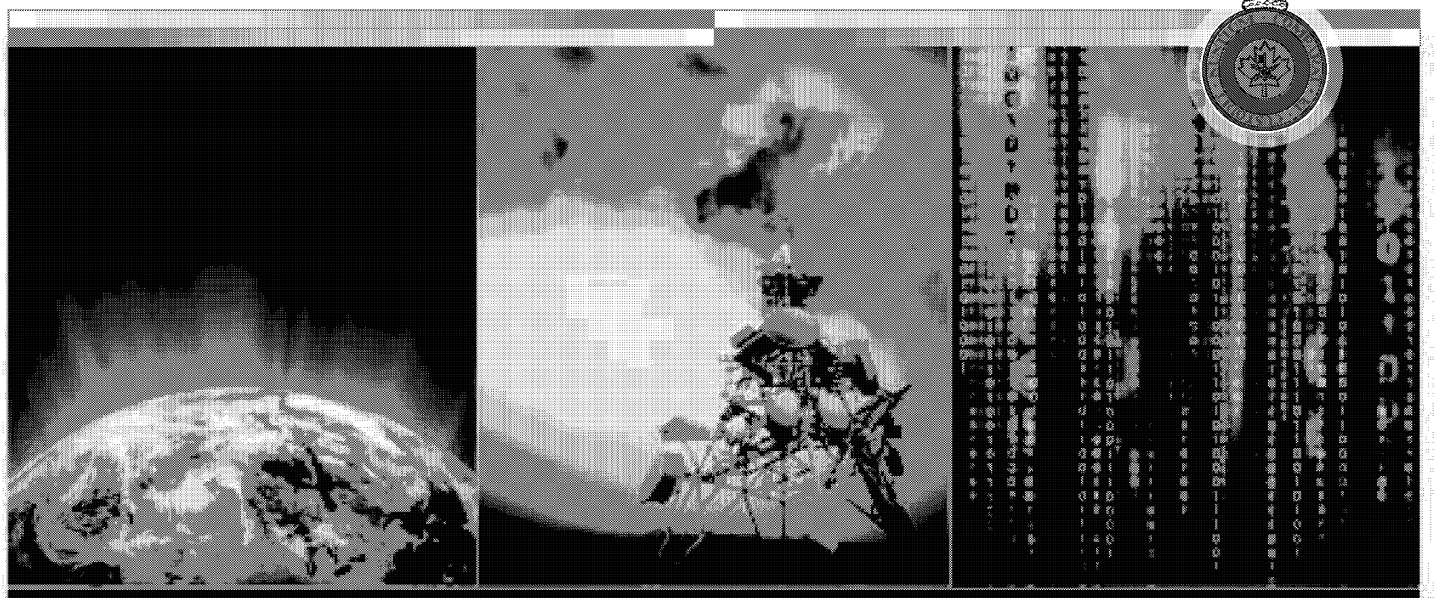
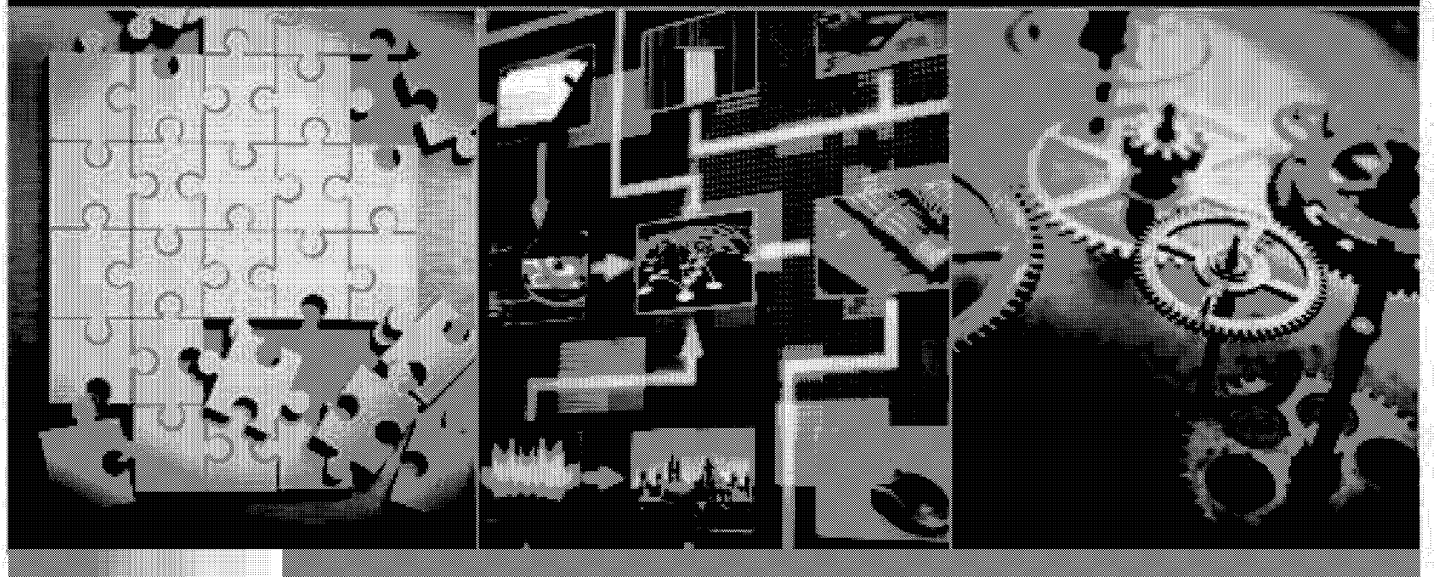
Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada



COMMUNICATIONS SECURITY ESTABLISHMENT CANADA

ANNUAL REPORT TO THE MINISTER OF NATIONAL DEFENCE

2011–2012



Canada

September 2012

Minister,

I am very pleased to submit to you the CSEC Annual Report for fiscal year 2011–2012. This was a significant year on a number of fronts. At the beginning of 2012, I took on the role of Chief, CSEC from my respected predecessor John Adams; additionally, CSEC was given a new place in government in 2011–2012 as a stand-alone department within the National Defence portfolio. The Orders-in-Council issued on November 16, 2011 established CSEC's new status and provided new delegations of authority to the organization. This was a historic milestone for CSEC, and we look forward to continuing to support the Government of Canada.

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 technological environment.

Over the past year, CSEC has continued to develop and implement new capabilities to support the Government of Canada's security and intelligence priorities and address cyber security threats. CSEC's role in Afghanistan [redacted] as Canada's combat operations ended in 2011 [redacted] The organization focused its activities to support the government's intelligence priorities to Cabinet Confidence Cabinet Confidence CSEC's unprecedented collaboration with partners, including Five Eyes, [redacted] helped expand information sharing and capabilities. CSEC's Tutte Institute for Mathematics and Computing, the only classified research institute of its kind in Canada, officially opened in September 2011, and we broke ground on CSEC's Long-term Accommodations project.

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:

- expanding CSEC's [redacted] operations to deliver timely and high-quality foreign intelligence to meet Government of Canada priorities;
- providing quick, flexible response capacity to meet the Government of Canada's intelligence needs in responding to emerging global incidents;
- implementing CSEC's responsibilities under the Government's *Cyber Security Strategy* and protecting Government of Canada's networks from threats;
- strengthening secure handling of TOP SECRET information through improvements to government systems;
- developing a legislative proposal for your consideration to confirm CSEC as a stand-alone agency, address previous concerns of successive CSE Commissioners and provide CSEC with the tools it needs to succeed in future;
- enhancing accountability and sound management systems to support CSEC as a stand-alone agency; and
- implementing the Deficit Reduction Action Plan as approved by the Government of Canada.

CSEC made important contributions to the government's security and intelligence priorities in 2011-2012. We look forward to continuing to help protect the security of Canada and Canadians in the year ahead.

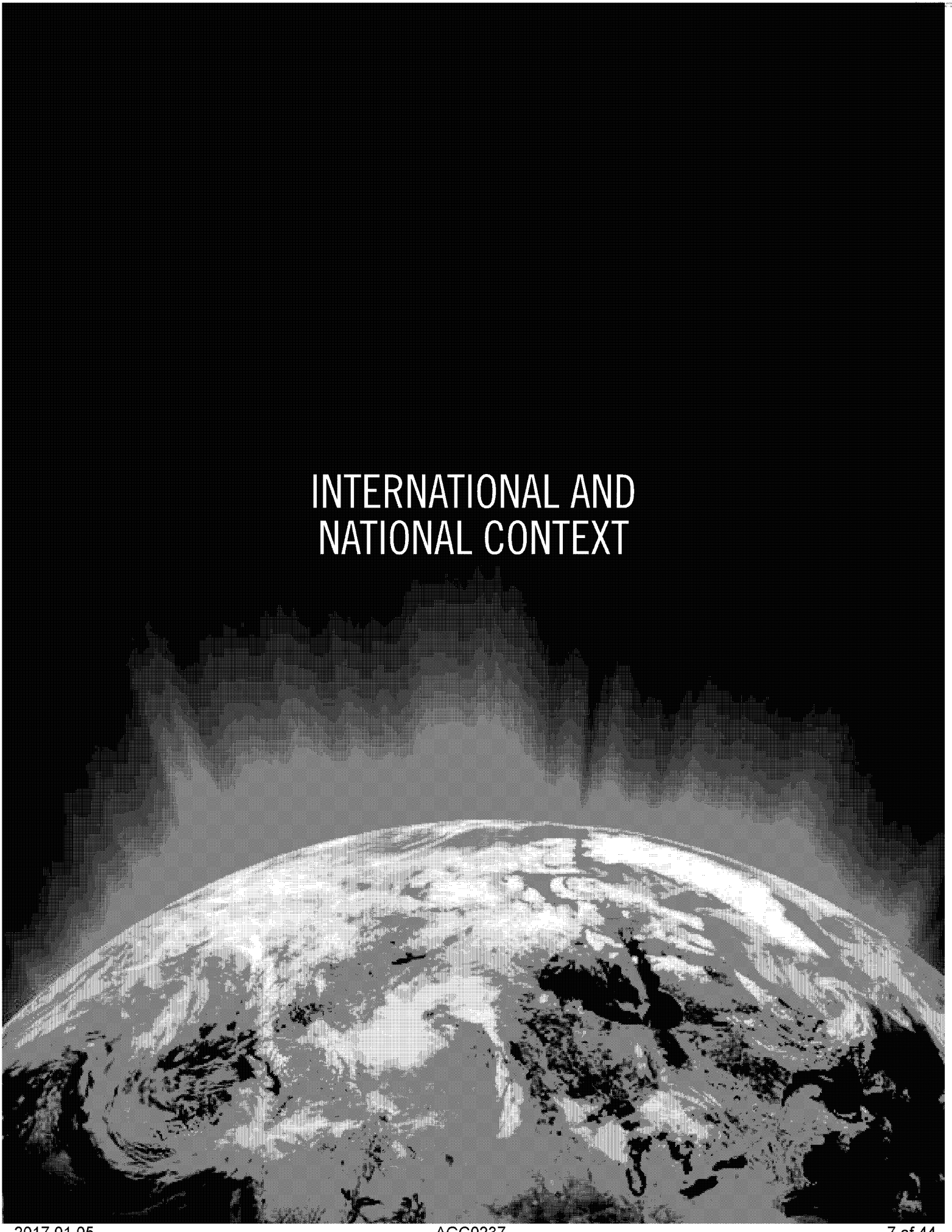
Sincerely,

John Forster
Chief

TABLE OF CONTENTS

LIST OF 2011–2012 HIGHLIGHTS

INTERNATIONAL AND NATIONAL CONTEXT



Significant events in 2011–2012 served to focus global and domestic attention on a number of key priorities. The capture and death of Osama bin Laden, the end of the Canadian combat mission in Afghanistan, the evolving global cyber threat, and [redacted] are a few examples of the security and intelligence (S&I) priorities that evolved this past year. To effectively operate in this dynamic environment, CSEC continued to work closely with its international partners, the Five Eyes. This cryptologic alliance consists of the US National Security Agency (NSA), the UK Government Communications Headquarters (GCHQ), the Australian Defence Signals Directorate (DSD) and the New Zealand Government Communications Security Bureau (GCSB).

[redacted]

CSEC supported and protected Canadian [redacted]

[redacted]

Foreign state-sponsored cyber intrusions took place on multiple GC departments this past year, raising concerns about cyber security. CSEC worked with many of the affected departments to enhance their networks' security to help prevent future incidents. These factors contributed to the GC's approval of increased cyber funding for numerous departments, including CSEC, which will be receiving [redacted] This represents a significant investment by the GC towards meeting the objective of 'Securing Government Systems' outlined in *Canada's Cyber Security Strategy* (CCSS).

The January 2012 arrest of a Canadian Naval officer on charges of spying linked to Russia drew considerable media attention to issues of foreign espionage. Relying on [redacted]

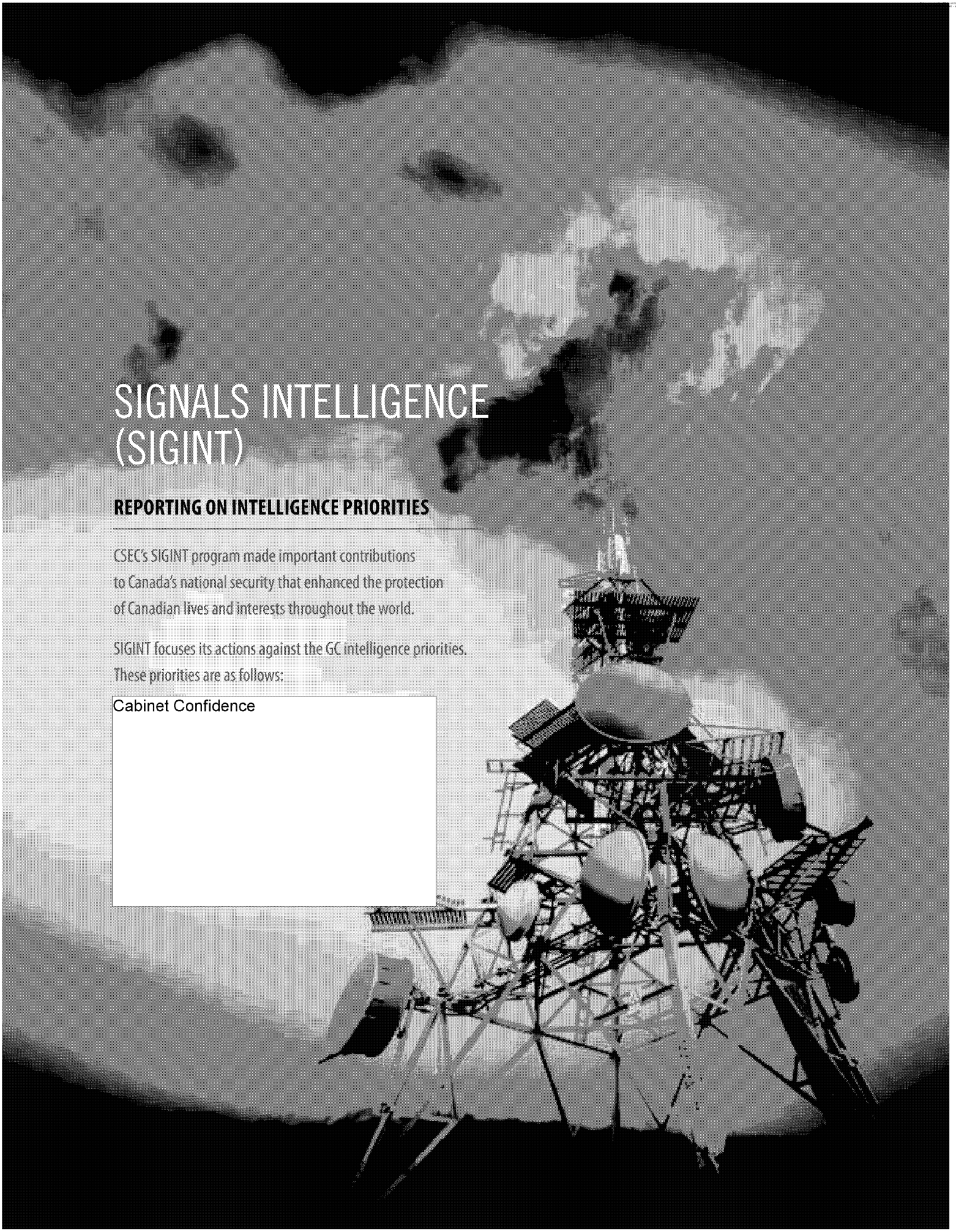
[redacted]

CSEC continued work this year to [redacted]

[redacted]

Lastly, CSEC's support role to the Canadian Forces and allies in Afghanistan evolved this past year as the Canadian combat mission drew to a close in July 2011. [redacted]

[redacted]



SIGNALS INTELLIGENCE (SIGINT)

REPORTING ON INTELLIGENCE PRIORITIES

CSEC's SIGINT program made important contributions to Canada's national security that enhanced the protection of Canadian lives and interests throughout the world.

SIGINT focuses its actions against the GC intelligence priorities. These priorities are as follows:

Cabinet Confidence

Cabinet Confidence

SIGINT provides actionable signals intelligence[1] for Cabinet

Cabinet Confidence

Cabinet Confidence Key clients include the RCMP, CSIS, DND, and DFAIT, [redacted]

In 2011–2012, SIGINT focused its intelligence collection on [redacted] in addition to various other groups or individuals that posed threats to Canadian or allied lives and interests.

[redacted]

Cabinet Confidence

Cabinet Confidence [redacted] CSEC collection activities are being realigned to reflect Cabinet Confidenc

Cabinet Confidence

In the near term [redacted]

[redacted]

Cabinet Confidence

1 Specific SIGINT reports graded "Actionable" intelligence have either

a) identified a threat to Canadian and/or allied interests, or
b) resulted in significant action being taken by the GC or
c) significantly influenced GC, CF or allied government decisions.

SIGINT processes roughly [redacted]

[redacted]

[redacted]

Cabinet Confidence

[redacted]

Reports in 2011–2012 provided valuable information to support

[redacted]

[redacted]

Cabinet Confidence

Cabinet Confidence [redacted] to GC clients including CSIS, DND, Health Canada, and DFAIT.

In 2011–2012, SIGINT continued to support this intelligence priority by focusing on the extent to which [redacted]

[redacted]

Cabinet Confidence

Cabinet Cor In 2011–2012, SIGINT collection in support of this [redacted]

Cabinet Confidence

Cabinet Confidence Its key clients are CBSA, DND, CSIS and RCMP, along with [redacted]

SIGINT continued this past year to successfully identify and intercept the communications of various groups and individuals [redacted] to facilitate the provision of SIGINT reporting to GC agencies in the area and increase success in countering these activities.

IRRELEVANT

SIGINT PARTNERSHIPS

IRRELEVANT

CSEC is committed to developing relationships within the Canadian S&I community, as demonstrated by its senior level engagement with DFAIT [redacted] (see 'Annex A: Special Reports'). Additionally, CSEC is currently in the midst of creating a framework MOU with [redacted] with a goal of moving forward with this partnership in 2012–2013.

Over the past year, collaboration with the Five Eyes partners has remained high on the list of CSEC's priorities. CSEC's alliance with NSA, GCHQ, DSD and GCSB continues to yield great [redacted] efficiency in achieving Canada's national security [redacted] interests. The demonstrated value to Canada's national security interests has prompted CSEC to develop IRRELEVANT

IRRELEVANT

In 2011–2012, CSEC worked closely with Five Eyes counterparts to better understand the [redacted]

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, as mandated by the *National Defence Act*. This program is divided into two branches: the Cyber Defence Branch, focused on cyber threats; and the Cyber Protection Branch, dedicated to providing guidance and services for the protection of GC information systems.

CYBER DEFENCE

The Cyber Defence Branch protects against sophisticated cyber threats. In 2011–2012, the Cyber Defence Branch continued its operations to detect, analyze, evaluate, mitigate, and defend against incidents that are occurring on GC networks. New techniques and tools to detect both known and previously unknown compromises were developed, deployed and, wherever possible, automated. CSEC monitors [redacted] departments for cyber intrusions - representing approximately [redacted] terabytes of data per day, which is the equivalent [redacted] pages of text.

Cyber Defence provides mitigation and preventative advice, as well as products and services based on a [redacted] schedule which considers the nature and severity of the cyber incident, the threat actor, and the GC sector affected. This is particularly important given the persistent and evolving nature of cyber threats to the GC.

Following the release of Canada's Cyber Security Strategy (CCSS) in October 2010, CSEC began receiving funding which was directed to develop cyber systems to provide CSEC's Cyber Threat Evaluation Centre (CTEC) and [redacted] areas with increased access to cyber threat data. These systems are currently functional and provide an enhanced perspective of the cyber threat affecting Government of Canada systems, and lay the foundation upon which an increased analyst complement will search out new threats and threat actors. Some of the systems automate analyst workflow to liberate resources to detect and defend against new threats.

NEW ROLE FOR THE CYBER THREAT EVALUATION CENTRE (CTEC)

CTEC was created in 2009 to promote greater synchronization between IT Security and SIGINT, a partnership that is vital to effectively curb cyber threats, as well as to act as the entry point into CSEC for the GC. Adding to this role, CTEC took on the function of Government of Canada Cyber Threat Evaluation Center (GC CTEC) in June 2011 under a Memorandum of Understanding with Public Safety Canada (PS). All cyber threat incidents identified at GC departments are now reported to GC CTEC. The picture this collated information creates forms the basis of increased cyber situational awareness and threat detection.

Improved Reporting Products

In 2011–2012, CTEC expanded its catalogue of products and services that convey important cyber threat information to stakeholders at various levels. The catalogue includes core monthly and yearly summary reports at the SECRET level that inform Chief Information Officers, Departmental Security Officers and IT security personnel of baseline threat knowledge; individual departmental reports which detail incidents that may have occurred on their network; and an interdepartmental assessment of the cyber threat to GC systems by the [redacted] actor.

[redacted]

CYBER PROTECTION

IRRELEVANT

IRRELEVANT

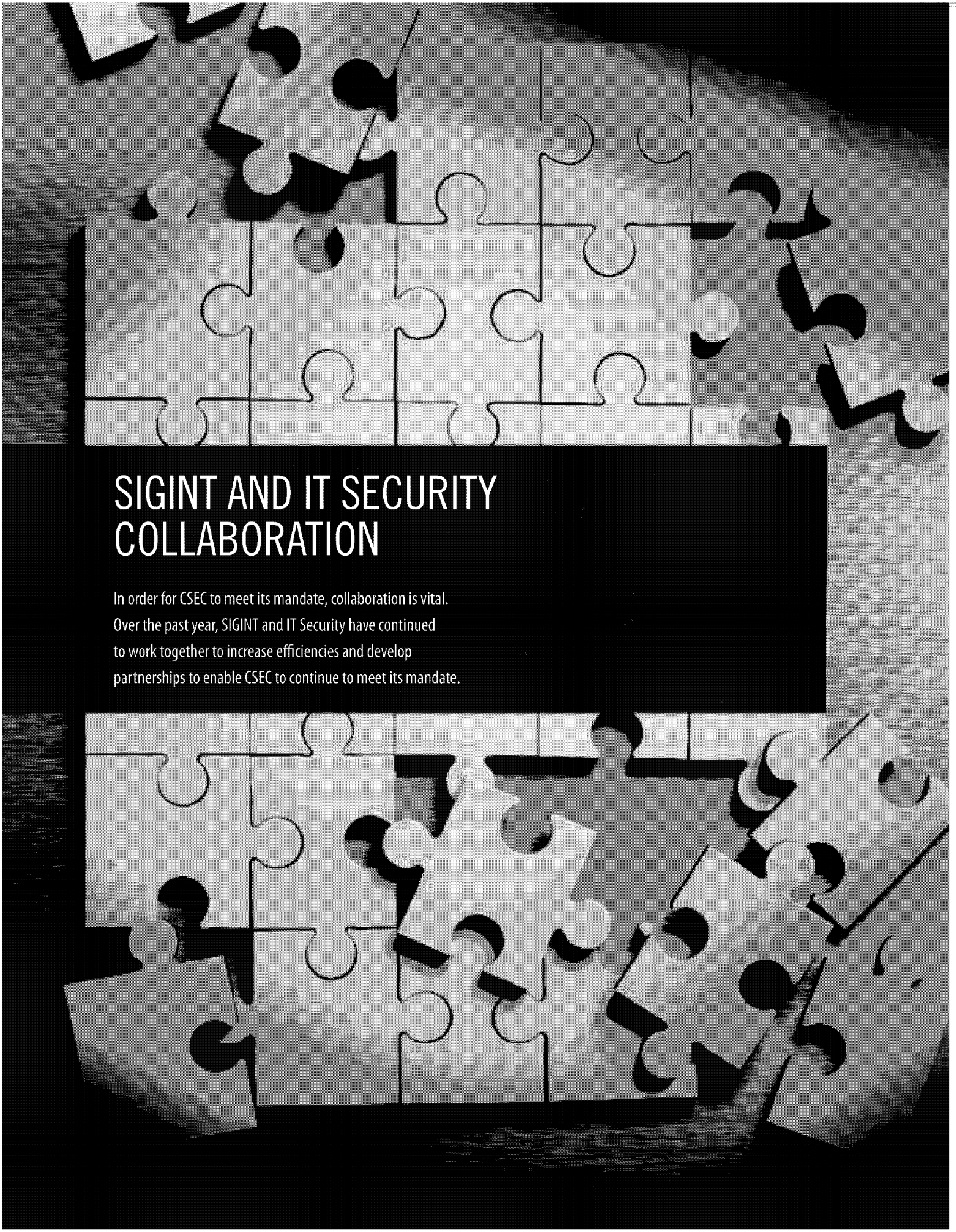
IRRELEVANT

IRRELEVANT

IT SECURITY PARTNERSHIPS

In the past year, CSEC continued to develop their partnership with

IRRELEVANT



SIGINT AND IT SECURITY COLLABORATION

In order for CSEC to meet its mandate, collaboration is vital. Over the past year, SIGINT and IT Security have continued to work together to increase efficiencies and develop partnerships to enable CSEC to continue to meet its mandate.

JOINT RESEARCH OFFICE (JRO)

CSEC established the JRO to ensure CSEC's research and experimental development program addresses science and technology issues critical to meeting its operational mandates.

The key activities of the JRO are to:

- ensure clear research requirements are addressed;
- leverage research representation and relationships;
- enhance predictive analysis to anticipate the hard problems of the future;
- establish a responsive research and technology transfer process; and
- foster out-of-program research work to accelerate innovation in the work place.

These activities permit CSEC to enhance and expand collaboration on science and technology issues with the Government of Canada and its partners in the allied community [redacted] academia and other research organisations.

In 2011–2012 the JRO developed the CSEC 2015 [redacted] development over the next three years. The office also established a [redacted] at an unclassified facility to leverage external research capacity and leading-edge technology to address certain mission critical challenges. As well, the office conducted an in-depth review of cyber defence-related research challenges to advance capabilities that can meet these challenges.

TUTTE INSTITUTE FOR MATHEMATICS AND COMPUTING (TIMC) OFFICIALLY OPENS

The TIMC, formerly the Cryptologic Research Institute (CRI), officially opened in September 2011. The only one of its kind in Canada, this classified mathematical and computational research facility works alongside and receives longer-term research priorities from the JRO.

One of the most striking features of the institute is its Advanced Collaborative Environment (ACE). The ACE is one of the world's most sophisticated collaborative spaces, providing researchers with the ability to conduct advanced computer interactions at the highest classification level (TOP SECRET//SI// ECI). These capabilities enable researchers across the allied cryptologic community to collaborate on the hardest mathematical and computing problem sets.

In 2011–2012, the TIMC engaged some of Canada's top academics and leveraged Canada's research partnerships within the allied cryptologic research community. The institute hosted two successful workshops, with attendees from international partner institutes. Through this collaboration, TIMC will continue to explore highly secure but publicly available cryptography and to overcome existing computing challenges.

CYBER DEFENCE

Analytic Collaboration on the Cyber Defence Mission

In 2011–2012, IT Security and SIGINT continued to integrate activities to respond to [redacted] cyber threats to the GC.

[redacted]

[redacted]

The "Big Dig"

[redacted]

Cyber Security Funding

In April 2012, the GC approved $153M over four years with an additional $42M ongoing of new funding for CSEC, TBS, SSC and PS to improve the security of federal cyber systems. These new resources will reinforce ongoing cyber defence efforts in SIGINT and IT Security and enhance CSEC's support capabilities to domestic partner departments and agencies. This funding supports Pillar 1 of Canada's Cyber Security Strategy: 'Securing Government Systems'. CSEC is receiving the largest share of this new funding: [redacted] including approximately [redacted] additional employees.

OTHER COLLABORATION

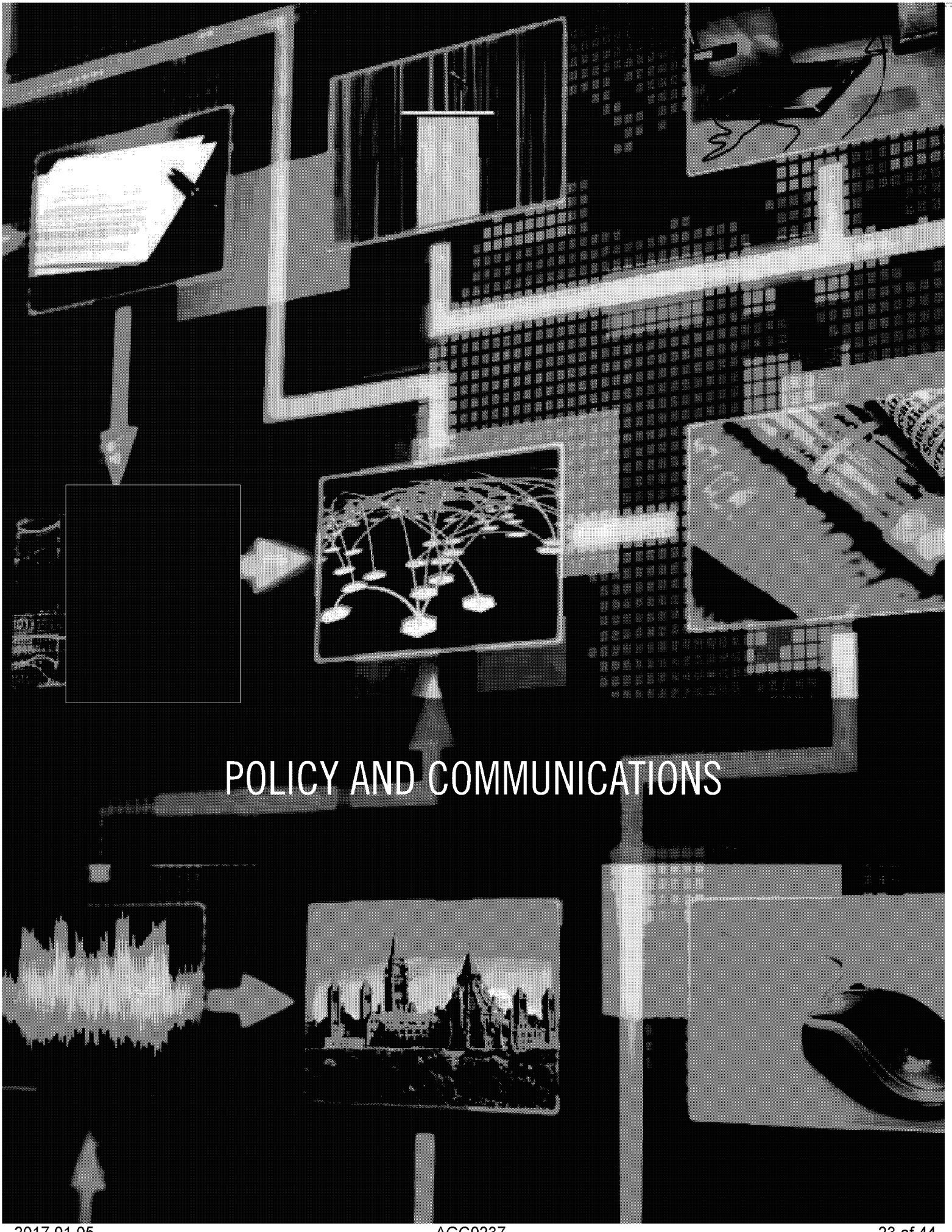
Joint Career Frameworks

IRRELEVANT

SIGNALS INTELLIGENCE AND IT SECURITY CHALLENGES

[redacted]

IRRELEVANT



REVIEW FOR LAWFULNESS

The Office of the CSE Commissioner (OCSEC) is an independent review body whose role it is to verify the lawfulness of CSEC's operational activities through classified reviews and to investigate and respond to external complaints about CSEC, if required. 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 OCSEC to support ten reviews, six of which were completed during the 2011–2012 timeframe. OCSEC also requested that CSEC provide additional records related to the current civil litigation by Messrs. Almalki, El-Maati, and Nureddin that may not have been examined during the Commissioner's previous review.

Intelligence as Evidence

IRRELEVANT

IRRELEVANT

In response to past recommendations of the CSE Commissioner to address Ministerial Directives (MDs) that pre-date the legislative establishment of CSEC in the National Defence Act, CSEC updated

IRRELEVANT

and 'Collection and Use of Metadata' Ministerial Directives. A new additional Ministerial Directive was issued to implement the Cabinet-approved Framework for Addressing Risks in Sharing Information with Foreign Entities, which outlines the decision-making process to be used in instances where the sharing of information may present a substantial risk of mistreatment.

Following implementation of a new synchronized process to harmonize the expiry of Ministerial Authorizations (MAs), work has continued to improve coordination of the CSEC Ministerial Authorization regime. Attention has shifted this year to harmonizing a number of MAs.

IRRELEVANT

On a related note, during the past year, CSEC received a greater number of Access to Information requests. When compared to the previous fiscal year, consultations requests increased by 62% and Access to Information requests by 28%.

IRRELEVANT

LIST OF CURRENT CSEC MINISTERIAL AUTHORIZATIONS AND DIRECTIVES

Ministerial Authorizations (MAs)[2]

Signals Intelligence MAs

- MA [redacted] (since January 2002)
- MA [redacted] (since January 2002)
- MA [redacted] (since March 2004)
- MA [redacted] (since December 2004)
- MA Support to Canadian Forces Operations in Afghanistan (since December 2006)
- MA Interception Activities [redacted] (July 2011)

Information Technology Security MAs

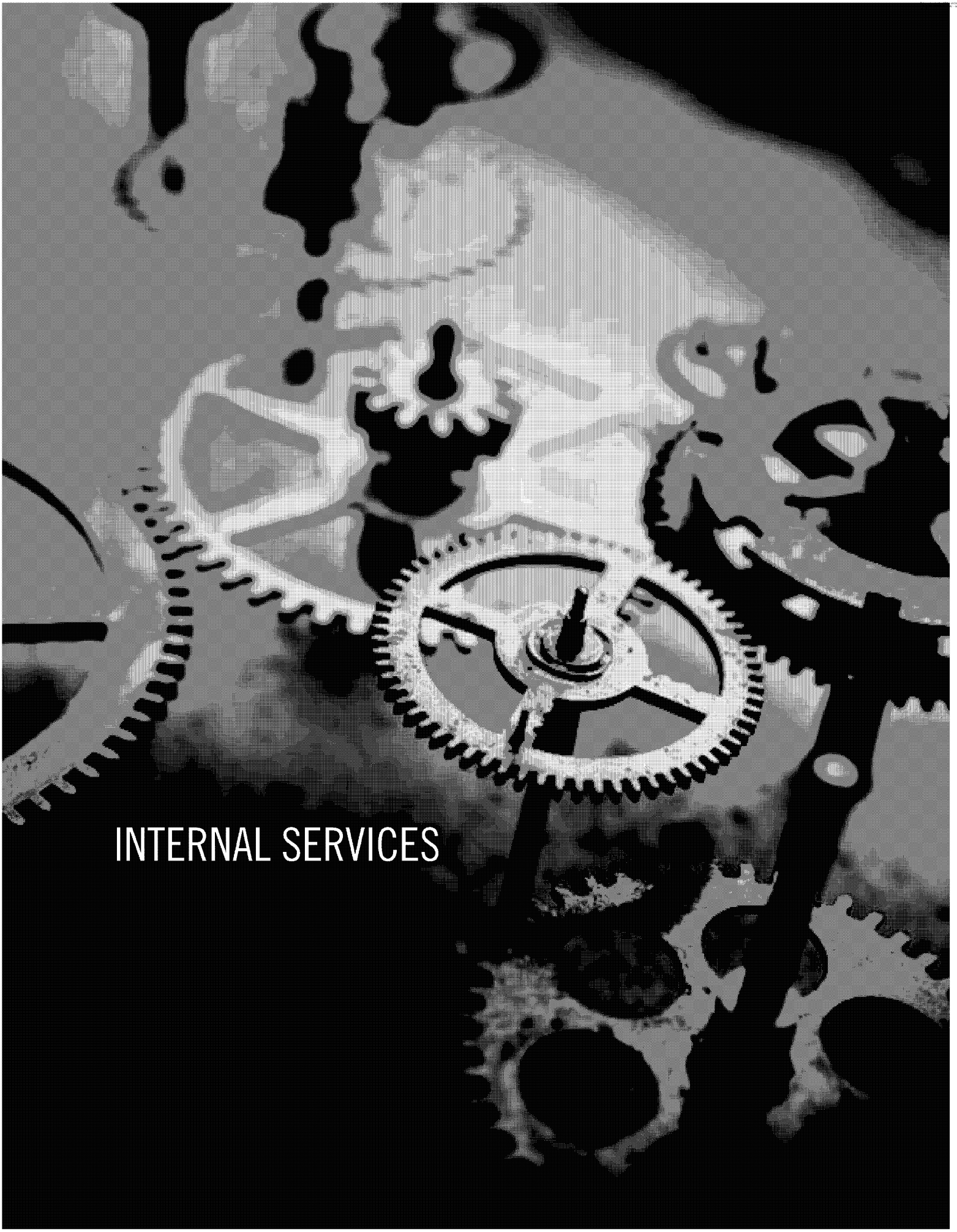
- MA Protection of Government of Canada Computer Systems and Networks - Active Network Security Testing (since April 2002)
- MA Protection of Government of Canada Computer Systems and Networks - Cyber Defence Operations (since January 2004)

Ministerial Directives (MDs)[3]

- MD Accountability Framework (June 2001)
- MD Privacy of Canadians (June 2001)
- MD IRRELEVANT IRRELE (November 2011)
- MD [redacted] Operations (January 2002)
- MD [redacted] Program (March 2004)
- MD Integrated Signals Intelligence (SIGINT) Operational Model (May 2004)
- MD Collection and Use of Metadata (November 2011)
- MD IRRELEVAN (June 2005)
- MD [redacted] (August 2006)
- IRRELEVANT IRRELEVANT (October 2009)
- MD Intelligence Priorities (updated annually)
- MD Risks in Foreign Information Sharing (November 2011)

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

3 CSEC also has six ECI MDs dealing with highly sensitive SIGINT initiatives.


INTERNAL SERVICES

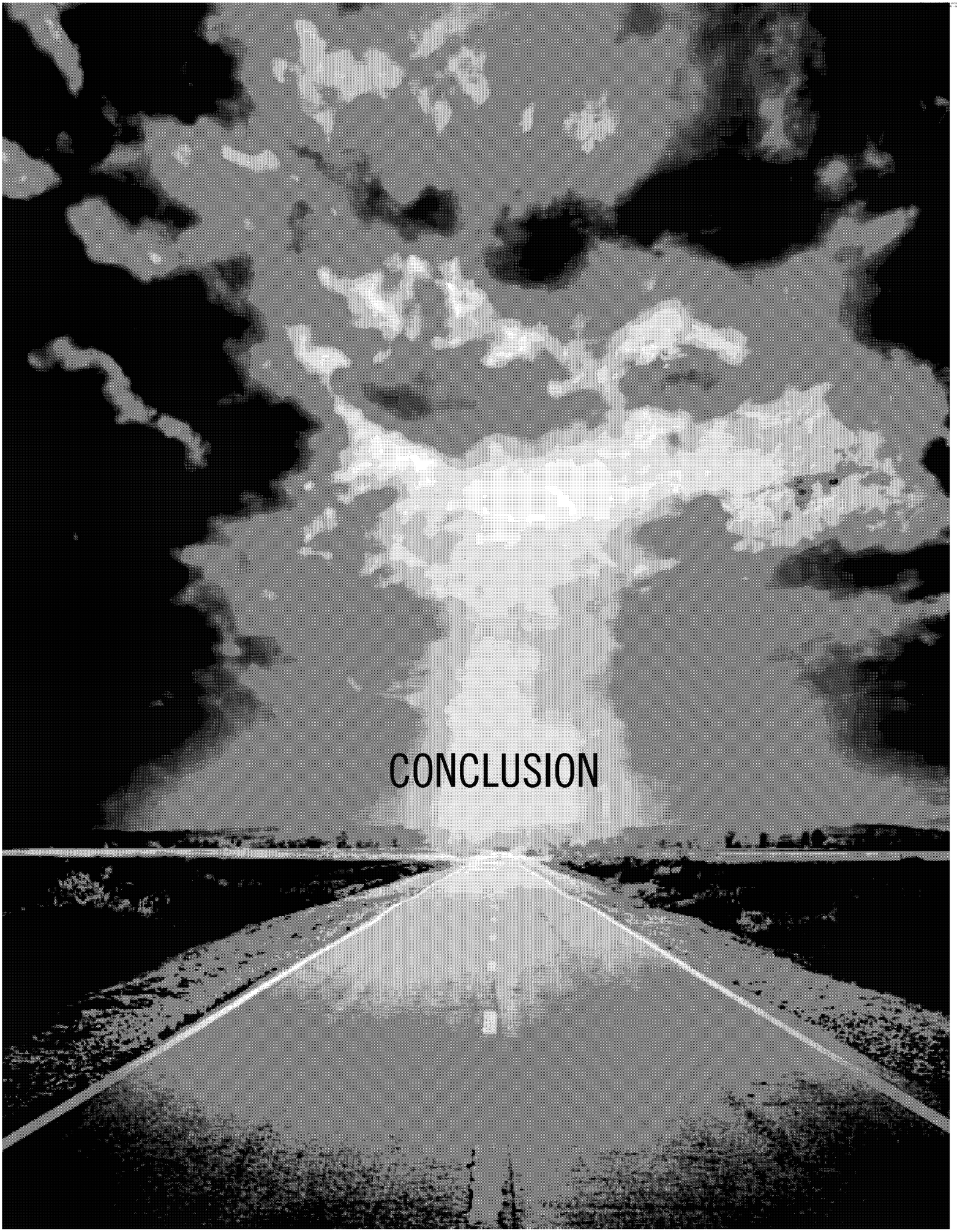
IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT


CONCLUSION

CSEC highlights from 2011–2012 include:

- Valuable SIGINT contributing to efforts ranging from [redacted]
- The development of tools and strategies to prevent and detect intrusions by cyber threat actors and assuming a new role as GC-CTEC;
- The official opening of the TIMC classified research institute;
- The establishment of CSEC as a stand-alone department within the National Defence portfolio; and
- Continued collaboration with domestic and international partners in response to the evolving threat environment.

IRRELEVANT

Looking forward to 2012–2013, CSEC will continue managing the [redacted] In view of the Canadian naval officer espionage case, CSEC is actively taking measures to raise confidence in its capabilities to safeguard sensitive information and demonstrate to the international community the GC support for priorities such as Cabinet Co

CSEC will continue to address a range of targets in support of stated GC Intelligence Priorities, particularly the priorities of Cabinet Co Cabinet Confidence CSEC 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: 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 ISOM 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 [redacted]

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

Special Report IRRELEV
Obligation

Special Report Privacy of Canadians
Obligation Voluntary- Response to OCSEC recommendation

Special Report IRRELEVANT
Obligation

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

A five-year review was conducted in 2009–2010 to evaluate whether CSEC and DND/CF efforts were adhering to a comprehensive accountability framework for Canadian SIGINT, as set out by the ISOM Ministerial Directive (MD). The results from the review, and subsequent direction from the ISOM Steering Committee (SC), led to the development of the Integration Action Plan (IAP) which aims to increase the efficiency of the Canadian SIGINT enterprise.

The ISOM IAP and CSEC's internal business planning regime are focused on establishing an enduring partnership by 2015. One of the primary enablers to this partnership was completed in 2011–2012 with the establishment of an integrated National SIGINT Priorities List (NSPL) that reflects the standing and ad hoc SIGINT requirements for the GC and the CF. The NSPL is a major step in integrating the full spectrum of Canadian SIGINT collection and reporting efforts, thus eliminating duplication and increasing efficiencies.

[redacted]

IRRELEVANT

[redacted] Cabinet Confidence

Cabin IRRELEVANT

IRRELEVANT

Looking ahead to 2012–2013, CSEC anticipates a number of key changes. Canadian [redacted]

[redacted]

[redacted] The enhanced cooperation between CSEC and CFIOG exemplifies the spirit of ISOM as progress is made towards the "single seamless Canadian cryptologic enterprise" envisaged for 2015.

SPECIAL REPORT: [redacted]

[redacted]

[redacted]

[redacted]

SPECIAL REPORT: [redacted]

[redacted]

SPECIAL REPORT: [redacted]

[redacted]

SPECIAL REPORT: [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

SPECIAL REPORT: IRRELEVANT

IRRELEVANT

[redacted]

4 [redacted]

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 2011–2012, 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-1-7, *Operational Procedures for Naming in SIGINT Reports*;
- OPS-1-15, *Operational Procedures for Cyber Defence Activities Using System Owner Data*; and
- OPS-1-14, *Operational Procedures for Cyber Defence Operations Conducted Under Ministerial Authorization*

Occasionally, CSEC and its Allies incidentally acquire information about their own nationals. To protect the individual's privacy, this information is suppressed in intelligence reports. However, CSEC may release the names of other identifying features of Canadian entities to Government departments or international Allies, but only under strict conditions, namely that the requesting entity have lawful authority to receive the information.

A review conducted by the Office of the CSEC Commissioner examined Operational Policy's releases of Canadian identities to Government of Canada clients over the period of January to June 2011. Results were positive for CSEC, with the Commissioner noting that such activities were conducted lawfully.

In 2011–2012, CSEC released [redacted] pieces of Canadian identity information stemming from [redacted] Canadian and allied foreign intelligence reports. This represents [redacted] in the number of identities released ([redacted] in 2010–2011) and [redacted] in the number of reports released ([redacted] in 2010–2011). As in years past, the majority of this information was released to CSIS [redacted] Canadian identities, or [redacted]%). In addition, CSEC released [redacted] Canadian identities to its Five Eyes partners.

CSEC's interaction with the RCMP's Special Information Handling Unit (SIHU) and with the RCMP-hosted multi-departmental National Joint Intelligence Group (NJIG) remained high in 2011–2012. [redacted]

2011–2012 was the first full fiscal year during which the release of Canadian identity information to other countries was subject to the GC *Framework for Addressing Risks in Sharing Information with Foreign Entities*. CSEC, in consultation with its Directorate of Legal Services (DLS), worked closely to develop and implement a comprehensive protocol to ensure that all such releases align with the Framework and CSEC's associated Ministerial Directive. Over [redacted] assessments were conducted by Operational Policy to support this decision-making. Operational Policy is revising OPS-2-1, *End-Product Sanitization/Action-on Procedures*, to reflect the Framework and MD.

In October 2011, DLS produced an opinion entitled Solicitor-Clier

Solicitor-Client Privilege

[redacted]

SPECIAL REPORT: INTERNAL SECURITY AND POLYGRAPH TESTING

IRRELEVANT

IRRELEVANT