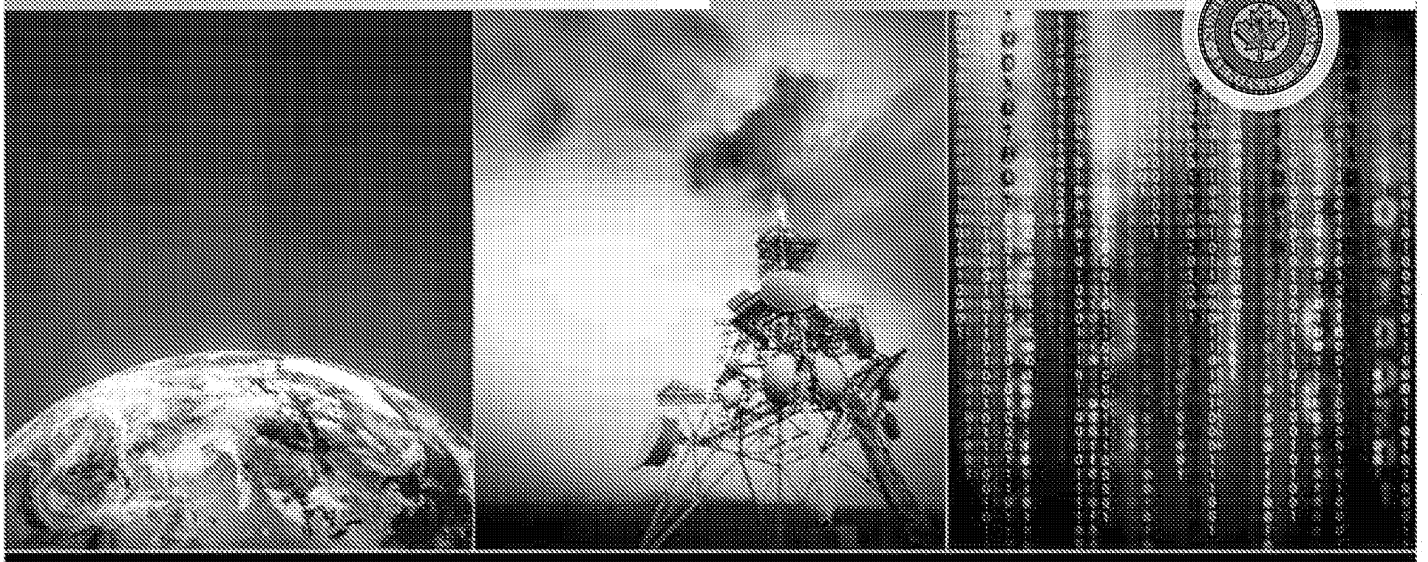
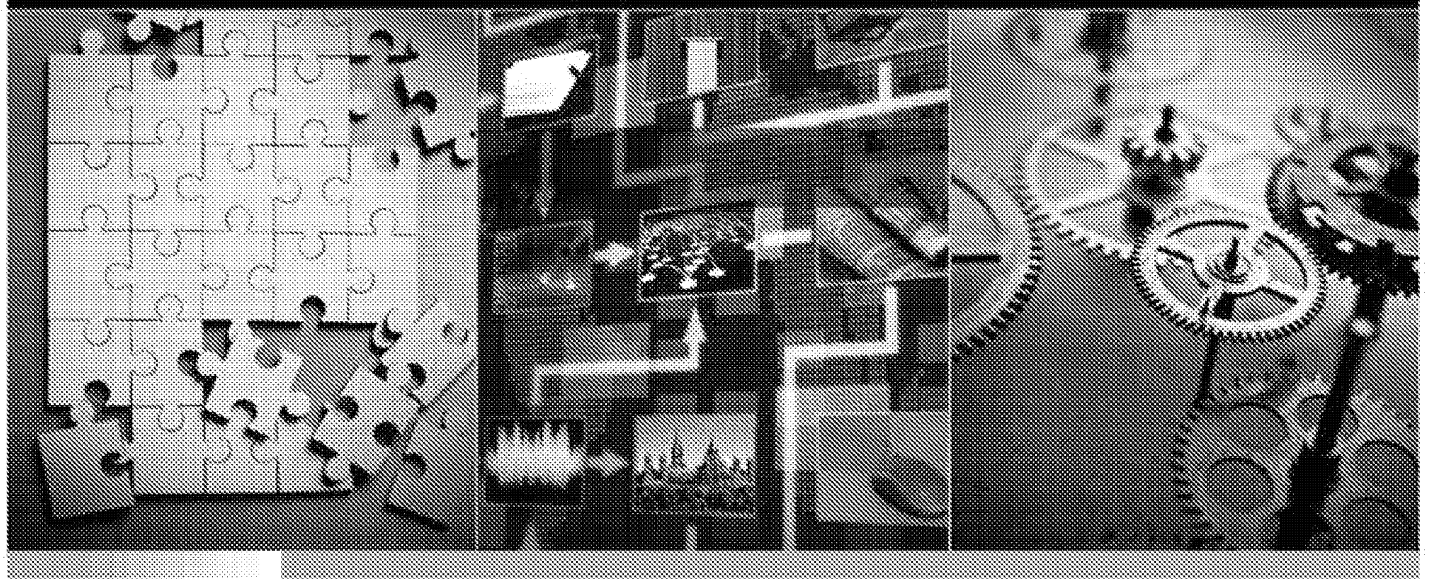
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada



COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

ANNUAL REPORT TO THE MINISTER OF NATIONAL DEFENCE

2012–2013



Canada

November 2013

Minister,

I am pleased to submit to you the CSEC Annual Report for fiscal year 2012–2013. This annual report flows from the requirement outlined in CSEC's *Accountability Framework* Ministerial Directive in which I have been directed to provide you with annual updates on CSEC's performance, strategic priorities, program initiatives and other issues of significance. Going forward, CSEC will be exploring ways in which this report can be coordinated and streamlined with our classified 2014–2015 Departmental Performance Report.

2012–2013 marked our first year as a stand-alone agency. This annual report details CSEC'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 planned efforts as we move forward in an ever-evolving operational and policy environment. Cabinet Confi

Cabinet Confidence

Throughout 2012–2013, CSEC has continued to develop and implement new capabilities to better fulfill its mandate of foreign signals intelligence collection, protection of information systems of importance to the Government of Canada, and provision of technical and operational assistance to federal law enforcement and security agencies. Specifically, the organization's activities were focused on the Government priorities related to Cabinet Confidence

Cabinet Confidence

Cabinet Confidence IRRELEVANT

IRRELEVANT

I am committed to seeing CSEC continue to successfully support the government's intelligence priorities and protect government information systems. In the coming year, our priorities include:

- providing a quick, flexible response capacity to meet the Government of Canada's intelligence needs in responding to emerging global incidents;
- expanding CSEC's [redacted] operations to deliver timely and high-quality foreign intelligence to meet Government of Canada priorities;
- continuing to invest in CSEC's [redacted] program, in order to maintain and expand capabilities in an increasingly challenging operating environment;
- Cabinet Confidence
- continuing to implement CSEC's responsibilities under the Government's *Cyber Security Strategy* such as ongoing work to strengthen the Government of Canada's cyber defence perimeter, in concert with the government-wide IT consolidation efforts headed by Shared Services Canada;

IRRELEVANT

CSEC made significant contributions to the government's security and intelligence priorities in 2012–2013. We look forward to continuing to help protect the security of Canada and Canadians in the year ahead.

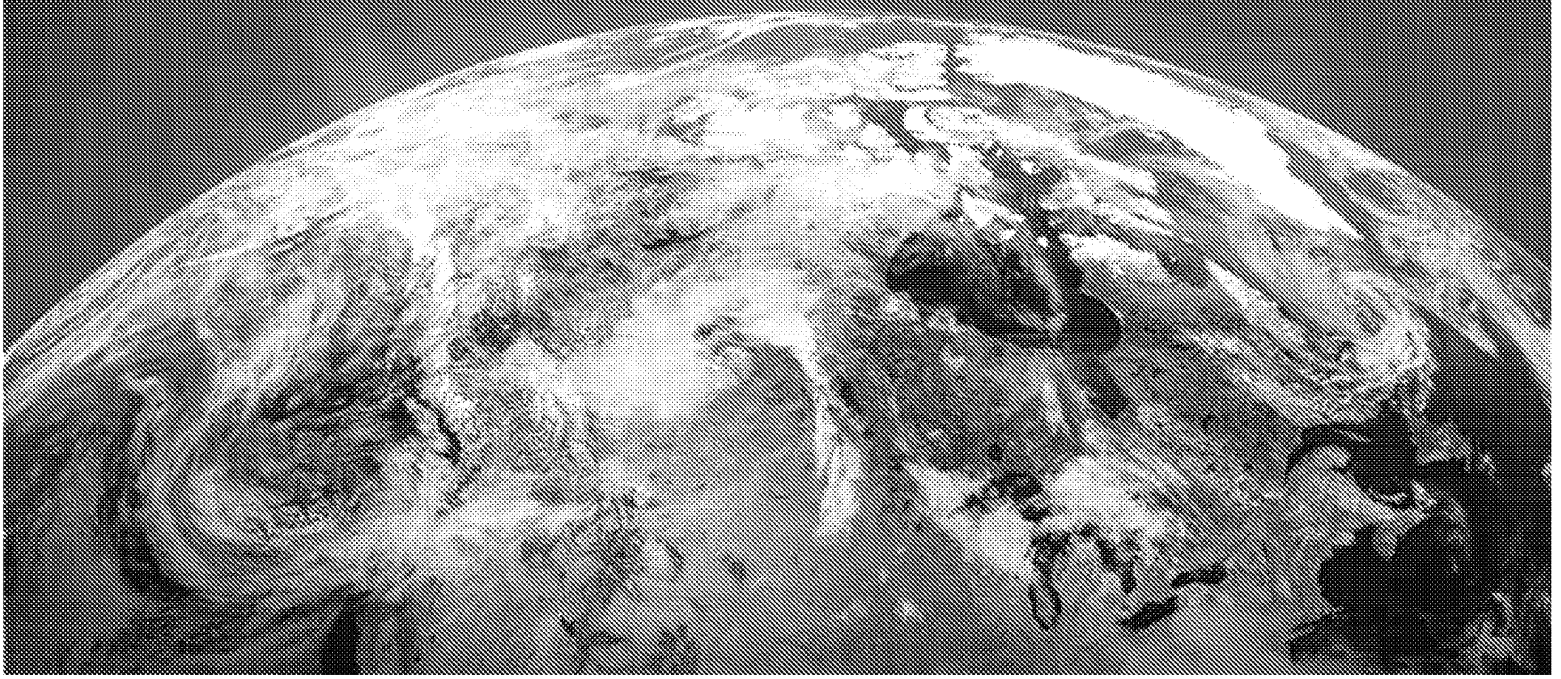
Sincerely,

John Forster
Chief

TABLE OF CONTENTS

LIST OF 2012–2013 HIGHLIGHTS

NATIONAL AND INTERNATIONAL CONTEXT



Important domestic and global events in 2012--2013 served to focus CSEC attention on a number of key security and intelligence (S&I) priorities, including [redacted] the evolving global cyber threat, as well as [redacted]

[redacted] and ties to terrorism continued to draw widespread concern from the international community in 2012--2013. Cabinet Confidence

Cabinet Confidence

[redacted]

International attention was also increasingly focused on the evolving global cyber threat this past year. In February 2013, Mandiant, a private US cyber security firm, released a report on the exponential scale of cyber threats and espionage that are being conducted against Western targets by the People's Republic of China's (PRC) military, the People's Liberation Army.

Cabinet Confidence

Cabinet Confidence [redacted]

[redacted]

Canada promoted its strategic interests through various multilateral fora in 2012--2013, including the [redacted] and the [redacted] Significantly, Canada was successful [redacted]

Canada continued efforts to Cabinet Confidence

Cabinet Confidence

Cabinet Confidence In the past year, the Government also identified a new Cabinet Confidence

Cabinet Confidence This priority served to focus attention on putting a stop to the Cabinet Confidence

Cabinet Confidence

[redacted]

With the death of Osama bin Laden in 2011, the nature of the terrorist threat has evolved, becoming more about shared ideologies among fractional groups or individuals and less about a single cohesive terrorist group. Although the combat mission in Afghanistan is now over, deployed Canadian Armed Forces (CAF) soldiers still face ongoing threats from Taliban insurgents in the region. Canada remains committed to countering the terrorist threat and supporting its allies.

IRRELEVANT

SIGNALS INTELLIGENCE

CSEC's SIGINT program made important contributions to Canada's national security that enhanced the protection of Canadian lives and interests in 2012-2013. The program provides 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

CSEC activities in 2012–2013 focused on the following Government of Canada intelligence priorities:

Cabinet Confidence

Cabinet Confidence

SIGINT provides actionable signals intelligence[1] for detecting and preventing [redacted] threats against North America, as well as against Canadian and allied interests abroad. Key clients include the Royal Canadian Mounted Police (RCMP), the Canadian Security Intelligence Service (CSIS), the Department of National Defence (DND), and the Department of Foreign Affairs, Trade and Development (DFATD), along with allied military and intelligence services.

In 2012–2013, SIGINT focused its intelligence collection on [redacted] groups or individuals whose activities or operations posed threats to Canadian or allied lives and interests, and direct threats to Canadian personnel, facilities and interests in Afghanistan.

This past year, SIGINT efforts led to the [redacted] groups' activities, the detection of extremist hackers, the continued support of the CAF in Afghanistan, and the support of ongoing efforts related to kidnappings and hostage situations involving Canadians abroad.

CSEC'S [redacted] TEAM DETECTS [redacted] HACKER

[redacted]

CSEC also provided support to the CAF in Afghanistan [redacted] teams were structured to meet a broad array of requirements, ranging from Cabinet Confidence in 2012–2013 CSEC's [redacted]

1 [redacted]

[redacted]

[redacted]

Cabinet Confid

CSEC produces intelligence on [redacted] to Canada and works to identify the actors behind [redacted] their doctrine, capability, intent, tactics and overall strategic approach.

[redacted]

CSEC continued to support efforts this past year related to kidnappings and hostage situations involving Canadians abroad, collaborating with domestic and foreign counterparts and regularly exchanging information. In particular, SIGINT continued to support [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

CSEC contributes foreign intelligence to support the Government's [redacted] including [redacted]

[redacted]

In 2012--2013, CSEC provided support for key events including the [redacted] to ensure the passage of timely and relevant intelligence and to support situational awareness. SIGINT also produced reports in support of Canada's positions and interests [redacted] CSEC supported Canada's international agenda and initiatives such as Cabinet Confidence

Cabinet Confidence

[redacted]

Cabinet Confidence

CSEC provides intelligence on activities linked to the [redacted] as well as on related Cabine

Cabinet Confidenc SIGINT produces actionable intelligence to assist Canadian authorities in [redacted] as well as actionable intelligence [redacted] CSEC provides valuable intelligence to CSIS, DND, Health Canada, DFATD, and others. Of principal concern this past year were Cabinet Confidence

Cabinet Confidence

In 2012–2013, SIGINT collection in support of the [redacted] intelligence priority focused on [redacted] IRRELEVANT

IRRELEVANT

Over the past year, CSEC collection also focused on [redacted] This information is vital for Canada to improve its understanding of these complex networks and to strengthen its counter measures.

Lastly, CSEC continued to report on: the acquisition and use of [redacted]

[redacted]

[redacted]

Cabinet Confidence

Cabinet Confidence threaten public safety and the integrity of Canada's economy and public institutions. In 2012--2013, Cabinet Confidence became a new stand-alone Government of Canada intelligence priority. Often focused on [redacted]

[redacted]

SIGINT collection in support of this priority focused on [redacted]

[redacted]

Cabinet Confidence

CSEC works closely with [redacted] to identify and monitor threats from foreign intelligence agencies. As part of its support to [redacted], CSEC reporting often results in identifying threats to Canadian interests [redacted]

In 2012--2013, SIGINT collection focused on identifying [redacted]

[redacted]

[redacted]

Cabinet Confidenc

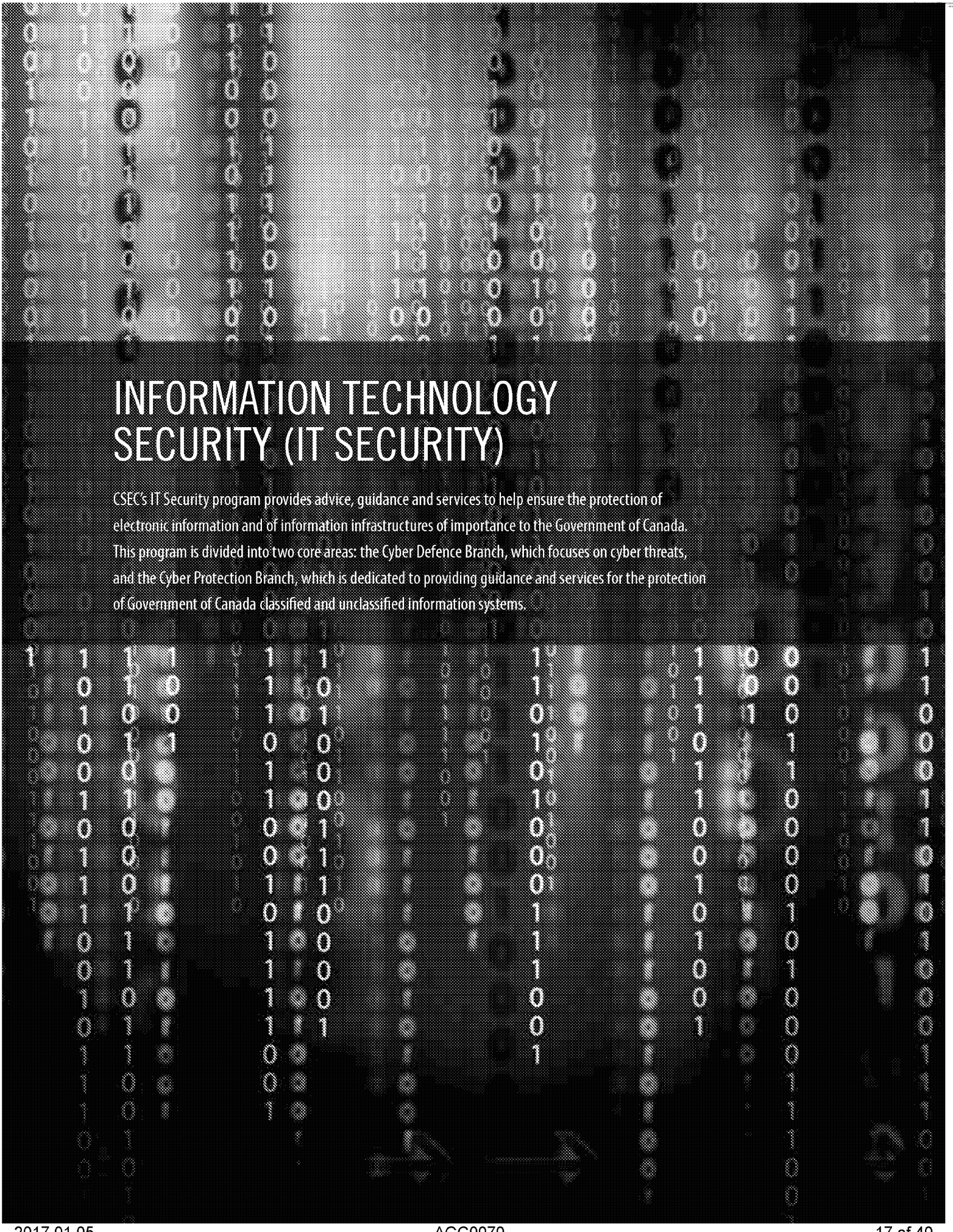
CSEC provides actionable intelligence on [redacted] including CBSA, DND, CSIS and RCMP, along with [redacted] CSEC reporting focuses on protecting Canada [redacted]

CSEC reporting this past year assisted in the protection of Canadian [redacted]

As part of Canada's operational strategy to combat Cabinet Cabinet C CSEC was active in identifying and intercepting the communications of various groups and individuals involved in [redacted] initiatives. SIGINT reports were successful in supporting [redacted]

[redacted]

IRRELEVANT



INFORMATION TECHNOLOGY SECURITY (IT SECURITY)

CSEC's IT Security program provides advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada. This program is divided into two core areas: the Cyber Defence Branch, which focuses on cyber threats, and the Cyber Protection Branch, which is dedicated to providing guidance and services for the protection of Government of Canada classified and unclassified information systems.

CYBER DEFENCE

In 2012–2013, CSEC's Cyber Defence Branch continued to develop products and services to detect, analyse, mitigate, and defend against threats to systems of importance to the Government of Canada. Its continued efforts to develop new techniques and tools to detect both known and previously unknown compromises and refine existing tools have led to increased automation of threat detection and mitigation action.

The use of commercial technologies provides state actors with intelligence collection capabilities while obscuring the identity of the originating agency. For example, CSEC recently identified an [redacted]

In collaboration with Shared Services Canada (SSC), CSEC continues to monitor Government of Canada networks for cyber intrusions through sensors on the Secure Channel Net. Over the past year, this monitoring has provided CSEC with approximately [redacted] which was analyzed to better understand the ways in which cyber threat actors are evolving their techniques in response to the Government's defensive measures.

Cyber Threat Evaluation Centre

CTEC was created in 2009 to promote greater synchronization between IT Security and SIGINT as well as to act as the entry point into CSEC for the Government of Canada. Since its creation, CTEC has taken on the function of Government of Canada Cyber Threat Evaluation Centre, whereby all cyber threat incidents identified in Government of Canada departments are now reported to CTEC. The cyber threat detection and cyber situational awareness developed and produced in CTEC is shared with Public Safety Canada's Canadian Cyber Incident Response Centre (CCIRC) to create a better national understanding of the cyber threat and to facilitate a more coordinated and effective response. CCIRC is responsible for coordinating a national response to any cyber security incident, with a focus on national critical infrastructure sectors. In order to enhance timely information sharing, a CCIRC official was integrated into CTEC in September 2012 and given full access to relevant CSEC classified information holdings.

In 2012–2013, CSEC efforts improved Government of Canada detection of and mitigation against state-sponsored threats and resulted in a decrease in the number of system compromises [redacted] compromises in 2012, compared to [redacted] in 2011).

Also over the past year, CTEC continued to develop a community of interest across government departments' IT functions to help better understand and defend against the cyber threat. The creation of SSC provided another partnership opportunity for CTEC to expand the reach of products, services and capabilities. CSEC will continue to develop its relationship with SSC over the next year as SSC's operations take shape.

[redacted]

CYBER PROTECTION

IRRELEVANT

[redacted]

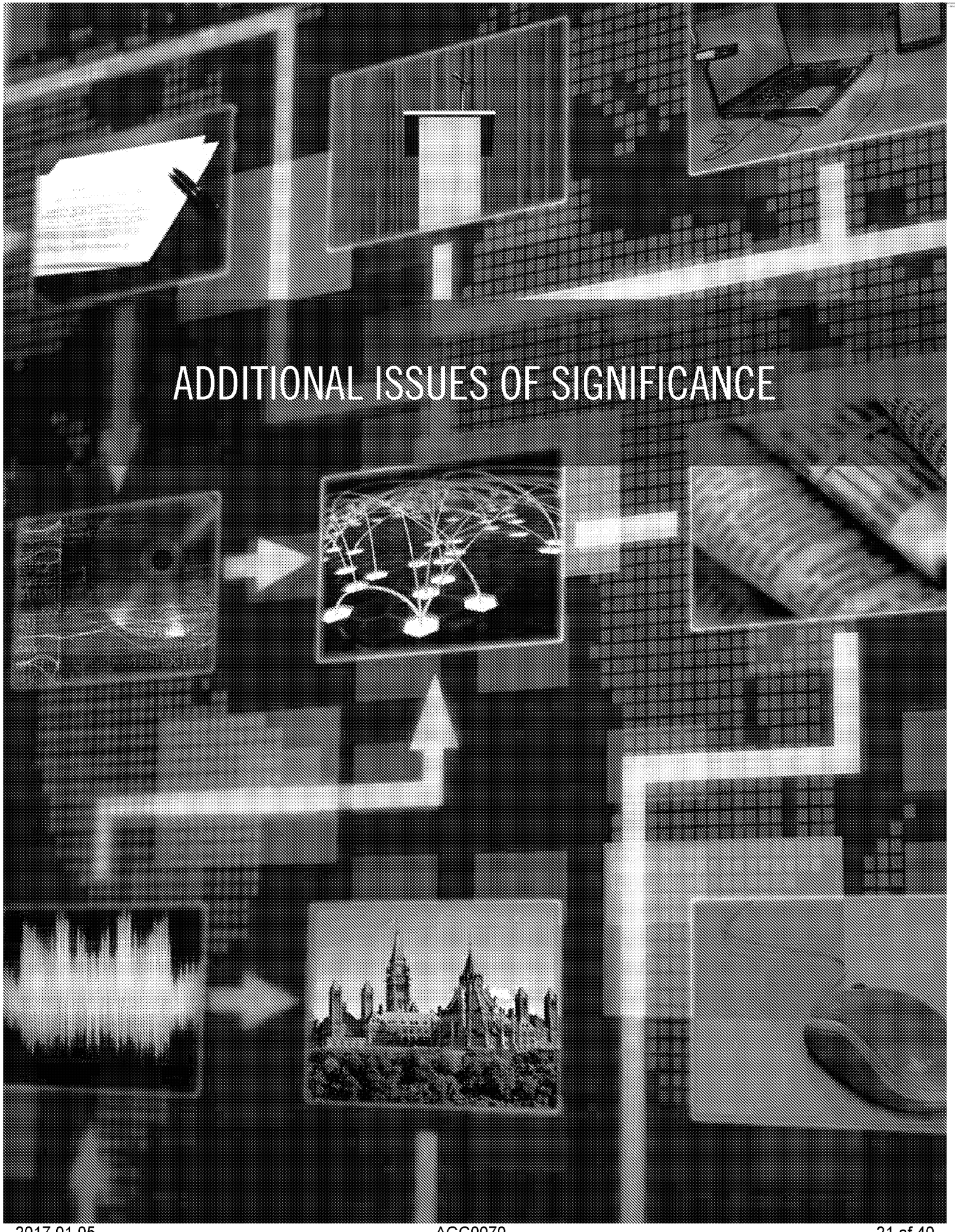
IRRELEVANT

IRRELEVANT

[redacted]

[redacted]

IRRELEVANT


ADDITIONAL ISSUES OF SIGNIFICANCE

SIGINT AND IT SECURITY COLLABORATION

In order to strengthen efforts on the cyber front, SIGINT and IT Security work closely [redacted]

[redacted]

EXTERNAL REVIEW FOR LAWFULNESS

The CSE Commissioner provides independent review of CSEC'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 CSEC activities. As with other federal agencies, CSEC 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, CSEC provided information to the CSE Commissioner to support nine reviews and one study. Six were completed during the 2012–2013 timeframe. CSEC also provided the Commissioner with additional records related to Solicitor-Client Privil

Solicitor-Client Privilege

Since the Office of the CSE Commissioner was established to review CSEC's activities, in every case where the Commissioner has been able to reach a definitive conclusion, CSEC has been found to be lawful.

AUTHORITIES

CSEC's operations are made possible by Ministerial Directives and Ministerial Authorizations. Under the *National Defence Act*, the Minister of National Defence issues written Ministerial Directives, which instruct CSEC with regard to its duties and functions. Additionally, CSEC annually requests approval from the Minister for several Ministerial Authorizations to authorize certain activities that are required for it to fulfill its mandate that would risk interception of private communications.

In light of CSEC's stand-alone status, the Ministerial Directives were updated in 2012–2013 to reflect the new streamlined reporting relationship between CSEC and the Minister of National Defence.

Cabinet Confidence

INTERNATIONAL INFORMATION SHARING

In 2011, CSEC was issued a Ministerial Directive on the *Framework for Addressing Risks in Sharing Information with Foreign Entities*. This Ministerial Directive aimed to balance CSEC'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.

As guided by Ministerial Directive, CSEC implemented a process for sharing information either directly or indirectly with foreign entities [redacted] using caveats that appropriately reflect the nature of its activities and the information it produces as a foreign signals intelligence agency. The process enables CSEC 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).

CSEC developed and implemented a process to operationalize the Ministerial Directive, and utilized the process in approximately [redacted] instances in 2012–2013.

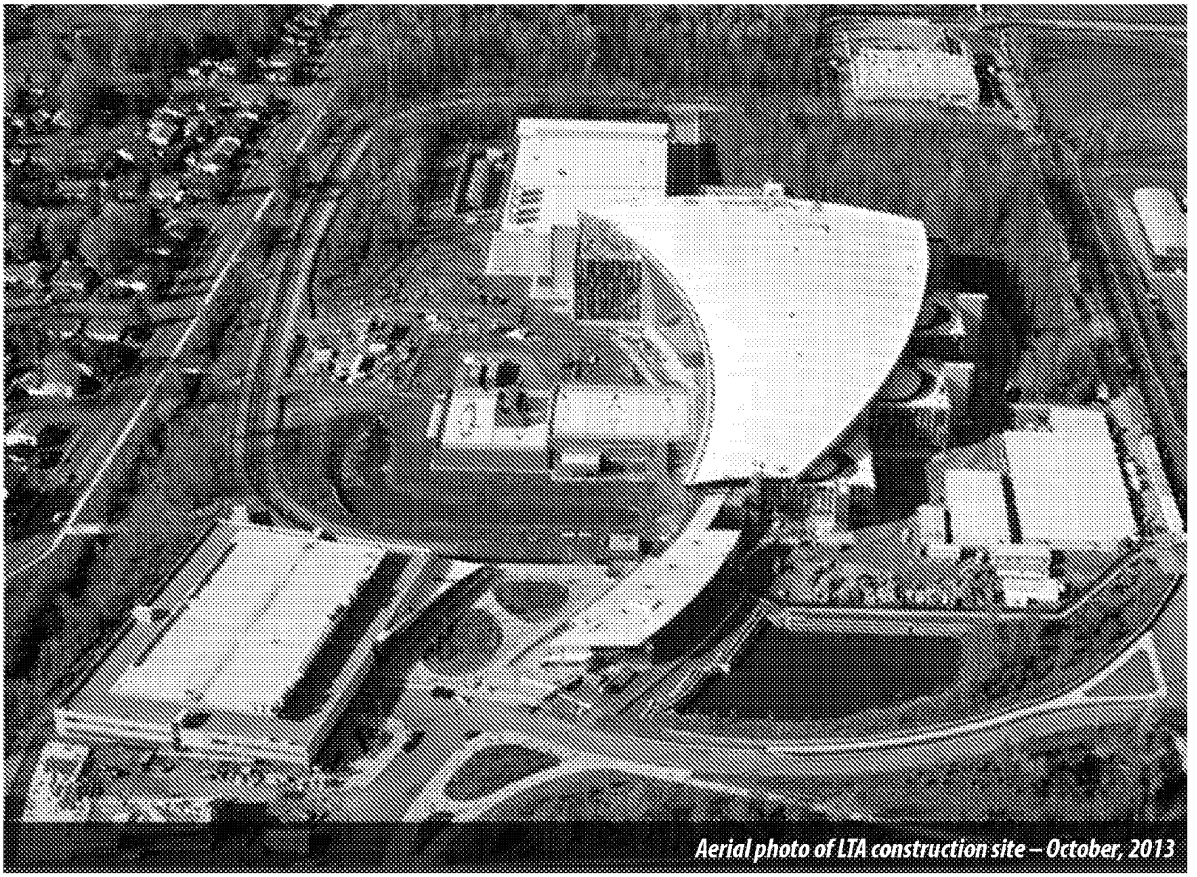
Similarly, the SIGINT program used this process to implement the Ministerial Directive in cases where CSEC shared information directly with [redacted] foreign entities. Over this past year, SIGINT continued to apply caveats and wording to restrict dissemination of reports shared directly with [redacted]

Over the past year, CSEC undertook a significant effort to harmonize application of its Ministerial Authorizations to ensure that they are applied against classes of activities, as specified in the existing legislation. The Ministerial Authorization Request Memos for 2012–2013 better described how mandated activities risk interception of private communications and how CSEC mitigates this risk. This harmonization effort also resulted in the reduction of the number of SIGINT Ministerial Authorizations from six to three.

IRRELEVANT

Cabinet Confidence

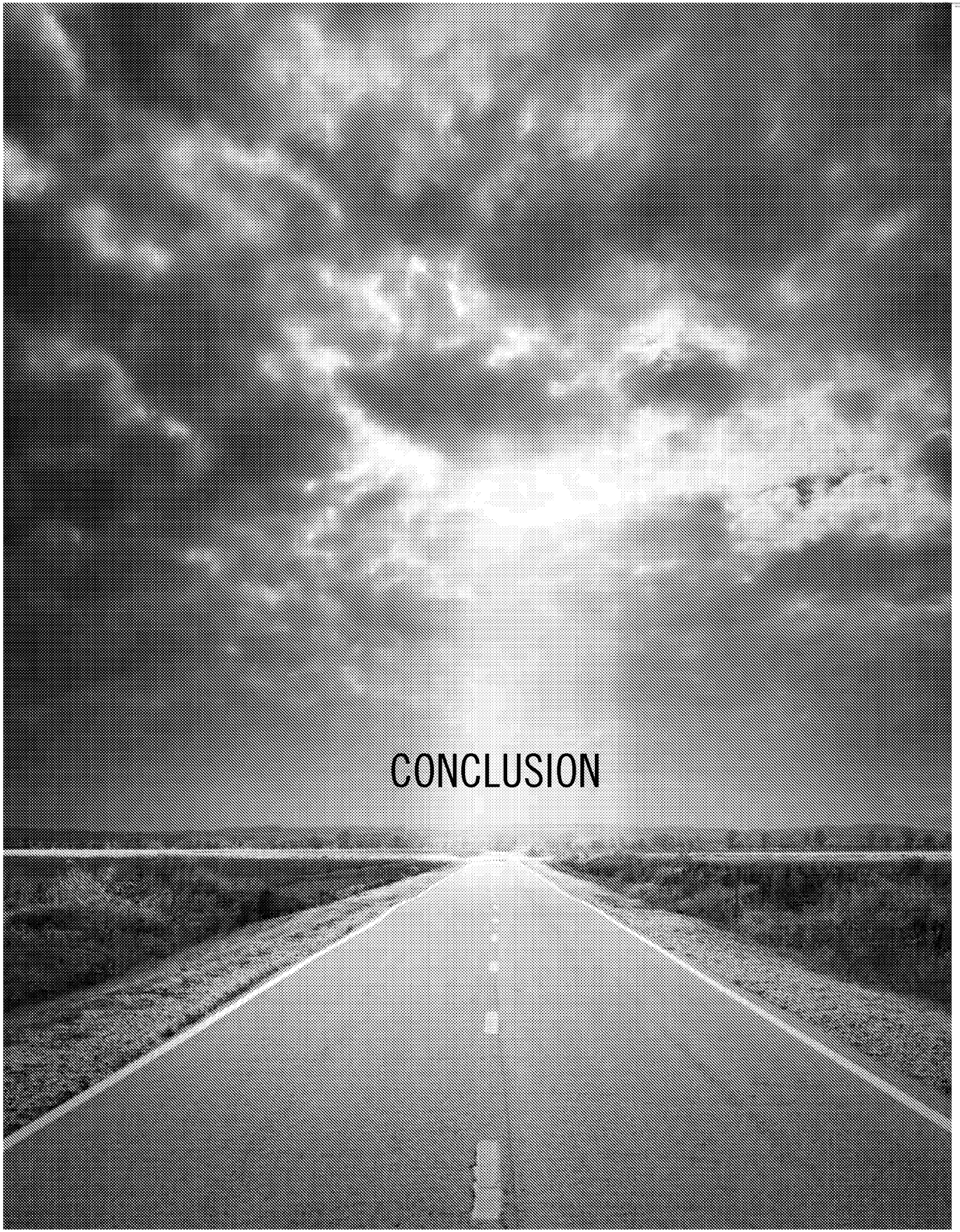
IRRELEVANT



Aerial photo of LTA construction site – October, 2013

IRRELEVANT

IRRELEVANT


CONCLUSION

CSEC highlights from 2012--2013 include:

- Valuable SIGINT contributions to a range of efforts, including: [redacted] and the protection of Canadian strategic interests [redacted]
- [redacted]
- Continued collaboration with domestic and international partners in response to the evolving threat environment, including contribution to [redacted]
- Cabinet Confidence
- IRRELEVANT

IRRELEVANT the Government of Canada's commitment to priorities such as Cabinet Confidence

CSEC will continue to support Government of Canada 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 CSEC 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 (June 2001)
- Privacy of Canadians (June 2001)
- 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 CSEC also has six Exceptionally Controlled Information Ministerial Directives dealing with highly-sensitive SIGINT initiatives.

ANNEX B: SPECIAL REPORTS (NON-ECI ONLY)

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

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: 2004 [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 a recommendation from the Office of the CSE Commissioner

---

Special Report: IRRELEVANT
Obligation:

SPECIAL REPORT: INTEGRATED SIGINT OPERATIONAL MODEL

The Integrated SIGINT Operational Model (ISOM) governance structure has evolved over the past year. A revitalized ISOM Steering Committee has provided positive change initiatives that advance the ISOM Ministerial Directive goals. The Integration Action Plan recommendations resulting from the ISOM five-year review and the emergence of a CAF [redacted] policy were the driving components for modernizing the ISOM governance model. The Steering Committee's primary goal remains to refine business practices and provide an effective and comprehensive accountability framework for Canadian SIGINT. Over the past year, the Deputy Minister for National Defence, the Chief of Defence Staff, and the Chief of CSEC were given an ISOM Ministerial Directive update and provided options for how to capitalize on the CAF/CSEC ISOM collaboration experience and to consider expanding the scope of cooperative efforts to include [redacted]

The integration of CSEC employees at the CAF Information Operations Group (CFIOG) Headquarters and Canadian Armed Forces Station Leitrim continued in 2012--2013 to align CAF SIGINT activities more closely with the national SIGINT authority and enhance accountability through oversight and review.

Within the Electronic Intelligence (ELINT) domain IRRELEVAN

IRRELEVANT

CAF deployed to Afghanistan continue to face a number of threats from Taliban insurgents in the region around Kabul [redacted]

Canadian SIGINT remains an important element for enhancing [redacted] Canada's contribution to the [redacted] Mission -- Afghanistan. [redacted] Support to CAF operations as well as CAF integration into the Canadian Cryptologic Enterprise remain the driving forces behind ISOM.

SPECIAL REPORT: [redacted]

[redacted]

[redacted]

The [redacted] program continues, [redacted] to be a highly valued source of foreign intelligence to the Government of Canada and its allies. This year, CSEC issued [redacted] reports based on information derived from the program [redacted]

During 2012–2013, CSEC's Five Eyes partners produced [redacted] reports derived from this [redacted] program. Allied reports from this source were viewed by CSEC clients in at least [redacted] government departments and agencies, providing intelligence that predominately related to the Government of Canada's Cabinet Cont Cabinet Confidence intelligence priorities.

SPECIAL REPORT: [redacted]

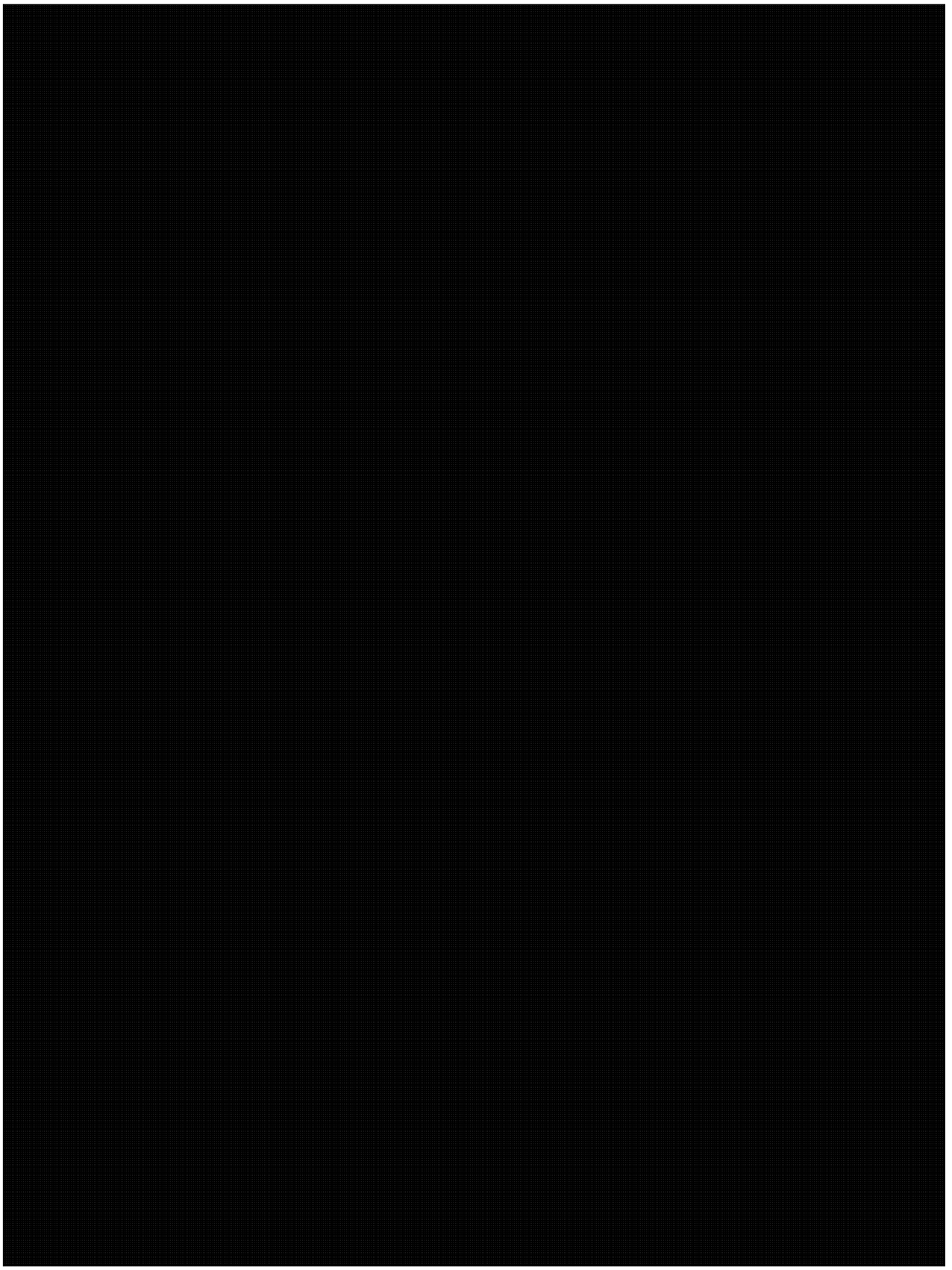
SPECIAL REPORT: [redacted]

[redacted]

[redacted]

SPECIAL REPORT: [redacted]

[redacted]



[redacted]

IRRELEVANT

IRRELEVANT

SPECIAL REPORT: PRIVACY OF CANADIANS

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

In 2012--2013, CSEC continued to strengthen the policy framework relating to privacy issues. CSEC secured approval and promulgation of several new or amended policy instruments that reinforce CSEC's ability to consistently apply, and demonstrate compliance with, the operational policy framework. These include:

- OPS-1, *Protecting the Privacy of Canadians and Ensuring Legal Compliance in the Conduct of CSEC Activities*
- OPS-1--8, *Operational Procedures for Policy Compliance Monitoring to Ensure Legal Compliance and the Protection of the Privacy of Canadians*
- OPS-1--13, *Operational Procedures Related to Canadian* [redacted] *Activities*
- OPS-1--14, *Operational Procedures for cyber Defence Operations Conducted Under Ministerial Authorization*
- OPS-3--1, *Operational Procedures for* [redacted] *Activities*
- IRRELEVANT

In 2012--2013, CSEC released [redacted] pieces of Canadian identity information to Government of Canada departments stemming from [redacted] Canadian and allied foreign intelligence reports. As in years past, the majority of identify information was released to [redacted] Canadian identities, or [redacted]%). These numbers indicate the aggregate number of releases.

In addition, CSEC released [redacted] Canadian identities to its Five Eyes partners. This represents a significant increase in the number of identities released in 2011--2012 [redacted] and is attributable to a [redacted] released to the US allies to enable them to efficiently assess the

[redacted] CSEC also refused to release [redacted] Canadian identities to its Five Eyes partners. For the most [redacted]

[redacted]

IRRELEVANT