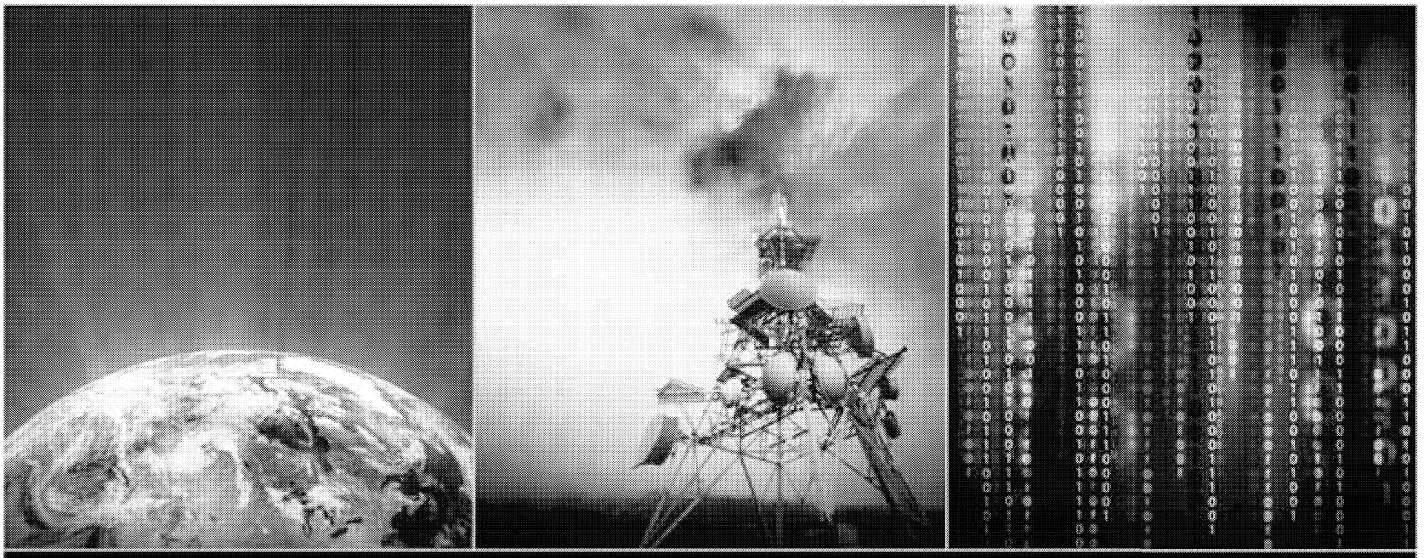
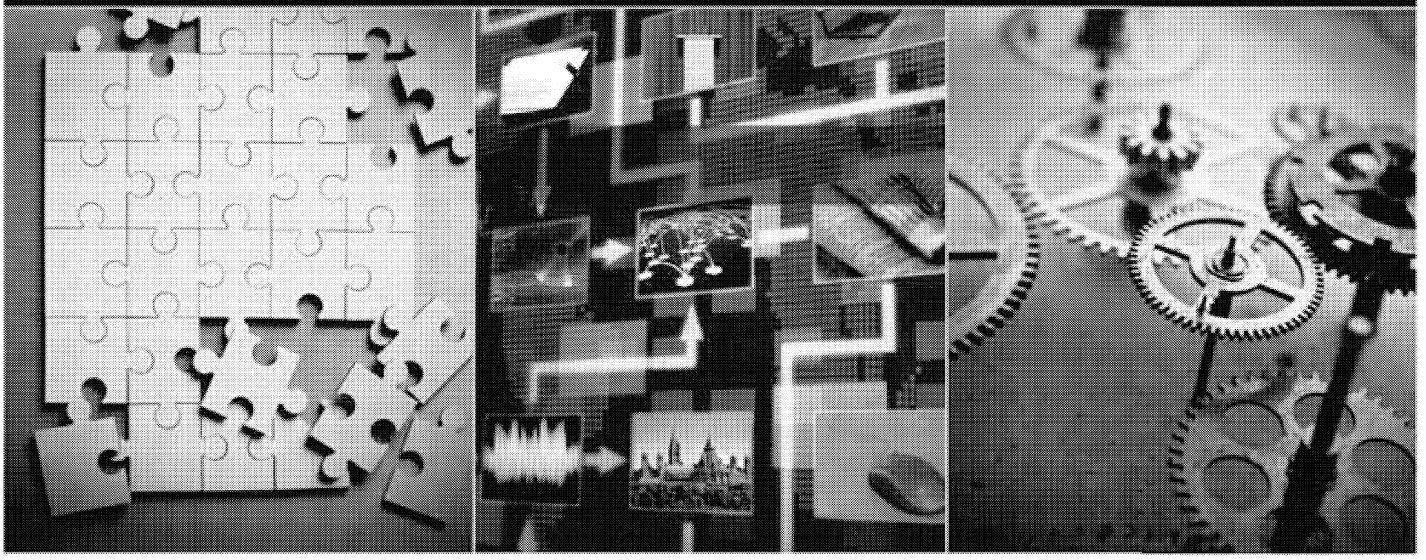
Communications Security Establishment | Centre de la sécurité des télécommunications



COMMUNICATIONS SECURITY ESTABLISHMENT

# ANNUAL REPORT TO THE MINISTER OF NATIONAL DEFENCE

## 2013–2014



Canada

October, 2014

Minister,

I am pleased to submit to you the Communications Security Establishment (CSE) Annual Report for fiscal year 2013–14. This annual report flows from the requirement outlined in CSE's Accountability Framework Ministerial Directive, requiring annual updates on CSE's performance, strategic priorities, program initiatives and other issues of significance. This year's report also includes an annex IRRELEVANT

This annual report details CSE's priorities and challenges over the past year, highlights our key accomplishments and addresses a number of special reporting requirements. It also outlines some of our intentions and efforts as we move forward in an ever-evolving operational and policy environment.

Throughout 2013–14, the organization's activities focused on supporting the Government of Canada's (GC) intelligence priorities, namely Cabinet Confidence Cabinet Confidence Our work directly impacted GC decision making and supported Canadian and Five Eyes partner efforts to respond to a variety of situations. Some of CSE's unique contributions over the past year include:

- [redacted]

All of these efforts were made more challenging by the continued unauthorized disclosures of classified information. CSE led the government's response to these disclosures, including addressing the damage and impacts to Canada, enhancing internal personnel security, and improving IT Security across our organization. We continue to see significant challenges as a result of these disclosures, including the changes in target behaviours.

Throughout 2013–14, CSE responded to an unprecedented number of media inquiries, participated in numerous Parliamentary appearances, and provided more public information on our activities than ever before. Following multiple classified and public Office of the CSE Commissioner (OCSEC) reviews, the Commissioner continued to find CSE activities to have been conducted in a lawful manner. Moreover, the Commissioner concluded that CSE is committed to protecting the privacy of Canadians. CSE will continue these efforts in order to establish more transparency as an agency and to enhance its public profile.

Fiscal Year 2013–14 was also marked by the completion of the exterior shell and the design and development of CSE's new facility. Substantial progress was made in the construction and interior fit up of CSE's new facility. The facility has reached full completion with employees scheduled to move into the new facility beginning in October 2014.

In the coming year, I am committed to seeing CSE continue to successfully support the Government's intelligence priorities and protect information and information systems of importance to the GC. Our priorities include:

- Providing a quick, flexible response capacity to meet the Government's intelligence needs in responding to emerging terrorist threats and global incidents such as the [redacted]
- Cultivating closer operational and policy collaboration with GC partners on domestic and international cyber issues of concern to the Government and in accord with Cabinet direction;
- Continuing to ensure that the privacy of Canadians or anyone within Canada is protected in the course of signals intelligence (SIGINT) and information technology security (ITS) operations and reporting;
- Remaining fully cooperative with and accountable to independent external review;
- Engaging the public as well as Parliament in order to establish greater transparency regarding CSE's activities and measures to protect the privacy of Canadians;
- Moving CSE, its employees, and equipment to the new facility;
- Continuing to foster a better relationship with private industry, with a particular focus on partnering to combat cyber threats targeting Canadian systems;
- Continuing to work with other departments to implement and strengthen Canada's cyber security strategy; and,
- Enhancing security at CSE and delivery of the Canadian Top Secret Network (CTSN) to GC partners.

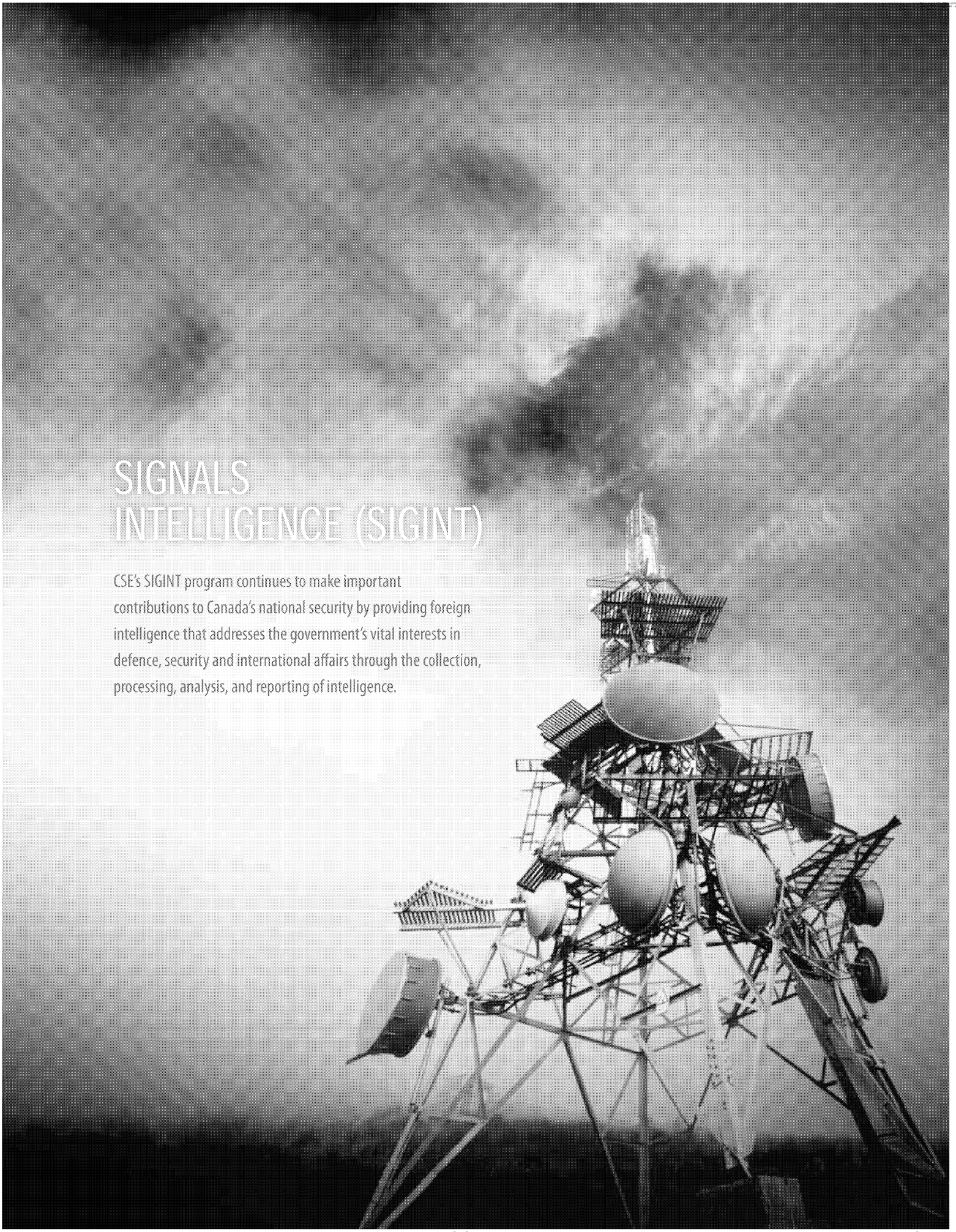
CSE made significant contributions to the GC's security and intelligence priorities in 2013–14. We look forward to continuing to help protect the security of Canada and Canadians in the year ahead.

Sincerely,

**John Forster**
*Chief*

# TABLE OF CONTENTS

## LIST OF 2013–2014 HIGHLIGHTS



# SIGNALS INTELLIGENCE (SIGINT)

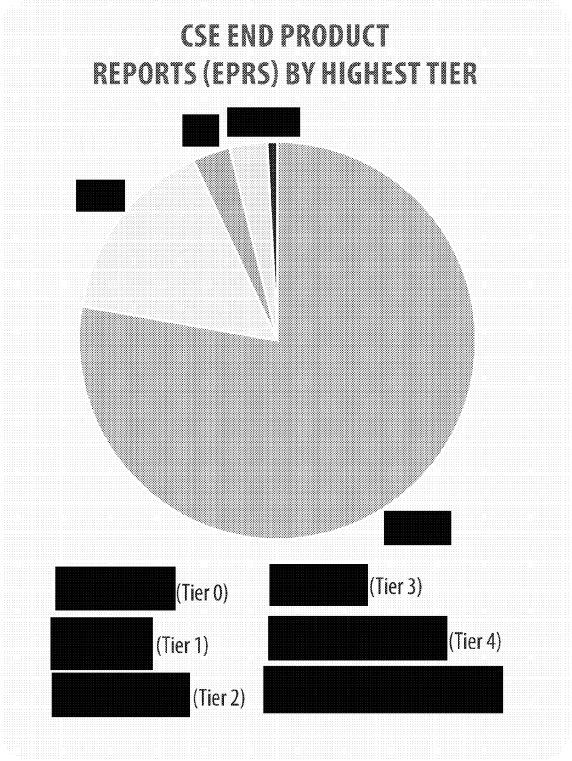
CSE's SIGINT program continues to make important contributions to Canada's national security by providing foreign intelligence that addresses the government's vital interests in defence, security and international affairs through the collection, processing, analysis, and reporting of intelligence.

## REPORTING ON INTELLIGENCE PRIORITIES

CSE activities in 2013–14 remained focused on the following GC intelligence priorities, which did not change from those selected in 2012–13:

Cabinet Confidence

In 2013–14, CSE issued [redacted] intelligence reports (known as End Product Reports, or EPRs) in line with GC intelligence priorities. Of those reports, 78 percent [redacted] addressed high importance [redacted] priorities to the GC.




Statistics on feedback from CSE's EPR recipients will be provided in this section on the degree to which the reports were read, satisfied an intelligence need, were rated as exceptional, or provided actionable intelligence[2].

Cabinet Confidence

Cabinet Confidenc are the most immediate potential source of harm to Canadians and Canadian interests that intelligence can help mitigate effectively. Canada is a target of Cabine at home and abroad, and intelligence produced under this priority helps ensure that Cabin threats to Canada, Canadians and our allies are pre-empted.

In 2013–14, SIGINT focused its intelligence collection on [redacted]

This past year, SIGINT efforts monitored Cabinet Co activities, supported the Canadian Armed Forces (CAF) and International Security Assistance Force (ISAF) in Afghanistan, contributed to the conviction of Cabin kidnappers, and supported other ongoing efforts related to kidnappings and hostage situations involving Canadians abroad.

Key clients include the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), Department of National Defence (DND), and the Department of Foreign Affairs, Trade and Development (DFATD), along with allied military and intelligence services.

1 This figure represents total EPRs issued. Note that one EPR may be attributed to multiple intelligence priorities, e.g. a single EPR may be attributed to both Cabinet Confidence

2 SIGINT reports graded "Actionable" intelligence have: a) identified a threat to Canadian and/or allied interests, b) resulted in significant action being taken by the GC, or c) significantly influenced decisions by the GC, the CAF or an allied government.

## SIGINT MONITORING OF [redacted]

Under Operation [redacted] CSE and CSIS partnered to corroborate [redacted]

In its continued efforts to provide support related to kidnappings and hostage situations involving Canadians abroad, CSE collaborated with domestic and foreign counterparts and regularly exchanged information. For example, a SIGINT-led operation provided Second Party[3] partners new information that enabled the [redacted] The operation used SIGINT [redacted] CSE [redacted] contributions also provided greater situational awareness of the [redacted]

| Cabinet Confidence | [redacted] |
|---|---|
| # of EPRs | [redacted] |
| As % of CSE SIGINT Production | [redacted]% |
| % of EPRs Read by at Least One Client | 99% |
| % of EPRs Rated as Satisfied Need | 74% |
| % of EPRs Rated as Exceptional | 32% |
| % of EPRs Rated as Actionable Intelligence (AI) | 9% |

Cabinet Confide

Cabinet Confidence

Cabinet Cor Intelligence produced under this priority identified [redacted]

4 [redacted]

5

3 Second Party refers to CSE's Five Eyes partnerships with NSA, GCHQ, GCSB and ASD.

[redacted]

Cabinet Confidenc[redacted]

| | |
|---|---|
| # of EPRs | [redacted] |
| As % of CSE SIGINT Production | [redacted]% |
| % of EPRs Read by at Least One Client | 87% |
| % of EPRs Rated as Satisfied Need | 50% |
| % of EPRs Rated as Exceptional | 20% |
| % of EPRs Rated as Actionable Intelligence (AI) | 7% |

**NOTE:** Given the time-sensitive nature of [redacted] SIGINT issued fewer EPRs in favour of an automated [redacted] system [redacted] detailed later in this report.

Cabinet Confidence

It is a GC objective to Cabinet Confidence

Cabinet Confidence This means [redacted] Intelligence produced under this priority assisted the GC and Canadian [redacted] by providing unique insight into the [redacted]

In 2013–14, SIGINT reporting supported Canada's highest priority [redacted]

## SIGINT REPORTING ON

[redacted]

SIGINT reporting also supported Canada's [redacted]

## ACTIONABLE REPORTING ON [redacted]

[redacted]

Cabinet Confidence

| | |
|---|---|
| # of EPRs | [redacted] |
| As % of CSE SIGINT Production | [redacted]% |
| % of EPRs Read by at Least One Client | 99% |
| % of EPRs Rated as Satisfied Need | 82% |
| % of EPRs Rated as Exceptional | 42% |
| % of EPRs Rated as Actionable Intelligence (AI) | 8% |

Cabinet Confidence

Cabinet Confidence [redacted]

[redacted]

In 2013–14, SIGINT collection in support of the Cabi intelligence priority focused on:

- [redacted]
- [redacted]
- [redacted]

## SIGINT REPORTING ON [redacted]

[redacted]

## PRECISE REPORTING ON [redacted]

[redacted]

Cabinet Confidence

| | |
|---|---|
| # of EPRs | [redacted] |
| As % of CSE SIGINT Production | [redacted]% |
| % of EPRs Read by at Least One Client | 99% |
| % of EPRs Rated as Satisfied Need | 81% |
| % of EPRs Rated as Exceptional | 31% |
| % of EPRs Rated as Actionable Intelligence (AI) | 6% |

Cabinet Confidence

Cabinet Confidence [redacted]

[redacted]

## SIGINT AND CSIS COLLABORATIVE INVESTIGATION ON [redacted]

[redacted]

Cabinet Confidence

| | |
|---|---|
| # of EPRs | [redacted] |
| As % of CSE SIGINT Production | [redacted]% |
| % of EPRs Read by at Least One Client | 81% |
| % of EPRs Rated as Satisfied Need | 56% |
| % of EPRs Rated as Exceptional | 27% |
| % of EPRs Rated as Actionable Intelligence (AI) | 6% |

Cabinet Confidence

Cabir[redacted]

[redacted]

## SIGINT MONITORING OF [redacted]

[redacted]

## SIGINT-CSIS COLLABORATION TO ENHANCE

[redacted]

## SIGINT-GCHQ COOPERATION

[redacted]

Cabinet Confidence [redacted]

| | |
|---|---|
| # of EPRs | [redacted] |
| As % of CSE SIGINT Production | [redacted]% |
| % of EPRs Read by at Least One Client | 100% |
| % of EPRs Rated as Satisfied Need | 48% |
| % of EPRs Rated as Exceptional | 57% |
| % of EPRs Rated as Actionable Intelligence (AI) | 19% |

Cabinet Confidence

Cabinet Confidence [redacted]

[redacted]

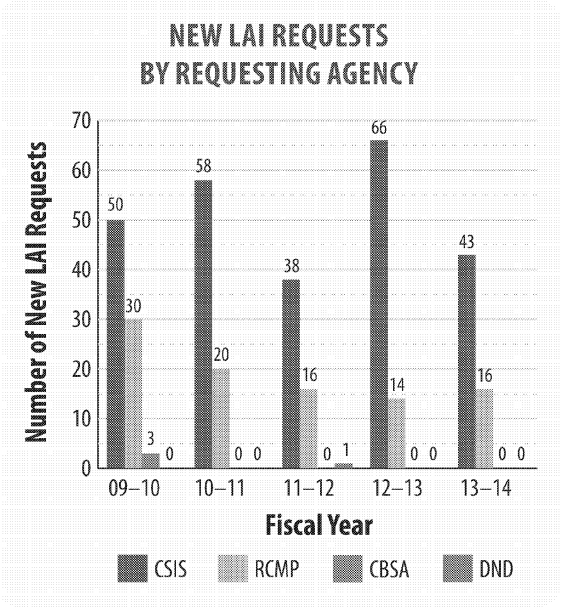
Cabinet Confidence

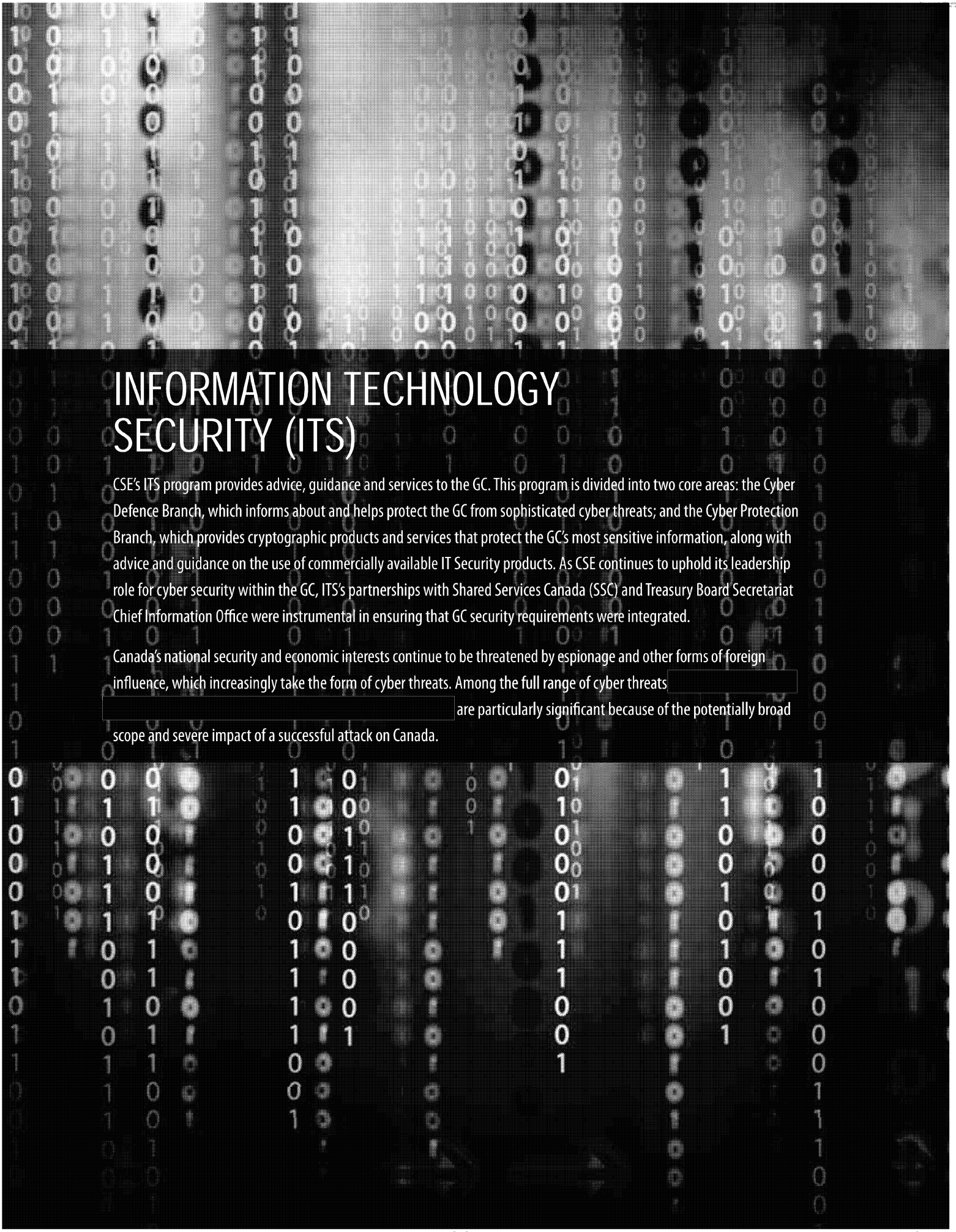
| | [redacted] |
|---|---|
| # of EPRs | [redacted] |
| As % of CSE SIGINT Production | [redacted]% |
| % of EPRs Read by at Least One Client | 100% |
| % of EPRs Rated as Satisfied Need | 90% |
| % of EPRs Rated as Exceptional | 46% |
| % of EPRs Rated as Actionable Intelligence (AI) | 13% |

IRRELEVANT

IRRELEVANT

to CSIS. In November 2013, the Federal Court questioned CSIS' authority to engage the collection resources of Second Party allies to intercept the private communications of Canadians under the general power to investigate under section 12 of the *CSIS Act*. Pending the appeal decision, CSIS requested that CSE limit its collection activities authorised by DIFTS to Canadian collection sites.





# INFORMATION TECHNOLOGY SECURITY (ITS)

CSE's ITS program provides advice, guidance and services to the GC. This program is divided into two core areas: the Cyber Defence Branch, which informs about and helps protect the GC from sophisticated cyber threats; and the Cyber Protection Branch, which provides cryptographic products and services that protect the GC's most sensitive information, along with advice and guidance on the use of commercially available IT Security products. As CSE continues to uphold its leadership role for cyber security within the GC, ITS's partnerships with Shared Services Canada (SSC) and Treasury Board Secretariat Chief Information Office were instrumental in ensuring that GC security requirements were integrated.

Canada's national security and economic interests continue to be threatened by espionage and other forms of foreign influence, which increasingly take the form of cyber threats. Among the full range of cyber threats [redacted] are particularly significant because of the potentially broad scope and severe impact of a successful attack on Canada.

## CYBER DEFENCE

In 2013–14, the Cyber Defence Branch continued to evolve efforts to find defensive solutions to prevent, detect, and defend against threats.

### *Dynamic Defence*

[redacted]

**DYNAMIC DEFENCE** [redacted]

[redacted]

[redacted]

### *Year-over-Year Trending*

In 2013, CSE's Cyber Threat Evaluation Centre detected [redacted] instances of [redacted] cyber activity against the GC, affecting [redacted] different departments. Of these incidents, [redacted] were identified as compromises; [redacted] of which resulted in data being exfiltrated. A compromise occurs when malware is successfully installed but no data leaves the network. Exfiltration is a more serious form of compromise, which occurs when a threat actor exports (i.e. steals) data from a network. This typically consists of network information and/or user credentials, both of which can be used to launch future intrusion attempts.

**Numbers and Types of Successful [redacted] Cyber Incidents at GC Departments: 2011–2013**

| YEAR | INCIDENTS | DEPARTMENTS | EXFILTRATIONS | COMPROMISES |
|---|---|---|---|---|
| 2011 | [redacted] | | | |
| 2012 | | | | |
| 2013 | | | | |

[redacted]

## MONITORING CYBER CRIME

In 2012, CSE expanded its monitoring to include publicly available [redacted]

Over the past three years, [redacted] consistently been the most targeted by cyber threat actors.

### *ITS Cyber Threat Intelligence Reports and Assessments*

ITS continued to produce and develop cyber threat intelligence reports, including the [redacted]

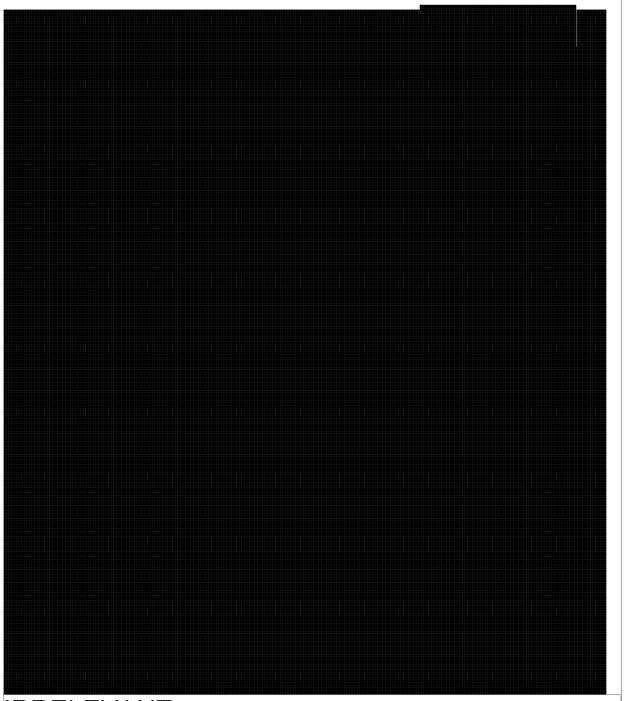
In addition to producing these regular tactical reports, ITS also launched a strategic assessment team to produce high level cyber threat assessments for the GC's Deputy Minister community. These reports have established ITS's credibility as an expert source of trending and sophisticated analysis for the GC.

## CYBER PROTECTION

IRRELEVANT

IRRELEVANT

IRRELEVANT



IRRELEVANT

IRRELEVANT

[redacted]

[redacted]

IRRELEVANT

# ADDITIONAL ISSUES OF SIGNIFICANCE

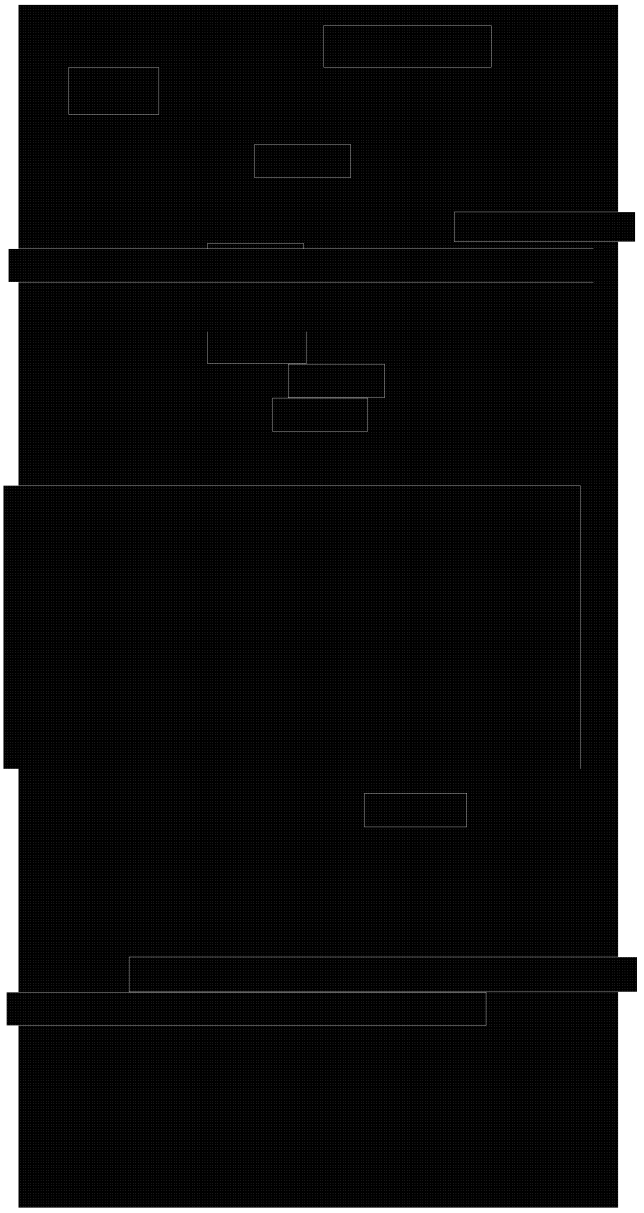
## SIGINT AND IT SECURITY COLLABORATION

In order for CSE to meet its mandate, collaboration is vital. Over the past year, SIGINT and ITS have continued to work together to increase efficiencies and develop partnerships.

In order to fortify cyber initiatives, SIGINT and ITS work closely to exchange data and analyses

[redacted]

[redacted]



## EXTERNAL REVIEW FOR LAWFULNESS

The CSE Commissioner provides independent review of CSE's activities to ensure compliance with the law and the protection of the privacy of Canadians. The Commissioner also undertakes any investigation deemed necessary into a complaint about CSE activities. As with other federal agencies, CSE is also subject to external review and audit by independent organizations including the Privacy Commissioner, the Auditor General, the Information Commissioner and Commissions of Inquiry.

This past year, CSE provided information to the CSE Commissioner to support eleven reviews and one study. Five reviews and one study were completed during the 2013–14 timeframe. Those reviews and studies are as follows:

- Review of CSE foreign signals intelligence information sharing with international partners;
- Review of the activities of the CSE Office of Counter Terrorism;
- Review of CSE 2012–13 foreign signals intelligence ministerial authorizations;
- Annual review of a sample of disclosures by CSE of Canadian identity information to GC clients and Second Party partners;
- Annual review of incidents and procedural errors identified by CSE in 2013 that affected or had the potential to affect the privacy of Canadians and measures taken by CSE to address them; and
- Study of CSE policy compliance monitoring framework and related activities.

The CSE Commissioner provided ten recommendations as a result of these reviews, all of which CSE accepted.

## AUTHORITIES

CSE's operations are made possible by Ministerial Directives (MD) and Ministerial Authorizations (MA). Under the *National Defence Act*, the Minister of National Defence (MND) issues written MDs, which instruct CSE with regard to its duties and functions. Additionally, CSE annually requests approval from the MND for several MAs to authorize certain activities that are required for it to fulfill its mandate, that would risk interception of private communications (PC)[8].

8 PCs are those that originate or terminate in Canada and where the originator has a reasonable expectation of privacy.

## INTERNATIONAL INFORMATION SHARING

In 2011, CSE was issued a MD on the *Framework for Addressing Risks in Sharing Information with Foreign Entities*. This MD aimed to balance CSE's mandate to share information, with the Government's obligations under international and domestic laws to ensure that it is not complicit in the mistreatment of any person.

From this MD, CSE implemented a process for sharing information either directly or indirectly with foreign entities [redacted] The process enables CSE to assess and mitigate, where possible, the potential risks of sharing information, and necessitates that the approval levels to share information must be proportionate to the risk of mistreatment that would result (i.e. the greater the risk, the more senior the level of approval required). In 2013–14, CSE formalized its practices for information sharing through its Second Party counterparts in a policy instrument.

CSE utilized the process in [redacted] instances in 2013–14.

The SIGINT program used this process to implement the MD in cases where CSE shared information directly with [redacted] foreign entities. Over this past year, SIGINT continued to apply caveats and wording to in order to restrict how these MND-approved [redacted] disseminate and utilize CSE reports within their national channels.

IRRELEVANT

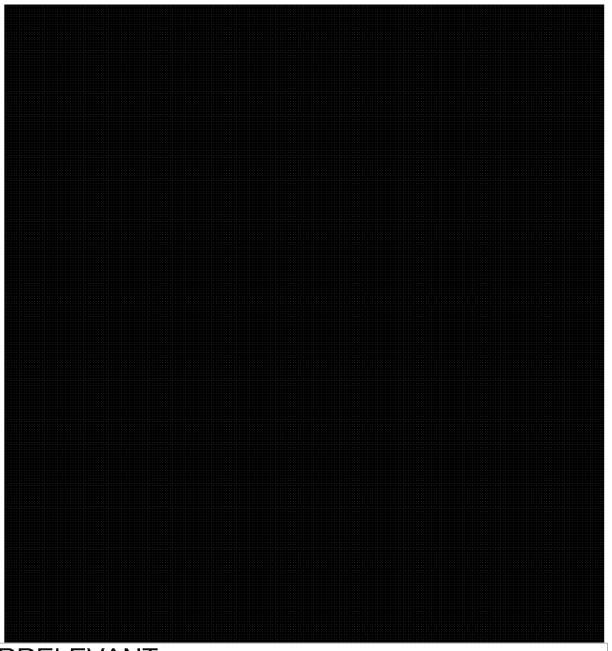
IRRELEVANT

### *Five Eyes*

CSE's cooperation with its Five Eyes partners is part of the foundation of its ability to provide valuable intelligence to the GC. As part of this effort, SIGINT actively looks to reuse and share technology between partners and collaborates closely in the areas of [redacted]

IRRELEVANT

SIGINT leveraged this partnership to fill operational gaps and broaden its dissemination of foreign intelligence. In 2013–14, CSE worked with partner agencies on the response to the unauthorized media disclosures of SIGINT material [redacted] Five Eyes partners cooperated to assess damage, mitigate the impact on collection, manage [redacted] concerns, and share lessons learned in media relations. The Five Eyes community also worked effectively on the [redacted]

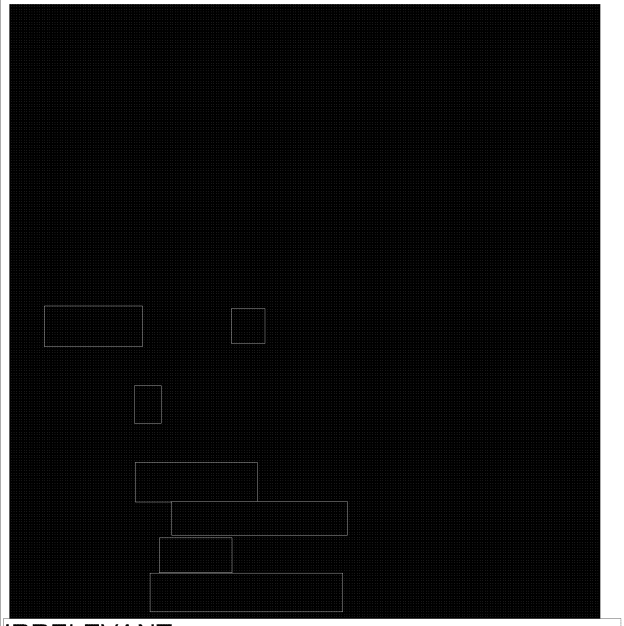


IRRELEVANT

IRRELEVANT

## *Raising Awareness of the Insider Threat*

As part of its contribution to the Five Eyes Safeguarding initiative, CSE tailored its security education and awareness program to four key audiences: new employees, staff, managers, and students. The curriculum is now being revised to include updated presentations, printed guides and reference materials, targeted workshops, and a video specific to insider threat issues. In 2013–14, approximately 1,200 employees attended security awareness training sessions.



IRRELEVANT

IRRELEVANT

[redacted]

Corporate Security responded to recent unauthorized disclosures by undertaking prioritized assessments of more than [redacted] employees at higher risk of exposure from the leaks, and by implementing a series of reinforcements to processes that impact [redacted] personnel. These reinforcements include increased access to intelligence reporting around counter-intelligence threats; the incorporation of risks directly stemming from [redacted] in [redacted] security briefings; and a redefinition of working relationships with partners in operational areas. When considering the scale of potential compromise to employee identities as a result of the disclosures, CSE considers these strengthened practices as enduring aspects of personnel security.

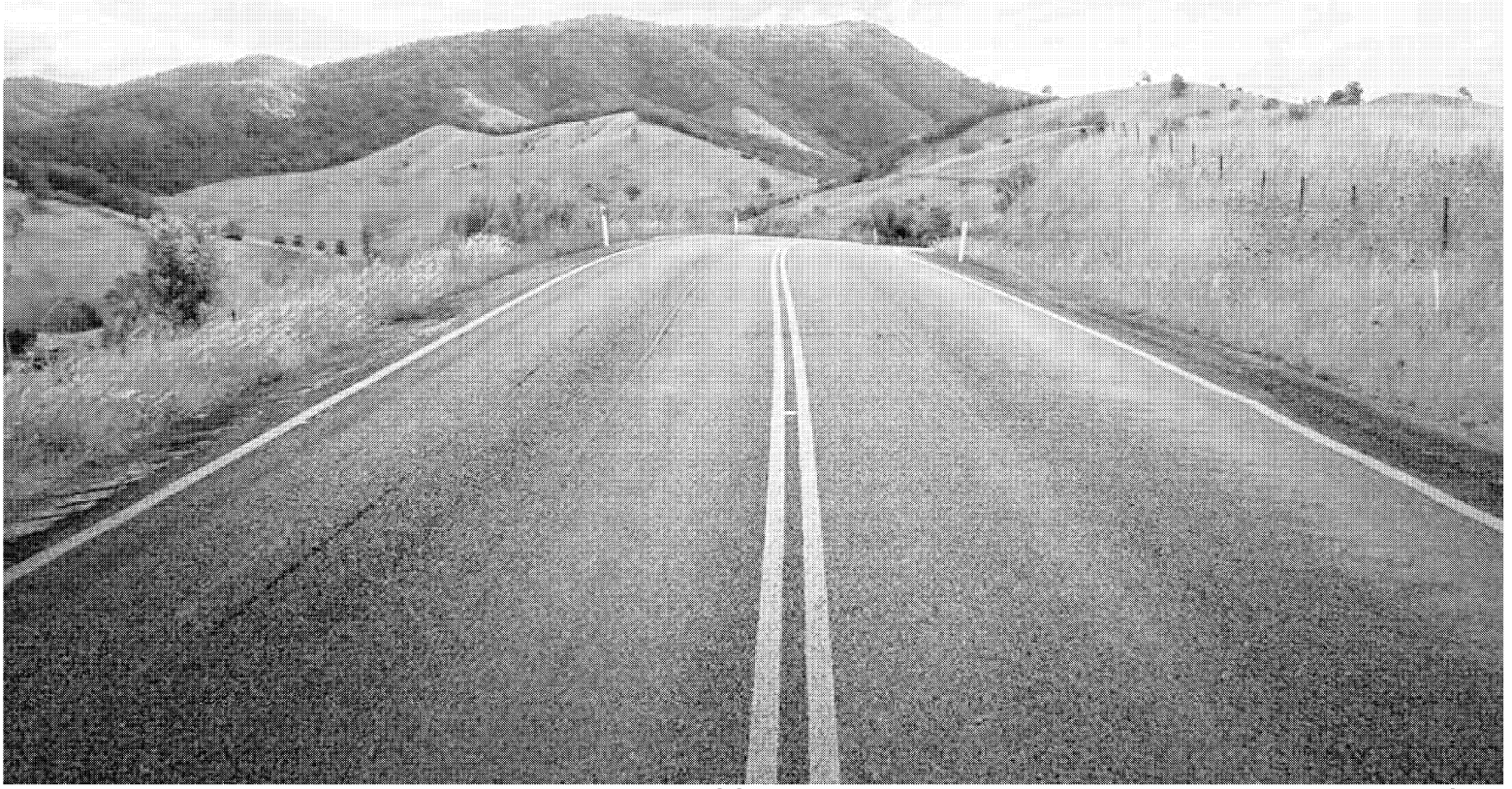
IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

# CONCLUSION



CSE highlights from 2013–14 include:

- CSE actionable intelligence gathered on [redacted] The intelligence gathered allowed GC clients to act promptly and ultimately [redacted]
- The precise and detailed intelligence collected by CSE on [redacted] This in turn supported the activities of DND, CSIS, the RCMP [redacted]
- The valuable CSE reporting on [redacted]
- The deployment of [redacted] on Shared Services Canada's secure channel network;
- IRRELEVANT
- 

Looking forward to 2014-15, CSE will continue to work to effectively address the evolving cyber threat; continue to ensure that the privacy of Canadians or anyone within Canada is upheld while conducting mandated activities; IRRELEVANT and demonstrate to the international community the GC's commitment to priorities such as Cabinet Confidence Cabinet Conf

CSE will continue to support GC Intelligence Priorities and will report against these priorities and its ongoing efforts to safeguard Canada's security through information security in next year's annual report.

# ANNEX A: LIST OF CURRENT CSE MINISTERIAL AUTHORIZATIONS AND DIRECTIVES

## *Ministerial Authorizations*[1]

Signals Intelligence Ministerial Authorizations

- [redacted] Collection Activities
- [redacted] Collection Activities
- [redacted] Collection Activities

Information Technology Security Ministerial Authorizations

- Cyber Defence Activities

## *Ministerial Directives*[2]

- Accountability Framework (November 2012)
- Privacy of Canadians (November 2012)
- IRRELEVANT
- [redacted] Operations (January 2002)
- [redacted] Program (March 2004)
- Integrated Signals Intelligence (SIGINT) Operational Model (May 2004)
- Collection and Use of Metadata (November 2011)
- IRRELEVANT
- [redacted] (August 2006)
- IRRELEVANT
- Intelligence Priorities (updated annually)
- Risks in Foreign Information Sharing (November 2011)

1 Ministerial Authorizations have a designated duration of one year; however approval may be sought annually for Ministerial Authorizations addressing an activity or class of activities required on a continuing basis. This list reflects current titles for each activity or class of activities.

2 CSE also has six Exceptionally Controlled Information Ministerial Directives (not listed) that deal with highly-sensitive SIGINT initiatives.

## ANNEX B: SPECIAL REPORTS

In addition to areas covered under the 2001 Ministerial Directive on CSE's Accountability Framework (performance, strategic priorities, program initiatives, and important policy, legal and management issues), CSE is also required to report on other specific issues. This Annex features special reports required either by Ministerial Directive or in response to OCSEC recommendations.

**Special Report** Integrated SIGINT Operational Model and the Mission in Afghanistan
**Obligation** 2004 Integrated SIGINT Operational Model Ministerial Directive

---

**Special Report** [redacted]
**Obligation** 2002 [redacted] Operations Ministerial Directive

---

**Special Report** [redacted]
**Obligation** 2012 [redacted] Ministerial Directive

---

**Special Report** [redacted]
**Obligation**

---

**Special Report** [redacted]
**Obligation** 2006 [redacted] Ministerial Directive

---

**Special Report** IRRELEVANT
**Obligation**

---

**Special Report** Privacy of Canadians
**Obligation** Voluntary – Response to recommendations from the Office of the CSE Commissioner

---

**Special Report** IRRELEVANT
**Obligation**

## SPECIAL REPORT: INTEGRATED SIGINT OPERATIONAL MODEL (ISOM) AND THE MISSION IN AFGHANISTAN

The ISOM represents the enhanced relationship between CSE and the Canadian Forces Information Operations Group (CFIOG). As of May 2004, under Ministerial Direction, the model established an integrated accountability framework for SIGINT operations. Prior to the model being established CFIOG was the primary authority for CAF-related SIGINT activities. Under the new model, except for deployed CAF operations, management and direction of SIGINT activities is provided by CSE.

In 2013–14, CSE launched a formal evaluation of ISOM to assess whether it aligns with future collaborative partnership goals of CSE and DND/CAF. The findings of that evaluation will help optimize partnership efforts, including support to military cyber operations.

While many of the CAF/CSE SIGINT processes and procedures are aligned, work continues to synchronize joint intelligence requirements. Since both the CAF Chief of Defence Intelligence (CDI) and CSE receive separate MDs on annual GC intelligence priorities, the alignment of the effort to satisfy these GC needs is critical to maximize SIGINT efficiency.

Over the past year, Canadian SIGINT remained an important element to enhance [redacted] the Canadian contribution to the [redacted] mission in Afghanistan [redacted] The ISOM challenge remains in sustaining and replicating the successes achieved in supporting deployed operations and moving forward to new challenges in 2014.

## SPECIAL REPORT: [redacted]

[redacted]

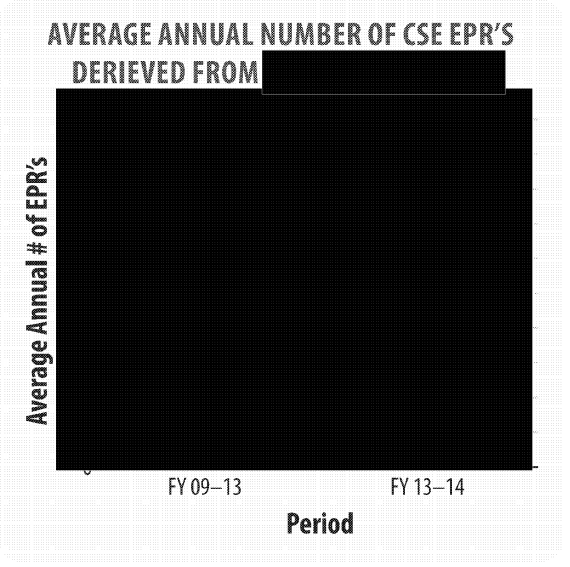
[redacted]

[redacted]

[redacted]

## SPECIAL REPORT: [redacted]

[redacted]



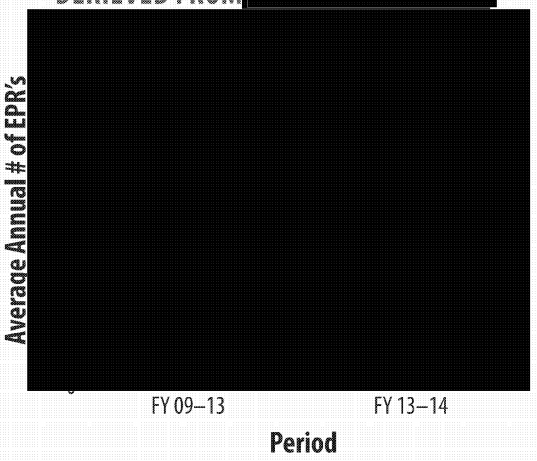
During 2013–14, CSE's Five Eyes partners produced [redacted] reports derived from this [redacted] program. This is a [redacted] percent [redacted] over the previous four fiscal years. Allied reports from this source were viewed by CSE clients in [redacted] government departments and agencies, providing intelligence that predominantly related to the GC's Cabinet Confidence and the Cabinet Confidence

[redacted]

## SPECIAL REPORT: [redacted]

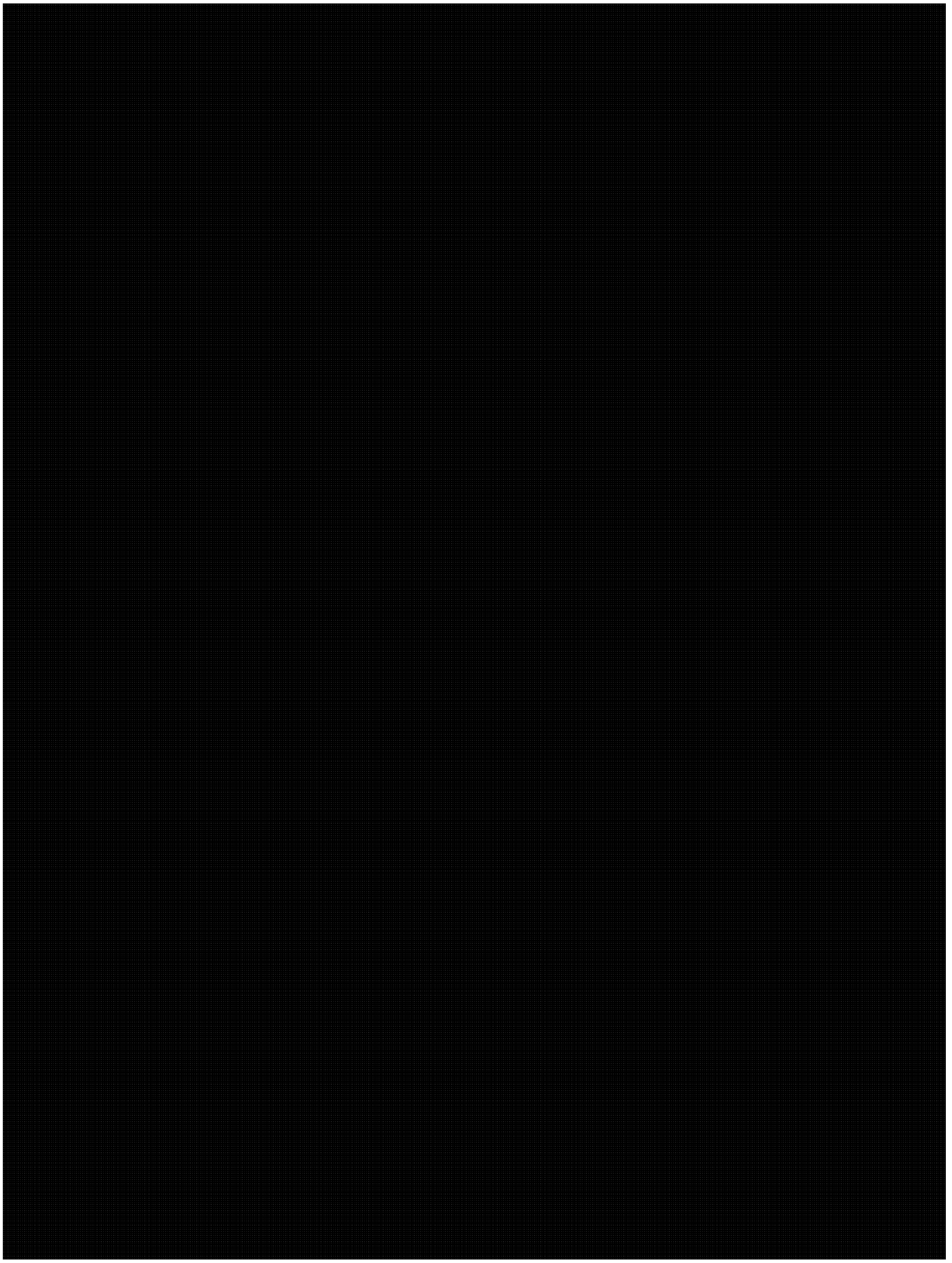
[redacted]

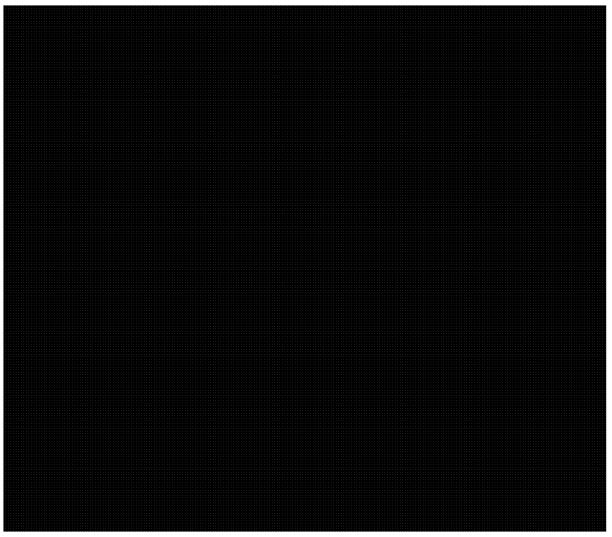
**AVERAGE ANNUAL NUMBER OF ALLIED EPR'S DERIVED FROM [redacted]**




## SPECIAL REPORT: [redacted]

[redacted]





IRRELEVANT

## SPECIAL REPORT: PRIVACY OF CANADIANS

As outlined in the *National Defence Act*, CSE is prohibited from directing foreign intelligence or ITS activities at Canadians or any person in Canada. Protecting the privacy of Canadians is an issue of paramount importance to CSE.

In 2013–14, CSE initiated a review of its operational policies in order to assess and strengthen existing measures to protect the privacy of Canadians in the use and retention of information. The Ministerial Directive on Privacy requires CSE to review its policies in light of significant technological changes.

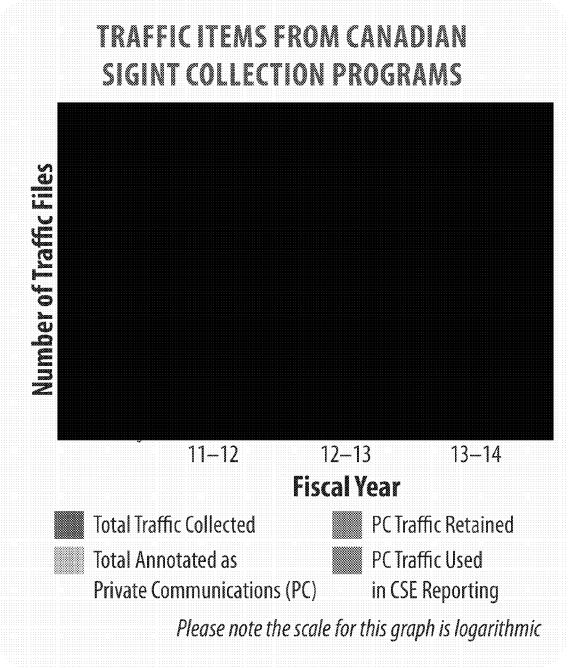
### *Canadian Identity Information*

From the intelligence reports produced by CSE and our Second Party allies, pieces of Canadian identity information were released to GC departments. This marked increase from the previous year is explained by the release of The release of this information allowed to notify the affected Canadian victims so that they could take appropriate actions to prevent further malicious activity by removing the malicious code and correcting the vulnerability that allowed the exploit to take place. Apart from this release, pieces of Canadian identity information were released, in 2012-2013. Of the the releases to CSIS accounted for approximately % of the total, or The remainder of the releases, were sent to other GC departments within the security and intelligence community (i.e. RCMP, CBSA, DND, DFATD, Public Safety Canada, Integrated Threat Assessment Centre, Financial Transactions and Reports Analysis Centre, Canadian Nuclear Safety Commission). CSIS continues to be CSE's main recipient of Canadian identity information, more than any other GC department.

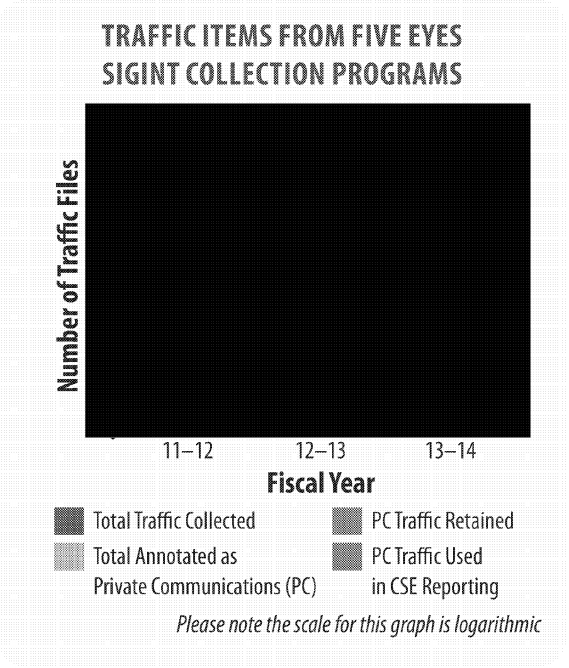
In 2013–14, Second Parties requested Canadian identities, of which were released. This is a from the previous year, when were released; however, during the previous year, of those releases were from a single cyber defence report.

### *Second Party Information Sharing and Privacy*

This year, based on the OCSEC recommendation from the Second Party Information Sharing Review (2013), CSE SIGINT is including statistics on recognized Second Party collected PCs for 2013–14. As previously mentioned, PCs are those that originate or terminate in Canada and where the originator has a reasonable expectation of privacy. Upon recognition in CSE's traffic repositories, SIGINT analysts must annotate PCs for deletion if they do not contain any foreign intelligence value, or for retention if they do contain information of foreign intelligence value.




During fiscal year 2013–14, out of a total of [redacted] traffic files derived from Canadian SIGINT Collection Programs, there were [redacted] percent) traffic files that were annotated as being recognized as a PC. Of these, [redacted] percent) are currently annotated as containing FI, and [redacted] percent) of these were used in EPRs. [redacted] percent) traffic files were annotated as having no FI value, and were marked for deletion.




Out of a total of [redacted] Five Eyes collected traffic files that were shared with CSE, there were [redacted] percent) recognized PCs.

Of the total recognized Five Eyes collected PCs identified in 2013–14, [redacted] percent) were annotated as PC with FI value, and of these, [redacted] percent) were used in Canadian EPRs. The remaining [redacted] percent) PC traffic files were identified as PC with no FI value, and were marked for deletion.

IRRELEVANT

IRRELEVANT