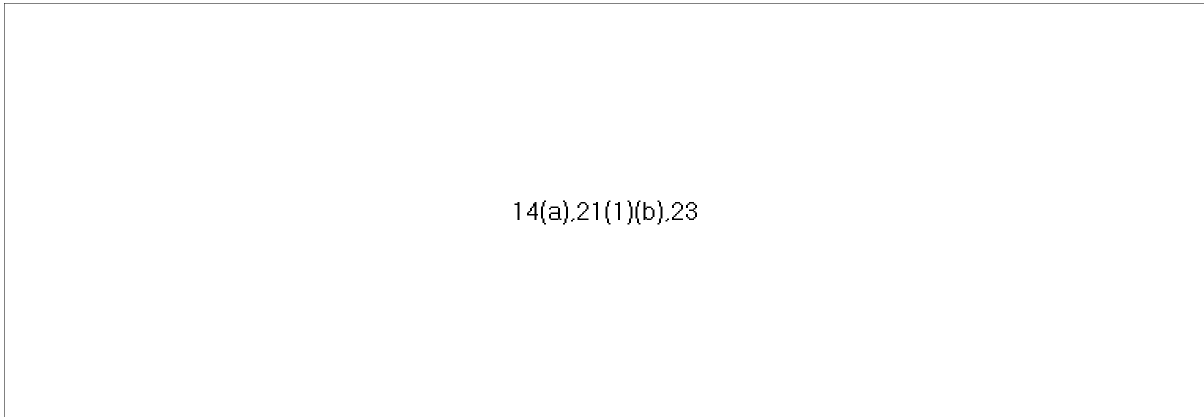


- o **Bill C-13: *Protecting Canadians from Online Crime Act*** – The Bill implements the Report to the Federal/Provincial/Territorial Ministers responsible for Justice and Public Safety: *Cyberbullying and the Non-consensual Distribution of Intimate Image's* recommendations to amend the *Criminal Code* to provide for new offence of non-consensual distribution of intimate images as well as complementary amendments to authorize the removal of such images from the Internet and the recovery of expenses incurred to obtain the removal of such images, the forfeiture of property used in the commission of the offence, a recognizance order to be issued to prevent the distribution of such images and the restriction of the use of a computer or the Internet by a convicted offender. The Bill also contains a broad set of investigative powers that modernize the *Criminal Code* including: preservation demands and orders; production orders for tracking data and transmission data; a streamlined process for obtaining warrants associated with interception of private communications, as well as corresponding powers for the *Mutual Legal Assistance in Criminal Matters Act* and the *Competition Act*. Bill C-13's first reading was November 20, 2013 and came into force March 10, 2015.
  
- o **Bill C-51: *Anti-terrorism Act*** – The Bill allowed for five major changes: (1) created the *Security of Canada Information Act*, which authorizes the Government of Canada institutions to disclose information to Government of Canada institutions that have jurisdiction or responsibilities in respect of activities that undermine the security of Canada; (2) created the *Secure Air Travel Act*, which is a new legislative framework for identifying and responding to persons who may engage in an act that poses a threat to transportation security or who may travel by air the purpose of committing a terrorism offence; (3) provides for amendments to the *Criminal Code*; (4) provides for amendments to the *Canadian Security Intelligence Act* to permit CSIS to take, within and outside Canada, measures to reduce threats to the security of Canada, including measures that are authorized by the Federal Court; and (5) provides for amendments to the *Immigration and Refugee Protection Act*.

23.21(1)(b)

o  
o





Ultimate Outcome - Criminal and national security threats are identified and acted upon, while respecting the privacy of Canadians

- **190** criminal threats in the areas of terrorism, organized crime, and drug cases were identified and acted upon by the RCMP in 2014-2015 (2013-2014: 289<sup>15</sup>). These investigations used electronic surveillance tools like the ones developed under the lawful access Initiative. Without the development of these tools, investigation of these offences would have been either technological or practically impossible, or prohibitively expensive.
- <sup>15(1).16(1)(c)</sup> national security threat investigations, involving <sup>15(1).16(1)(c)</sup> were identified and acted upon by CSIS in 2014-2015. These cases were on matters such as terrorism, espionage and foreign influenced activities. As with the RCMP, work on these cases was facilitated to an extraordinary degree by those tools developed this year and in prior years under this initiative.
- **0** people were prosecuted this year for wilfully intercepting or disclosing a private communication without lawful excuse (2013-2014: 0). This indicated that law enforcement and intelligence agencies are using interception tools appropriately and within the confines of the law, respecting the privacy of Canadians.
- **4** significant Supreme Court decisions concerned lawful access issues (2013-2014: 2). In these cases, the court had to consider how best to balance Canadian's privacy interests, as protected by the *Charter*, with other important state interests, such as the importance of ensuring public safety through effective law enforcement, and uncovering the truth in the questions being considered by the court. These decisions will all govern and inform Canada's approach to lawful access going forward. A description of the nature and impact of these decisions is provided below:

<sup>15</sup> There is no clear indication as to the variance from year to year; this could be the result of multiple variables. Also, 2013-2014 was the first year that the number of criminal threats was tracked and reported on in this report, therefore, it is difficult to analyze why there were any changes from one year to another.



### 3.1 Performance Results

Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
<b>Long Term Outcome</b>						
Criminal and national security threats are identified and acted upon, while respecting the privacy of Canadians	Number of national security and serious crime <sup>16</sup> cases investigated using lawful access capabilities	Collated annually	Trendline <sup>17</sup>	N/A	RCMP, CSIS	190 (RCMP) Terrorism: 61 Org. Crime: 57 Drugs: 72  15(1)
	Number of prosecutions against officers or servants of Her Majesty In right of Canada for offences under section 184 or section 193 of the <i>Criminal Code</i>	Collated annually	0	0	PS	No private communications were intercepted, nor were intercepted communications disclosed, without lawful excuse

<sup>16</sup> For CSIS the definition of "Serious Crime" includes "Terrorism and threats to the security of Canada" such as: (a) espionage or sabotage that is against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage; (b) foreign influenced activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person; (c) activities within or relating to Canada directed toward or in support of the threat or use of acts of serious violence against persons or property for the purpose of achieving a political, religious or ideological objective within Canada or a foreign state; and (d) activities directed toward undermining by covert unlawful acts, or directed toward or intended ultimately to lead to the destruction or overthrow by violence of, the constitutionally established system of government in Canada. For RCMP the definitions of Terrorism, Organized Crime, and Drugs includes the following *Criminal Code* offences: Participation in the activity of a terrorist group; Facilitating terrorist activities; Commission of an offence for a terrorist group; Instructing to carry out terrorist activity; Laundering proceeds; Participating in activities of a criminal organization; Instructing commission of an offence for a criminal organization; Trafficking in narcotic; Possession of a narcotic for purpose of trafficking; Importing a narcotic; Possession for the purpose; and, Production.

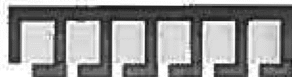
<sup>17</sup> Although every effort was made to establish baselines and targets, in some cases this was not feasible due to the reactive nature of the indicator. As such, data will be collected year after in order to establish a trend line.

15(1)

Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
21(1)(b).23						
<b>Intermediate Outcomes</b>						
Lawful access policy and legal issues are addressed	Number of bills/legislation tabled, policies and initiatives undertaken relating to lawful access	Collated annually	4 <sup>21</sup>	N/A	All	<p><b>6 (Total) – 1 (RCMP), 2 (PS), 6 (DOJ), 1 (CSIS), 1 (IC), 0 (PPSC)</b>                      Note: Bill C-51 and the Transparency reporting guidelines were presented by three departments but only counted once.</p> <p><b>RCMP:</b></p> <ul style="list-style-type: none"> <li>• Bill C-51</li> </ul> <p><b>PS:</b></p> <ul style="list-style-type: none"> <li>• Bill C-51</li> <li>• Development of transparency guidelines for telecommunications service providers.</li> </ul> <p><b>DOJ- CLPS and PSDI:</b></p> <ul style="list-style-type: none"> <li>• 23</li> <li>• 69(1)(g)re(a)</li> <li>• 14(a).23</li> </ul>

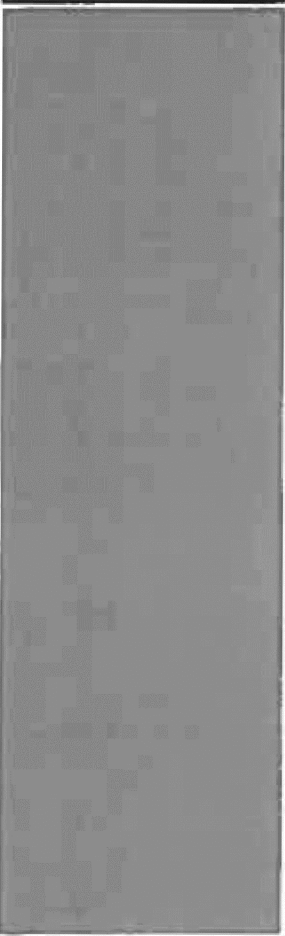
<sup>20</sup> Based on 2013-2014 input only.

<sup>21</sup> Based on 2013-2014 input only.



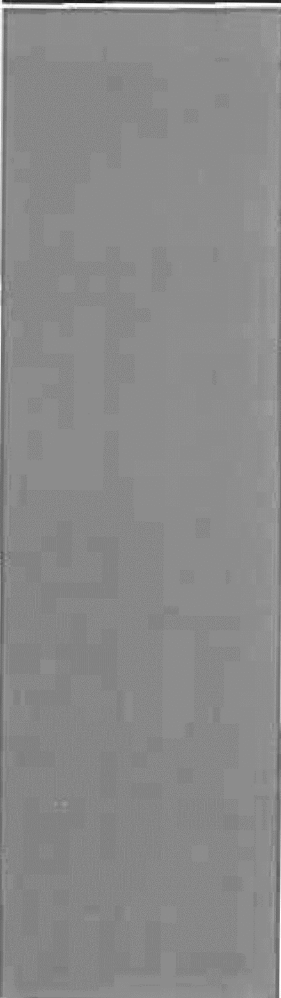
Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						<b>CSIS:</b> 15(1).16(1)(c).16(1)(b) <b>ISED:</b> <ul style="list-style-type: none"><li>Development of transparency guidelines for telecommunications service providers</li></ul>
Electronic communications and data can be collected	Percentage of networks that have integrated interception capabilities	Collated annually	15(1).16(1)(b).16(1)(c)		RCMP, CSIS	15(1).16(1)(b).16(1)(c)
15(1).16(1)(b).16(1)(c)						



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						15(1),16(1)(b),16(1)(c)
	Number of days of interception blackouts	Collated annually	TBD	TBD	RCMP, CSIS	






Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
	Percentage of network tools that required an upgrade or replacement within three years of service	Collated annually	TBD	15(1),16(1)(b),16(1)(c)	RCMP, CSIS	15(1),16(1)(b),16(1)(c)
	15(1),16(1)(b),16(1)(c)	Collated annually	TBD	TBD	RCMP, CSIS	

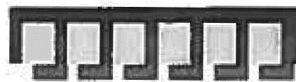
15(1),16(1)(b),16(1)(c)



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						15(1),16(1)(b),16(1)(c)
	\$ and FTE's spent on retrofitting or updating existing solutions	Collated annually	Trendline	N/A	RCMP, CSIS	



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						15(1),16(1)(b),16(1)(c)



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
Electronic communications can be accessible and useful	Percentage of collected electronic communications that is processed into readable/useful intelligence or evidence	Collated annually	TBD	15(1)	RCMP, CSIS	15(1)

**Immediate Outcomes**

Lawful access issues are understood	21(1)(b)				
-------------------------------------	----------	--	--	--	--

<sup>25</sup> In some cases where a new indicator was developed during the 2013-2014 reporting year it was not possible to demonstrate performance data for that year as data collection practices may not have been in place.

<sup>26</sup> Senior management includes ADM or DM equivalents.



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						<p>Media lines, Q&amp;As, Opening Remarks</p> <ul style="list-style-type: none"><li>• 1 Memo to support meeting with PCO regarding Intercept Challenges</li><li>• 2 Paper on Policy and Operational Impacts of R v. Spencer</li><li>• 1 Inquiry of Ministry</li><li>• 1 IP21C</li><li>• 1 Transparency reporting guidelines</li><li>• 1 Ops Fees</li><li>• 1 Cyber Crime report to D/Commr</li></ul> <p><b>PS Highlights:</b></p> <ul style="list-style-type: none"><li>• Memo to S/ADM on: Bill S-4 (Supp B Estimates); Bill C-13 (Supp B Estimates); and Electronic Surveillance and Privacy (Supp B Estimates).</li><li>• Memo to DM: Issuing guidance to telecommunications service providers on transparency reporting</li><li>• <div data-bbox="1356 818 2024 980" style="border: 1px solid black; padding: 5px; text-align: center;">21(1)(b)</div></li><li>• Memo to the S/ADM and Memo to the DM: Updated response to CSIS and the RCMP on Lawful Access funding</li><li>• Memo to the DM – Telecommunications Service Providers transparency report for digital information requests</li><li>• Memo to the DM – Update on the development of transparency guidelines</li><li>• Memo to the S/ADM – Responding to the RCMP letter on Transparency</li><li>• Memo to the Minister – Guidance for telecommunications transparency reporting</li><li>• Memo to the DM – Exploring options to obtain basic subscriber information for investigators</li><li>• Memo to the DM – Recent calls for increased transparency reporting on electronic surveillance</li></ul>

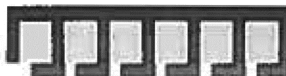


Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	<ul style="list-style-type: none"> <li>• Memo to the S/ADM and DM – Meeting with Telus to discuss transparency reporting for electronic surveillance</li> <li>• Memo to the Minister- PS speaking engagement at the LAES Working Group</li> <li>• Memo to Minister – PS panelist at 15(1)</li> <li>• Memo to the S/ADM – Lawful access funding re-profile</li> <li>• Memo to the DM – Next steps in transparency reporting for digital information requests</li> <li>• Memo to Minister – Status of lawful access policy development and medium term way forward</li> </ul> <div style="border: 1px solid black; padding: 2px; text-align: center;">23</div> <p><b>DoJ – CLPS Highlights</b></p> <ul style="list-style-type: none"> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> <li>• [REDACTED]</li> </ul> <div style="border: 1px solid black; padding: 2px; text-align: center;">21(1)(b).23</div> <p><b>DoJ – PSDI Highlights (All LSUs)</b></p> <ul style="list-style-type: none"> <li>• Office of the Privacy Commissioner’s Report on the RCMP’s Warrantless Access to Subscriber Information (Annual Report</li> </ul>
						<div style="border: 1px solid black; padding: 2px; text-align: center;">23</div>

23



Program Outputs and Outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						to Parliament) •  •  •  23
	Percentage of prosecutors surveyed whose understanding of lawful access issues had improved	Collated annually	Trendline	N/A	PPSC	90.5%  • 19 of 21 National Wire Tap Expert Committee meeting participants who completed the feedback form reported that their knowledge had significantly or moderately increased.
	Percentage of police officers surveyed whose understanding of lawful access issues had improved	Collated annually	Trendline	N/A	RCMP	N/A
Electronic communications on telecommunications networks are intercepted	Percentage of operational situations where electronic data communications can be collected through	Collated annually	15(1).16(1)(c)		RCMP, CSIS	15(1).16(1)(c)  <b>Significant Achievements:</b>



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
	network interception					15(1).16(1)(c)
Electronic communications and data that are inaccessible through network interception are captured	15(1).16(1)(c)	Collated annually	TBD	Maintain baseline	RCMP, CSIS	15(1).16(1)(c)
A broad range of intelligence and evidence is processed from collected electronic communications	The average time required to develop and deploy software features and fixes, to systems that process intercepted/captured product into useable formats for analysis	Collated annually	15(1).16(1)(c)		RCMP, CSIS	15(1).16(1)(c)
						15(1).16(1)(c)





Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
	Percentage of known data sources that are Inaccessible	Collated annually	15(1),16(1)(c)		RCMP, CSIS	15(1),16(1)(c)
Policy advice	Number of briefings given or reports produced annually	Collated annually	Trendline	N/A	All	<p>S2 (Total)</p> <p>15 (IC), 4 (PS), 4 (PPSC), 10 (CSIS), 11 (RCMP), 8 (DOJ- CLPS)</p> <p><b>Highlights:</b>  <b>ISED Highlights (15):</b></p> <ul style="list-style-type: none"> <li>• DG brief on Transparency Report Information</li> <li>• ISP-Specific transparency reporting information – DG briefing</li> <li>• Transition 1-pager on Lawful Access</li> <li>• Lawful Access (Condition of License) 1-pager</li> </ul> <p style="text-align: center;">23</p> <p><b>CSIS Highlights (10):</b></p> <ul style="list-style-type: none"> <li>• 7 documents/briefing packages produced in support of the</li> </ul>
						15(1),16(1)(c)



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						<p>senior management briefings Itemized in Indicator 8.1</p> <ul style="list-style-type: none"><li>• 2 Canadian papers prepared for international meetings in May and November 2014.</li><li>• 15(1).16(1)(c) report revised (in conjunction with RCMP) to reflect current network Intercept capabilities as of September 2014.</li></ul> <p><b>RCMP Highlights (11):</b></p> <ul style="list-style-type: none"><li>• 15(1).16(1)(c)</li><li>• LAES reports</li><li>• National Wiretap Experts Group meeting reports</li><li>• Tactical Analysis Team reports</li><li>• 15(1).16(1)(c)</li><li>• A statistical report detailing the amount, type and breakdown of interceptions across federal and provincial levels</li><li>• Memo to PS re: five eyes lawful access legislation</li></ul> <p><b>PS Highlights (4):</b></p> <ul style="list-style-type: none"><li>• Memorandum to DG NSOD: Electronic surveillance and privacy;</li><li>• Memorandum to DG NDOD: Forbearance;</li><li>• Memorandum to DG NSOD: Lawful Access – Obtaining CRTC subscriber information</li><li>• Memorandum to DG: Lawful Access – for CACP LAC</li></ul> <p><b>DoJ – CLPS Highlights (8):</b></p> <ul style="list-style-type: none"><li>• Press Conference (Background Brief) on C-13</li><li>• Media Interviews on C-13 (4)</li><li>• Preparation of Transparency Reporting Guidelines</li></ul> <p>23</p>



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						<p><b>DoJ – PSDI Highlights (All LSUs)<sup>31</sup>:</b></p> <ul style="list-style-type: none"> <li>• 23</li> <li>• 8 Briefings to RCMP Clients on topics associated to lawful access (no specific advice provided), as well as review of RCMP briefing material for Deputy Commissioners on lawful access topics.</li> </ul>
Legal advice/support and prosecution services	Number of cases requiring advice on lawful access issues	Collated annually	Trendline	N/A	DoJ	<p>5 (Total)</p> <p>5 (DoJ- CLPS)</p> <p>23</p>

23
----



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						23
						23
						23

23



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification		
						<ul style="list-style-type: none"> <li>•</li> <li>•</li> </ul> <p style="text-align: center;">23</p>		
						69(1)(g)re(f)		
						<table border="1" style="width: 100%;"> <tr> <td style="width: 70%; text-align: center;">69(1)(g)re(f)</td> <td style="width: 30%; text-align: center;">23</td> </tr> </table>	69(1)(g)re(f)	23
						69(1)(g)re(f)	23	
<ul style="list-style-type: none"> <li>•</li> </ul> <p style="text-align: center;">23</p>								
	<b>Number of PPSC lawful access files involving legal advice and support (Including preparing judicial authorizations)</b>	<b>Collated annually</b>	<b>Trendline</b>	<b>N/A</b>	<b>PPSC</b>	<b>515 (Total)</b>		

23
----



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						23
						23
						23
						23

23



Programs, outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
Meetings, engagement and training	Number of meetings to develop or share technical and legal tools/skills e.g. meetings with partners (International and domestic) and non government stakeholders)	Collated annually	Trendline	N/A	All	<p>207 (Total) 132 (CSIS), 7 (PPSC), 45 (RCMP), 23 (DoJ- CLPS),</p> <p><b>Highlights:</b></p> <p><b>PPSC:</b></p> <ul style="list-style-type: none"><li>• 23</li><li>• CCSO Cybercrime WG conference calls and meetings</li></ul> <p><b>CSIS:</b></p> <ul style="list-style-type: none"><li>• 15(1),16(1)(c)</li><li>• 23</li><li>• 15(1),16(1)(c),23</li></ul> <p><b>RCMP:</b></p> <ul style="list-style-type: none"><li>• 15(1),16(1)(c)</li><li>• RCMP participated in LAES sub-working group of the CACP with Provincial and municipal law enforcement from Canada. (semi-annually)</li><li>• 31 Partnership outreach meetings with various telecoms services providers to facilitate lawful access</li><li>• 5 Tactical Analysis Team meetings</li><li>• CEWG Executive (1)</li><li>• CEWG Automotive Focus Group (1)</li></ul>



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
------------------------------	-----------	-----------	----------	--------	--	-------------------------------------

- **CEWG Mechanical Focus Group (1)**
- **CEWG Alarms Focus Groups (1)**
- **Australia (bi-lateral) (1)**

14(a).23





Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						<ul style="list-style-type: none"> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> <li>•</li> </ul>
	Number of engagement and training sessions with stakeholders at the national and international level	Collated annually	Trendline	N/A	All	<p>95 (Total) 10 (DoJ- CLPS), 2 PPSC, 29 RCMP, 54 CSIS,</p> <p><b>Key deliverables:</b> <b>PPSC:</b></p> <ul style="list-style-type: none"> <li>• Ontario Regional Office held a one day wiretap session on</li> </ul>

23

Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						<p>November 28, 2014</p> <ul style="list-style-type: none"><li>• School for Prosecutors Level II, July 21-23, 2014.</li></ul> <p><b>RCMP:</b></p> <ul style="list-style-type: none"><li>• 8 meetings. "Team Canada" holds quarterly training sessions nationally. They also hold 3 to 4 International sessions with International partners.</li><li>• 3 Intercept Monitor Training courses</li><li>• 18 other meetings and training sessions with others</li></ul> <p><b>CSIS:</b></p> <ul style="list-style-type: none"><li>•</li><li>•</li><li>•</li><li>•</li><li>•</li><li>•</li></ul> <p>15(1).16(1)(c)</p> <p><b>DoJ- CLPS:</b></p> <ul style="list-style-type: none"><li>•</li><li>•</li><li>•</li><li>•</li><li>•</li><li>•</li></ul> <p>23</p> <p><b>DoJ – PSDI Highlights (All LSUs)<sup>36</sup></b></p>

23



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						14(a).23
Network interception tools/solutions	Number of integrated tools developed annually	Collated annually	15(1).16(1)(b).16(1)(c)		RCMP, CSIS	15(1).16(1)(b).16(1)(c)
	Number of tactical tools developed annually	Collated annually	15(1).16(1)(b).16(1)(c)		RCMP, CSIS	



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
						15(1),16(1)(b),16(1)(c)
Entry and Alternative capture trials/solutions	15(1),16(1)(b),16(1)(c)	Collated annually	15(1),16(1)(b),16(1)(c)		RCMP, CSIS	0 (RCMP)  15(1),16(1)(b),16(1)(c)
		Collated annually			RCMP, CSIS	
		Collated annually			RCMP, CSIS	

<sup>39</sup> Preliminary discussions were held with a third service provider, however there were insufficient funds to proceed with this project.



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
	15(1),16(1)(b),16(1)(c)					15(1),16(1)(b),16(1)(c)
		Collated annually	15(1),16(1)(b),16(1)(c)	N/A	CSE	15(1),16(1)(b),16(1)(c)
		Collated annually		N/A	CSE	15(1),16(1)(b),16(1)(c)
		Collated annually	15(1),16(1)(b),16(1)(c)	RCMP, CSIS	15(1),16(1)(b),16(1)(c)	

15(1),16(1)(b),16(1)(c)



Program outputs and outcomes	Indicator	Frequency	Baseline	Target	Organization responsible for data collection	Performance Results & Justification
	15(1),16(1)(b),16(1)(c)	Collated annually	15(1),16(1)(b),16(1)(c)		RCMP, CSIS	15(1),16(1)(b),16(1)(c)
Decryption and other cryptographic techniques		Collated annually	15(1),16(1)(b),16(1)(e)	N/A	CSE	15(1),16(1)(b),16(1)(c)

<sup>43</sup> Based on 2013-2014 input only.

15(1),16(1)(b),16(1)(c)

