



Communications Security
Establishment Canada

Centre de la sécurité
des télécommunications Canada



COMMUNICATIONS SECURITY
ESTABLISHMENT CANADA

ANNUAL REPORT TO THE MINISTER OF NATIONAL DEFENCE 2010–2011

September 2011

Minister:

I am very pleased to submit to you the CSEC Annual Report for fiscal year 2010–2011. This eleventh Annual Report discusses CSEC's priorities and challenges over the past year, highlights our key accomplishments and addresses a number of special reporting requirements. It also focuses on some of our future intentions and efforts to remain relevant in an ever changing technological environment.

In 2010–2011, CSEC continued to mature as an organization uniquely positioned to lead Government of Canada (GC) efforts to address cyber security threats. We are also at the forefront of the Five-Eyes partnership in the development of many key capabilities, such as our highly productive [REDACTED] program. In addition to our ongoing commitment to address GC Intelligence Priorities, CSEC is also providing critical support to Canada's security and intelligence community on emerging issues, including [REDACTED] in support of Canadian Forces operations as well as GC efforts to combat [REDACTED]

Cabinet Confidence

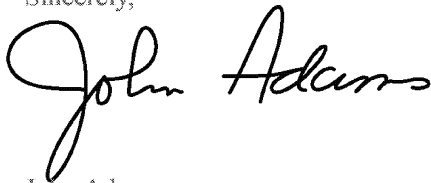
Internally, CSEC is placing significant emphasis on enhancing our accountability and reporting regimes to reflect our growth and increasing prominence. In 2010–2011, CSEC participated in the Management Accountability Framework exercise for the first time and will continue to pursue similar initiatives to mature our corporate management framework.

With the contract for the Long-Term Accommodations awarded, CSEC is turning its attention to evolving and building for the future. CSEC 2015, a statement of our strategic vision, outlines how we will maximize the collaborative opportunities of our new space to meet our organizational challenges. Equipping CSEC for the future will require investment across the organization. One of the keys to our success will be the effective use of automation to manage and maximize the benefits of the tremendous volume of information generated by our enhanced cyber threat monitoring [REDACTED]. We will also continue to leverage our [REDACTED] Second Party partners [REDACTED] including [REDACTED]. Through these and other tactics, CSEC will be best positioned to continue mission-critical functions and respond to emerging issues of concern to the GC and our allies, such as [REDACTED] protection.

Cabinet Confidence

Our greatest asset in addressing the challenges of today and preparing to tackle the issues of tomorrow is our exceptionally talented and dedicated workforce — Team CSEC. As Chief, I am committed to building on our potential by cultivating an organizational culture of transformational leadership and collaboration that recognizes the significant contribution of our employees to safeguard Canada's security.

Sincerely,



John Adams
Chief

c.c. Stephen Rigby, National Security Advisor to the Prime Minister
Robert Fonberg, Deputy Minister, National Defence

TABLE OF CONTENTS

NATIONAL AND INTERNATIONAL CONTEXT	1
Domestic Environment	1
Global Environment	2
SIGNALS INTELLIGENCE	3
Reporting on Intelligence Priorities	3
IRRELEVANT	7
Signals Intelligence Challenges	7
INFORMATION TECHNOLOGY SECURITY	9
Cyber Defence	9
Cyber Protection	10
IT Security Challenges	12
JOINT COLLABORATION: SIGINT AND IT SECURITY	13
Joint Research Office (JRO)	13
Cryptologic Research Institute (CRI)	13
Other Collaboration	14
POLICY, COMMUNICATIONS AND PARTNERSHIPS	15
Lawful Review	15
Authorities	16
Communications	17
Partnerships	17
Policy, Communications and Partnerships Challenges	19
INTERNAL SERVICES	21
IRRELEVANT	21
.....	22
.....	23
.....	23
.....	25
.....	25
.....	26
.....	26
.....	26
CONCLUSION	29
ANNEX A: List of Current CSEC Ministerial Authorizations and Directives	31
ANNEX B: Special Reports	33

LIST OF 2010–2011 HIGHLIGHTS

IRRELEVANT	4
[REDACTED]	5
[REDACTED]	5
CSEC Contribution to GC Efforts to Cabinet Confidence	6
[REDACTED]	7
Implementing Canada's Cyber Security Strategy (CCSS)	10
Newly Deployed Sensors Lead to Cyber Incident Discovery	10
IRRELEVANT	11
Advancing Allied Research Collaboration	13
[REDACTED]	18
IRRELEVANT	22
The Cohort Foundational Learning Experience at CSEC	23
CSEC Strengthens its Accountability and Reporting Regime	24

NATIONAL AND INTERNATIONAL CONTEXT

In our strategic effort to keep pace with an ever-changing threat and technology environment, CSEC continues to monitor domestic and global trends in security and intelligence and maintain a reputation for rapidly adapting our approaches to most effectively respond to changing needs.

However, in the context of resource constraints, the challenge continues to be addressing long-standing priorities such as Cabinet Confidence while remaining responsive to emerging priorities shaped by recent events.

DOMESTIC ENVIRONMENT

Within the Government of Canada (GC), priorities for foreign intelligence collection have remained quite stable. Addressing Cabinet Confidence continues to be the number one priority of the Canadian Security and Intelligence (S&I) community [REDACTED]

In fiscal year (FY) 2010–2011, support for the Canadian combat mission in Afghanistan remained a key priority moving towards the planned end of the combat mission in 2011. Following the November 2010 announcement of a continuing training mission in Afghanistan, CSEC efforts have been directed [REDACTED]

██████████ in 2010–2011 have increased the focus of GC efforts on a number of emerging priorities. With the release of Canada's Cyber Security Strategy in October 2010, significant attention was focussed on the need to address cyber threats to Canada. However, our perspective on those threats has been enhanced by the discovery in early 2011 of significant ██████████ state-sponsored cyber intrusion activity affecting multiple GC departments. Similarly, the challenge posed by ██████████ was first highlighted by the ██████████

██████████ has led the GC to develop legislative and operational measures to deter further ██████████

Canada's S&I community itself has also come under scrutiny. The final report of the Commission of Inquiry into the Investigation of the Bombing of Air India Flight 182 was released in June 2010 and followed by a Government Response and Action Plan in December. A key focus of the Commission was the importance of improved coordination and information sharing among partners in the S&I community. These views have also been echoed in a recent Senate committee report. While no specific action on these recommendations has been taken to date, the implications for CSEC could be significant.

The end of 2010 brought to a close a year of unusually ██████████. Beginning with ██████████ fiscal year 2009–2010 and continuing with ██████████ these ██████████ have provided the S&I community with a number of lessons learned that will be of great value when Canada ██████████

GLOBAL ENVIRONMENT

A striking theme of the international security and intelligence environment in 2010–2011 is the recognition of the global nature of threats and vulnerabilities. In addressing these threats, CSEC continues to work with its international partners in the Five-Eyes cryptologic alliance, 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).

Canada was also not alone in uncovering major cyber incidents in 2010–2011. Countries like France and Australia as well as security firms RSA and Comodo have hit the front pages with the detection of sophisticated cyber intrusions targeting government and internet security related information. Cyber security has also been a significant focus of government attention in 2010–2011, including the full launch of the US Cyber Command approach to synchronized cyber defence based at NSA. In the UK, cyber threats have been listed among the top four priority risks in the British *National Security Strategy*. An added dimension has been the prevalence of cyber activism, including the efforts to both promulgate and cripple the Wikileaks website and the reprisals taken by the hacking group *Anonymous* against companies perceived as anti-Wikileaks. *Anonymous* also disabled government websites in Tunisia and Egypt in support of democratic protests in those countries. Undoubtedly, the cyber threat environment is evolving at a pace that poses a significant challenge, not only to Canada but also to our Allies.



SIGNALS INTELLIGENCE

The CSEC Signals Intelligence (SIGINT) program continued to make important contributions to Canada's national security in FY 2010–2011 through its efforts to support GC Intelligence Priorities. These contributions enhanced the protection of Canadian lives and interests throughout the world.

REPORTING ON INTELLIGENCE PRIORITIES

The successful conduct of SIGINT operations requires specific, focused objectives and requirements as well as the ability to prioritize targets of the highest possible importance to Canada. Through a major annual update and quarterly review process, CSEC produces a National SIGINT Priorities List (NSPL) based on direction from the Minister of National Defence on Cabinet-approved GC Intelligence Priorities as well as input from key departments and agencies. This year's NSPL continues to reflect GC Intelligence Priorities focusing on

Cabinet Confidence

Cabinet Confidence

This report notes a number of CSEC achievements throughout the fiscal year in addressing these priorities, including [REDACTED]. Looking ahead to FY 2011–2012, SIGINT will continue to address a wide range of targets with emphasis on the issues of highest importance as determined by Cabinet. In the face of standing requirements and other emerging intelligence needs, the CSEC SIGINT program remains committed to addressing GC Intelligence Priorities through its internal reallocation and prioritization exercises.

Cabinet Confidence

CSEC provides actionable signals intelligence¹ for detecting and preventing **Cabinet** threats against North America, as well as against Canadian and allied interests abroad. Key clients are the Canadian Security Intelligence Service (CSIS), the Department of National Defence (DND), and the Department of Foreign Affairs and International Trade (DFAIT), along with allied military and intelligence services.

With a focus on the protection of Canadians at home and abroad, targets representing a “threat to life” are, in fact, the single highest priority associated with SIGINT analytic activity and targeting. In 2010–2011, CSEC identified and intercepted communications of various groups and individuals involved in threats against Canadian and allied interests, particularly in relation to [REDACTED] high-profile kidnappings. CSEC reporting has resulted in protecting the lives of Canadian and allied nationals **Cabinet Confiden**

Cabinet Confidence

For example, CSEC continues to track and develop [REDACTED] to mitigate the significant risk of attacks and kidnappings carried out by [REDACTED]

IRRELEVANT**Cabinet Confidence**

CSEC continues to provide intelligence support for **Cabinet Confid**
Cabinet Confidence

Cabinet Confidence

¹ 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.

[REDACTED]

Cabinet Confidence

[REDACTED]

Cabinet Confidence

In 2010–2011, CSEC provided actionable intelligence for both GC and allied government clients on activity linked to

Cabinet Confi

Cabinet Confidence

Cabinet Confidence

SIGINT

reporting supported [REDACTED]
[REDACTED] and facilitated
the [REDACTED] As well, reporting identified
entities and activities of concern to CSIS, DND, Health Canada, DFAIT
and others. As reflected in Canada's intelligence priorities, CSEC
responded to requirements regarding [REDACTED]

[REDACTED]

For example, CSEC was recently successful in attributing the
activity of a well known cyber actor, [REDACTED]

[REDACTED]

Cabinet Confidence

CSEC works closely with CSIS and its Five-Eyes partners to identify and monitor threats [redacted] **Cabinet Confidence**

SIGINT insight also helps [redacted] **Cabinet Confidence**

Cabinet As part of its [redacted] support role, CSEC reporting often results in [redacted] opportunities and identification of threats to Canadian interests. In 2010–2011, close collaboration with UK and US counterparts led to the disruption of some [redacted] operations based on the technical expertise CSEC provided to GCHQ [redacted] [redacted] on a specific aspect of the [redacted] [redacted] program.

Cabinet Confidence

CSEC conducts SIGINT development efforts and reporting to support the GC [redacted] **Cabinet Confi** In particular, CSEC assists in providing

Cabinet Confidence

Cabinet Confi In the past year, CSEC provided intelligence on a number of [redacted]

[redacted] As well, CSEC monitors the policies and activities of actors [redacted] [redacted], and [redacted] which have demonstrated increased interest in [redacted]

[redacted] CSEC also participates in the [redacted] in collaboration with Five-Eyes [redacted] partners to further enhance information flow and to increase understanding of [redacted]

Cabinet Confidence

CSEC provides actionable signals intelligence on [redacted] **Cabinet Con** and [redacted] **Cabinet Confidence** to key clients such as CBSA, DND, CSIS and RCMP. CSEC's focus is the provision of intelligence to protect Canada and its Allies from [redacted] **Cabinet Confidence** and from

Cabinet Confidence

Cabinet Confi Key activities include [redacted]

In 2010–2011, CSEC successfully identified and intercepted the communications of various groups and individuals, including [redacted]

CSEC CONTRIBUTION TO GC EFFORTS
To **Cabinet Confidence**

CSEC has made a significant contribution to GC efforts to [redacted]

[redacted] In addition, CSEC reporting has made significant contributions to our understanding of [redacted]

Cabinet Confidence

CSEC addresses [redacted] **Cabinet Confidence** requirements generally linked to: **Cabinet Confidence**

Cabinet Confidence

Cabinet Confidence as well

as coverage of breaking issues and crises. In response to emerging crises, CSEC generated reporting on [redacted]

[redacted] CSEC also addressed a number of requirements for foreign intelligence related to the [redacted]

TOP SECRET//COMINT//CANADIAN EYES ONLY

In 2010–2011, CSEC provided significant intelligence support for
Cabinet Confidence

Cabinet Client Relations Officers (CROs) frequently provide timely

[REDACTED]

[REDACTED]

CSEC significantly enhanced collection [REDACTED]

[REDACTED]

[REDACTED] IRRI

IRRELEVANT

IRRELEVANT

[REDACTED]

IRRELEVANT

SIGNALS INTELLIGENCE CHALLENGES

Collaboration [REDACTED]

As Five-Eyes nations [REDACTED] seek to increase their level
of cooperation [REDACTED] it is becoming clear that policy
and legal differences in the respective countries can negatively
influence collaborative efforts. IRRELEVANT

IRRELEVANT

IRRELEVANT

Efforts to collaborate in the cyber domain
are also complicated as this area has yet to be clearly defined from
legal and policy standpoints. Among the Five-Eyes there are varying

2 A SIGINT report is rated "Exceptional" when a) it is shown or briefed to a Canadian/allied Cabinet Minister-equivalent or above, b) it provides unique insight on issues of importance to the client, or c) it strongly corroborates other information of importance to the client.

approaches to the cyber security mission and the complexity of assuring multinational collaboration is compounded by the number of potential GC players in the cyber security domain, and the need to ensure clear lines of authority and responsibility to enable [REDACTED] in this highly technical field. While it is a significant challenge to resolve fundamental national differences in policy and law at a rapid operational tempo, CSEC is working in various fora to address these issues.

Emerging Priorities and Building for the Future

IRRELEVANT

IRRELEVANT



INFORMATION TECHNOLOGY SECURITY

The CSEC IT Security program aims to protect electronic information and information infrastructures of importance to the GC, as mandated by the NDA. This program is the lead technical authority for IT security for the GC and is divided into two branches: the Cyber Defence Branch, focussed on cyber threats; and the Cyber Protection Branch, which provides product architectural and engineering guidance and services for the protection of GC information systems.

CYBER DEFENCE

The CSEC Cyber Defence Branch undertakes efforts to help protect the GC from sophisticated cyber threats. Operations are conducted to detect, analyze, evaluate, mitigate, and defend against incidents that are occurring on Government systems of importance. The following sections outline in greater detail CSEC's accomplishments over the past year in strengthening the security posture of the Government by preventing cyber intrusions, including those conducted by the most sophisticated threats to Canada's national security.

In 2010–2011, the Cyber Defence Branch became fully operational after a year of transition that saw the establishment of new reporting lines, the development of direct and sustained relationships with key departments, the deployment of a highly developed sensor capability on Public Works and Government Services Canada's (PWGSC) Secure Channel Net (SCNet), and the strengthening of relationships within the S&I community.

IMPLEMENTING CANADA'S CYBER SECURITY STRATEGY (CCSS)

The CCSS recognizes CSEC's unique capabilities and leadership role in combating cyber threats to GC networks. CSEC directed first year CCSS funding to invest in systems that will provide CSEC's Cyber Threat Evaluation Centre and [REDACTED] areas with increased access to threat data. These systems will provide an enhanced perspective of the cyber threats affecting Government of Canada systems and lay the foundation upon which an increased analyst complement will search out new threats and threat actors.

The Cyber Threat Evaluation Centre

CSEC's Cyber Threat Evaluation Centre (CTEC) was created in 2009 to ensure greater coordination and synchronization between the CSEC IT Security and SIGINT programs and to act as the entry point into CSEC for Government in all matters related to cyber defence. It provides cyber threat detection and cyber situational awareness at a variety of classification levels to a diverse set of stakeholders that range from senior Government executives through to IT security professionals, as well as to CSEC's domestic and allied partners. This information provides decision makers and IT security professionals with the ability to more effectively defend against cyber threats specific to the GC, and to anticipate future cyber threats.

In the past year, CTEC increased the set of reporting products and services that convey important cyber threat information to these stakeholders:

- A core monthly report that provides a baseline of threat knowledge at the SECRET level for distribution to Chief Information Officers and IT security personnel. These details include the scope of the threat (number of incidents), information about threat actors (what [REDACTED] are employing which technical exploitation capabilities), and the severity of the threat (based on how many systems have been compromised).
- Products that provide a unique perspective on the capabilities, tradecraft and targeting by the [REDACTED] cyber threat actors.
- Unclassified reports and mitigation advice for broad distribution across government. CTEC has worked to establish these low-classification reports that are based on highly sensitive information to allow the broadest possible distribution.

Sensor Deployment

In October 2010, CSEC initiated a sensor deployment [REDACTED]

NEWLY DEPLOYED SENSORS LEAD TO CYBER INCIDENT DISCOVERY

Enhanced CSEC monitoring through the deployment of the [REDACTED]

[REDACTED] In a large scale effort, CSEC engaged with partners in the federal IT security community and provided immediate mitigation advice implemented by affected departments to address the threat.

CYBER PROTECTION

IRRELEVANT

TOP SECRET//COMINT//CANADIAN EYES ONLY

IRRELEVANT

IRRELEVANT

IRRELEVANT

IRRELEVANT

IT SECURITY CHALLENGES

Evolving Cyber Threat and Technology Environment

Cyber threats are constantly evolving, both in frequency of occurrence and sophistication. As CSEC capitalizes on recent investments to advance our capabilities and capacities to combat the growing cyber threat, the more threats are discovered. Canada is not alone in facing this challenge – a global reality that both government and non-government systems are constantly at risk with no quick solution. CSEC has identified a need for supplementary investment to expand coverage to detect these threats through additional sensor development and deployment as well as other enhanced analytic and defence capabilities. In other internal efforts to keep pace, the CSEC IT Security program is also placing an emphasis on prioritization of clients needs and developing automated cyber defence tools to allow for quick response and mitigation.

CSEC also needs to keep pace with the rapid evolution of technologies such as cloud computing and wireless devices and networks. As these new technologies emerge, clients become eager to incorporate them into their day-to-day business in order to work more efficiently. CSEC continues to engage with GC clients to emphasize the importance of thorough product examination prior to deployment in order to provide the appropriate security guidance necessary to protect GC information and information systems at both the classified and unclassified levels. The ability to recruit and retain highly-qualified technical personnel will be crucial to addressing this and other challenges.



JOINT COLLABORATION: SIGINT AND IT SECURITY

JOINT RESEARCH OFFICE (JRO)

CSEC has established the JRO to ensure CSEC's research and experimental development program addresses the immediate science and technology issues critical to meeting both the CSEC SIGINT and IT Security mandates. The key objectives of the JRO are to:

- Ensure critical 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;
- Foster out-of-program research work to accelerate workplace innovation; and
- Effectively and economically manage the research program.

These activities permit CSEC to pursue enhanced collaboration on science and technology issues with external partners based on a thorough understanding of research activities, gaps, priorities and opportunities.

In FY 2010–2011 the JRO identified, prioritized and promulgated CSEC research requirements for enhanced coordination internally and with key domestic and allied partners. Increased engagement with Defence Research & Development Canada (DRDC) was also pursued to identify relevant research activities for coordination,

including cyber-related research. As well, a [REDACTED]

ADVANCING ALLIED RESEARCH COLLABORATION

CSEC is emerging as a leader in the area of research collaboration within the Five-Eyes alliance. In October 2010, CSEC coordinated and hosted the first Five-Eyes Research Chiefs meeting to be held in many years. CSEC benefited from additional perspectives on research challenges from allied partners. In follow-up, each partner agency is identifying areas of strength and weakness to best coordinate our respective research programs. The event was the first official activity hosted in the new Cryptologic Research Institute facility.

CRYPTOLOGIC RESEARCH INSTITUTE (CRI)

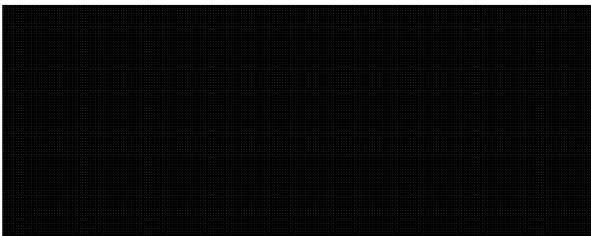
In order to tackle the hardest methodological problems on the technical horizon, the newly-renovated CRI Facility in Ottawa opened its doors to the first of its cryptologic researchers in November 2010. CSEC is working with leading IT providers to complete the technology integration in the collaborative spaces. The program continues to be coordinated through the JRO and in support of the objectives in the *CSEC Strategic Plan*.

The four primary responsibilities of the CRI are to:

- Address the most important scientific challenges facing CSEC;
- Attract and engage Canada's top researchers to work in support of CSEC;
- Obtain the highest possible return on Canada's research partnerships within the allied Cryptologic Research Community; and
- Create and maintain a world leading cryptologic research knowledge center to enable effectual knowledge discovery and transfer.

A vital part of the new CRI facility is its Advanced Collaborative Environment (ACE). The ACE will be one of the world's most sophisticated collaborative spaces, providing researchers with the ability to conduct video conferences and advanced computer interactions at the highest classification level. These capabilities will significantly increase the ability of researchers across the cryptologic intelligence community to collaborate on the hardest mathematical problem sets.

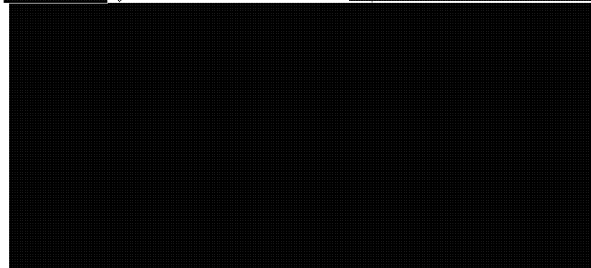
Over the past fiscal year there has been a significant increase in the number of top Canadian and leading international academic researchers engaged to work for the CRI. The CRI is also facilitating the ability of its researchers to access resources in the National Capital Region through the establishment of a Memorandum of Understanding (MOU) with Carleton University providing CRI members with access to university facilities. In October 2010, the CRI also hosted a Knowledge Discovery workshop in partnership with Carleton University aimed at identifying key "open problems" that face the S&I community.



OTHER COLLABORATION

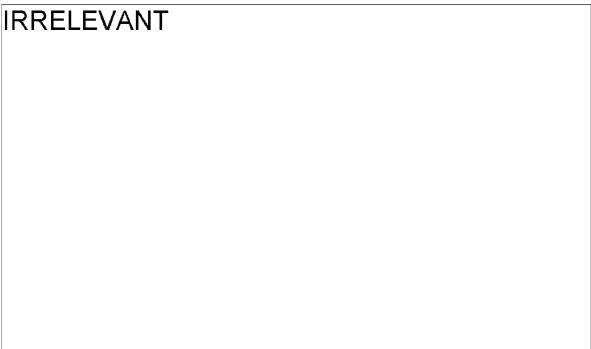
Analytical Collaboration

Over 2010–2011, CSEC's IT Security and SIGINT programs have further refined an integrated approach in response to the [REDACTED] cyber threat to GC networks. [REDACTED]



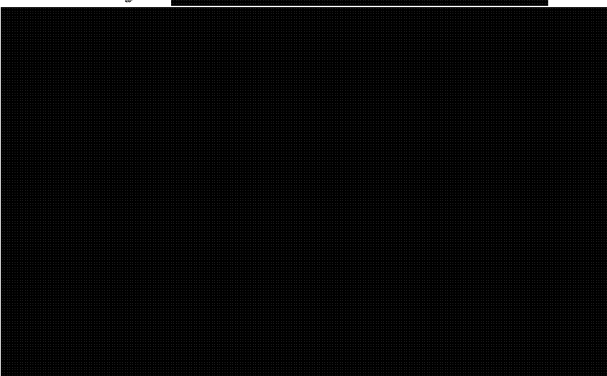
The Joint Career Framework

IRRELEVANT



Tools and Expertise

CSEC's SIGINT and IT Security programs are also sharing relevant staff expertise and tools that support CSEC cyber defence activities, such as identifying the source of cyber intrusions. This includes the [REDACTED] to [REDACTED]. This has enabled IT Security to better assess the extent of cyber compromises and it is expected that the demand for [REDACTED] services will grow. [REDACTED]



POLICY, COMMUNICATIONS AND PARTNERSHIPS

LAWFUL REVIEW

As with other federal agencies, CSEC is subject to review by the Privacy Commissioner, the Auditor General, the Information Commissioner and Commissions of Inquiry. The CSE Commissioner is CSEC's primary review official, whose role it is to ensure the lawfulness of CSEC activities and to investigate and respond to complaints, if required. In addition to the CSE Commissioner, CSEC is also subject to review as a federal agency.

In FY 2010–2011, CSEC provided information to the Office of the CSE Commissioner (OCSEC) in response to eleven reviews, six of which were completed:

- Computer Network Defence;
- Active Network Security Testing;
- Disclosure of Information about Canadians to GC Clients;
- Contact Chaining;
- SIGINT Ministerial Authorizations; and
- Targeting and Selector Management.

Ongoing reviews pertain to:

- Information Sharing with Second Parties;
- Retention and Disposal of Information Obtained under Ministerial Authorization;

IRRELEVANT

- A review of the CSEC Privacy Incident File; and
- A review of CSEC activities related to [REDACTED]

Furthermore, OCSEC has requested that CSEC provide any new identified 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

TOP SECRET//COMINT//CANADIAN EYES ONLY

IRRELEVANT

TOP SECRET//COMINT//CANADIAN EYES ONLY

COMMUNICATIONS

PARTNERSHIPS

IRRELEVANT

IRRELEVANT

reuse and sharing of technology between the partners. A very recent worthwhile accomplishment was a [REDACTED] of [REDACTED]

From a SIGINT operations perspective, CSEC is considered a key player among the Five-Eyes, with leading expertise in key capabilities and reporting lines (e.g., [REDACTED]). A number of highlights from the 2010–2011 reporting period underscore the contribution of CSEC to the allied community, in return for which Canada derives significant benefit, in terms of expertise and shared resources.

International Partners

Over the past year, collaboration with the traditional Five-Eyes partners has remained at the forefront of CSEC's priorities as the 65-year-old alliance continues to manifest unparalleled integration and efficiency in achieving Canada's national security and foreign policy interests. Also, the demonstrated value to Canada's national security interests has prompted CSEC to maintain a high-level of priority on enhancing relationships [REDACTED]

CSEC engages with its Allies in both technical and operational collaboration. CSEC is working with its Five-Eyes partners to further technical integration of our respective systems and to optimize interoperability. As part of this effort, CSEC actively pursues the

In the face of a growing cyber threat, the Five-Eyes community continued to evolve and expand its collaborative approach on cyber security under the auspices of the [REDACTED]

In 2010–2011, CSEC's collaboration with its Five-Eyes partners on IT security was significant. This collaboration with allied partners, particularly the NSA [REDACTED]

CSEC recognizes the value-added contribution of [REDACTED]

(see Annex B Special Report: [REDACTED])

POLICY, COMMUNICATIONS AND PARTNERSHIPS CHALLENGES

IRRELEVANT

IRRELEVANT

TOP SECRET//COMINT//CANADIAN EYES ONLY

INTERNAL SERVICES

IRRELEVANT

TOP SECRET//COMINT//CANADIAN EYES ONLY

IRRELEVANT

IRRELEVANT

CSEC 2015 STRATEGIC PRIORITIES

1. Strengthen "Team CSEC" and prepare for [REDACTED] IRRELEVANT
2. Adopt innovation and agile business solutions
3. Expand our [REDACTED] [REDACTED]
4. Improve analytic tradecraft
5. Automate manual processes
6. Synchronize the cryptologic enterprise for the cyber security mission
7. Enable [REDACTED] IRRELEVANT for threat mitigation

IRRELEVANT

TOP SECRET//COMINT//CANADIAN EYES ONLY

IRRELEVANT

AUDIT, EVALUATION AND ETHICS

IRRELEVANT

IRRELEVANT

TOP SECRET//COMINT//CANADIAN EYES ONLY

IRRELEVANT

TOP SECRET//COMINT//CANADIAN EYES ONLY

CONCLUSION

CSEC is proud to report on the many successes of the past fiscal year including:

- Critical SIGINT contributions to disrupting terrorist networks both at home and abroad;
- Effective detection and mitigation of the most significant series of cyber intrusions on GC networks that has been detected to date;
- Development of tools and engagement strategies to both prevent and detect future intrusions;
- Innovative collaboration with domestic and allied partners in response to the changing threat and technology landscape; and

IRRELEVANT

Across the organization, CSEC is focussed on developing the cutting-edge capabilities and capacities that will enable the organization to enhance its leadership role in key areas (e.g. cyber security [REDACTED]) as well as provide ongoing critical support to GC clients and allied partners in the context of a shifting global security and threat landscape. IRRE

IRRELEVANT

From the perspective of both its foreign intelligence and IT security missions, CSEC also continues to experience [REDACTED] in the volumes of valuable SIGINT traffic and cyber defence data processed on a daily basis. CSEC is committed to responding to this and other challenges noted throughout this report through the effective use of innovative tradecraft, tools and automation that will also allow us to continue to do more with available resources. Enhanced collaboration both internally and across a broad range of domestic [REDACTED] has been and will continue to be a key focus of CSEC activities. Our accomplishments in this area serve to cement CSEC's domestic and international reputation as an agile, innovative and valuable partner.

Looking forward, CSEC has released a new strategic vision, *CSEC 2015*, focussed on the seven priorities that are key to meeting operational challenges while maximizing the potential for collaboration and innovation provided by CSEC's new accommodations. Future annual reports on CSEC priorities, activities and challenges will serve to highlight our progress towards this vision in our ongoing efforts to safeguard Canada's security through information superiority.

TOP SECRET//COMINT//CANADIAN EYES ONLY

ANNEX A: LIST OF CURRENT CSEC MINISTERIAL AUTHORIZATIONS AND DIRECTIVES**MINISTERIAL AUTHORIZATIONS (MAs)³***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)

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)⁴

- MD Accountability Framework (June 2001)
- MD Privacy of Canadians (June 2001)
- MD [REDACTED]
[REDACTED]
- 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 (March 2005)
- MD [REDACTED]
- MD [REDACTED] (August 2006)
- [REDACTED]
[REDACTED]
- MD Intelligence Priorities (updated annually)

³ 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.

⁴ CSEC also has three ECI MDs dealing with highly sensitive SIGINT initiatives.

TOP SECRET//COMINT//CANADIAN EYES ONLY

ANNEX B: SPECIAL REPORTS

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.

NUMBER: 1
 SPECIAL REPORT: ISOM and the Mission in Afghanistan
 OBLIGATION: 2004 Integrated SIGINT Operational Model Ministerial Directive
 SPECIAL HANDLING: TOP SECRET//COMINT//CEO

NUMBER: 2
 SPECIAL REPORT: [REDACTED]
 OBLIGATION: 2002 [REDACTED] Operations Ministerial Directive
 SPECIAL HANDLING: TOP SECRET//COMINT//CEO

NUMBER: 3
 SPECIAL REPORT: [REDACTED]
 OBLIGATION: 2004 [REDACTED] Ministerial Directive
 SPECIAL HANDLING: TOP SECRET//COMINT//CEO

NUMBER: 4
 SPECIAL REPORT: IRRELEVANT
 OBLIGATION: [REDACTED]
 SPECIAL HANDLING: TOP SECRET//COMINT//CEO

NUMBER: 5
 SPECIAL REPORT: Privacy of Canadians
 OBLIGATION: Voluntary - Response to CSE Commissioner Recommendations
 SPECIAL HANDLING: TOP SECRET//COMINT//CEO

NUMBER: 6
 SPECIAL REPORT: [REDACTED]
 OBLIGATION: 2006 [REDACTED] Ministerial Directive
 SPECIAL HANDLING: TOP SECRET//COMINT//CEO [REDACTED]

NUMBER: 7
 SPECIAL REPORT: IRRELEVANT
 OBLIGATION: [REDACTED]
 SPECIAL HANDLING: SECRET

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

As reported last year, a five-year Review was conducted in 2009–2010 to confirm that CSEC and DND/CF efforts were meeting the intent of the ISOM Ministerial Directive (MD) for a comprehensive accountability framework for Canadian SIGINT. In 2010–2011, the results from the Review and subsequent direction from the ISOM Steering Committee have resulted in an Integration Action Plan (IAP) that will afford greater efficiencies and effectiveness within the Canadian SIGINT enterprise.

The ISOM IAP and CSEC's internal business planning regime are working towards an enduring and fully integrated partnership by 2015. One of the primary enablers of the partnership is establishing an integrated SIGINT requirements list for the GC and the CF. A single National SIGINT Priorities List (NSPL) is a major step in integrating the full spectrum of Canadian SIGINT collection and reporting efforts and will eliminate duplication of effort.

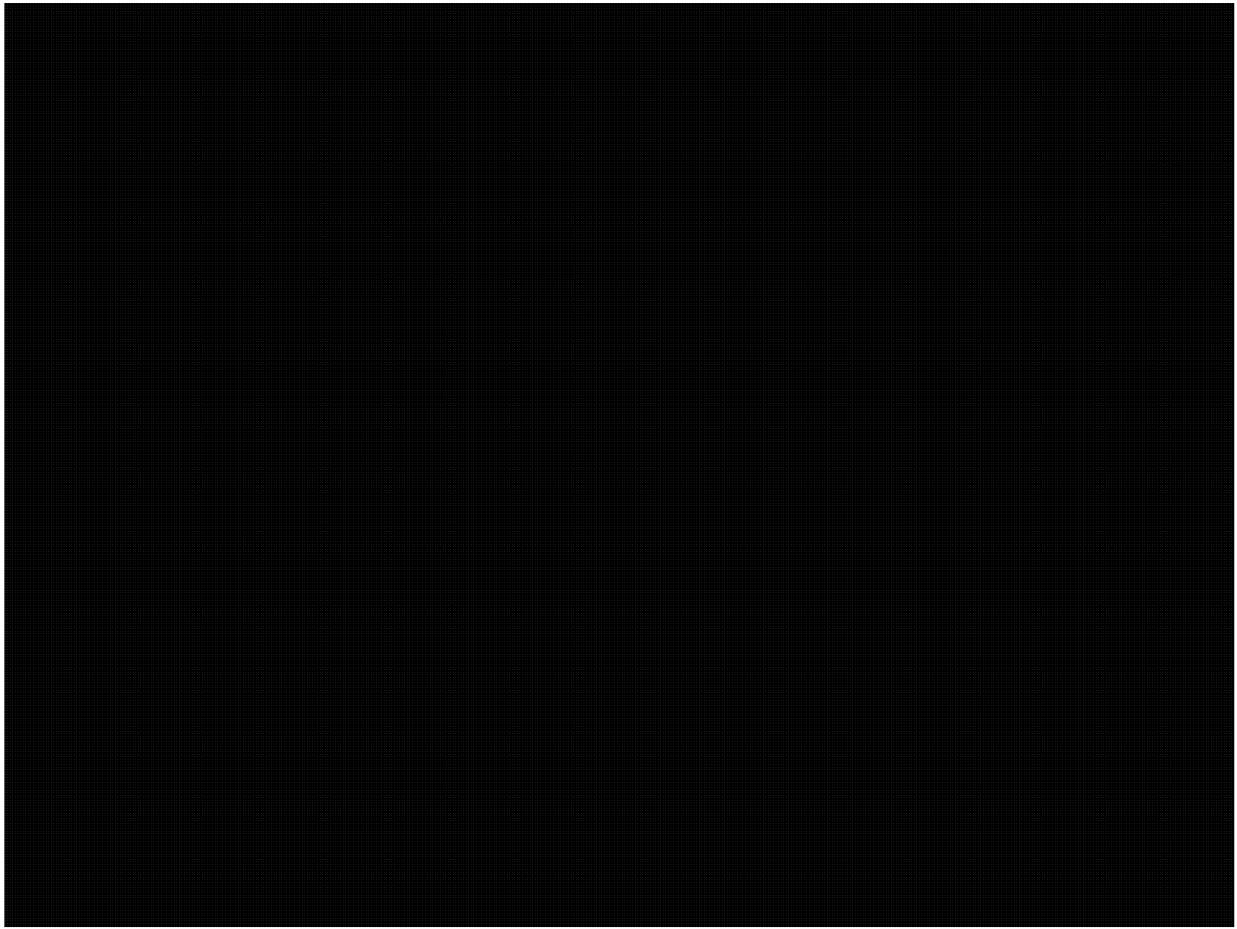
IRRELEVANT

Managing the transition from the existing CF mandate in southern Afghanistan through the end of the combat mission [REDACTED] will accelerate CSEC's efforts to implement the next generation ISOM over the next year. Institutionalized capabilities like the integrated [REDACTED] at CSEC and CFS Leitrim will continue to support the operational demands and requirements of the tactical commanders, as required. At the same time, [REDACTED] will continue to address GC requirements while enhancing the Canadian contribution to the overall Five-Eyes SIGINT Enterprise.

Through the [REDACTED] Program, CSEC has now [REDACTED] to complement other [REDACTED] capabilities. The resulting enhanced cooperation between CSEC and CFIOG exemplifies the spirit of ISOM and is an acknowledged best practice by allied partners.

2. SPECIAL REPORT: [REDACTED]

3. SPECIAL REPORT: [REDACTED]



4. SPECIAL REPORT: [IRRELEVANT]

IRRELEVANT

5. SPECIAL REPORT: PRIVACY OF CANADIANS

Under the *NDA*, CSEC is explicitly 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 2010–2011, 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-1-10, *Operational Procedures for Metadata Analysis* [REDACTED];
- OPS-1-12, *Procedures for Active Network Security Defence (ANST)*;
- OPS-1-13, *Procedures for* [REDACTED] *and Joint CSEC-CF Activities*; and
- OPS-3-1, *Procedures for* [REDACTED] *Operations*.

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 a specific operational requirement for the information.

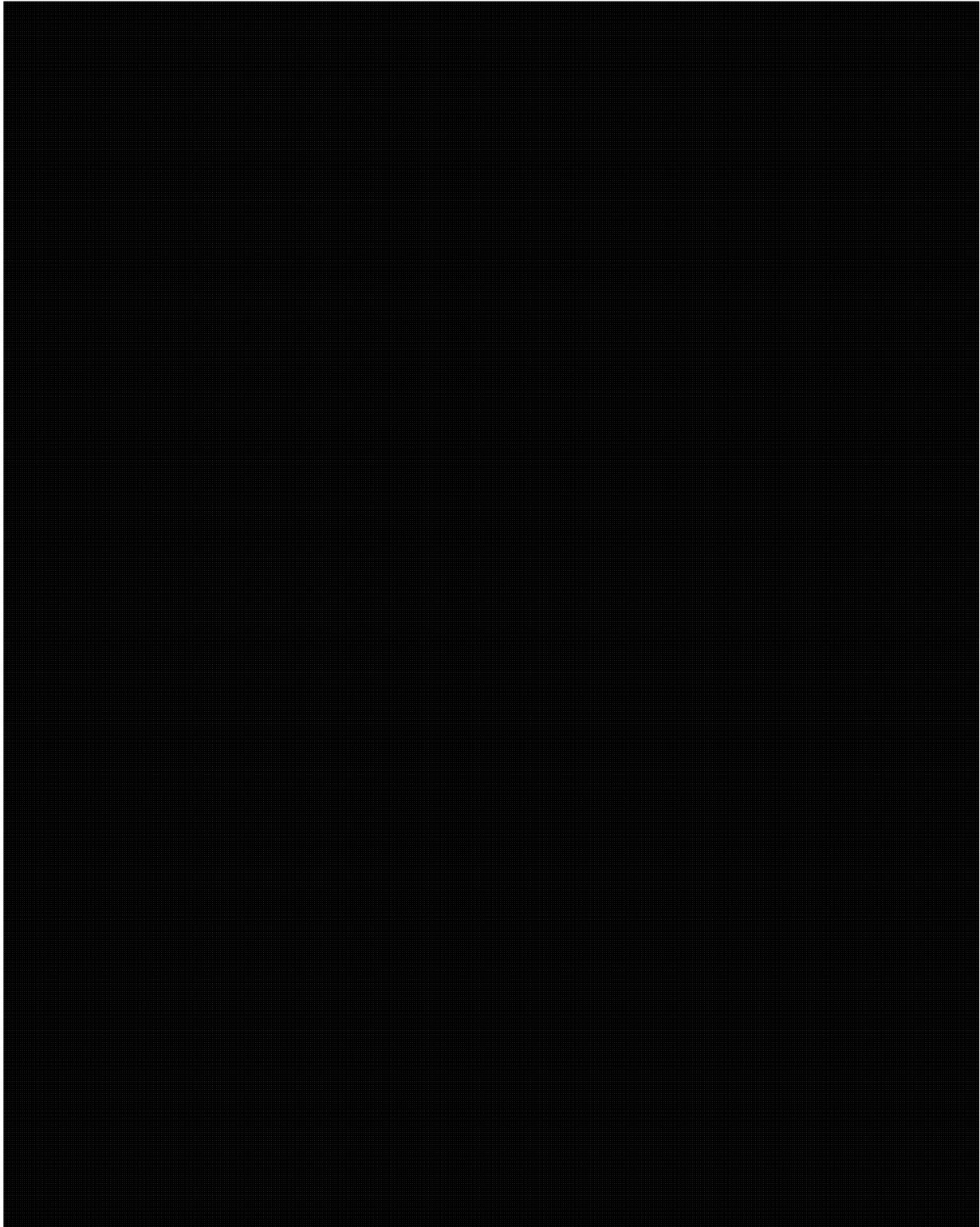
A review conducted by the Office of the CSEC Commissioner examined CSEC's releases of Canadian identities to GC clients over the period of April to September 2010. Results were positive for CSEC, with the Commissioner noting that such activities were conducted lawfully.

In 2010–2011, 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 2009–2010) and [REDACTED] in the number of reports released ([REDACTED] in 2009–2010). 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.

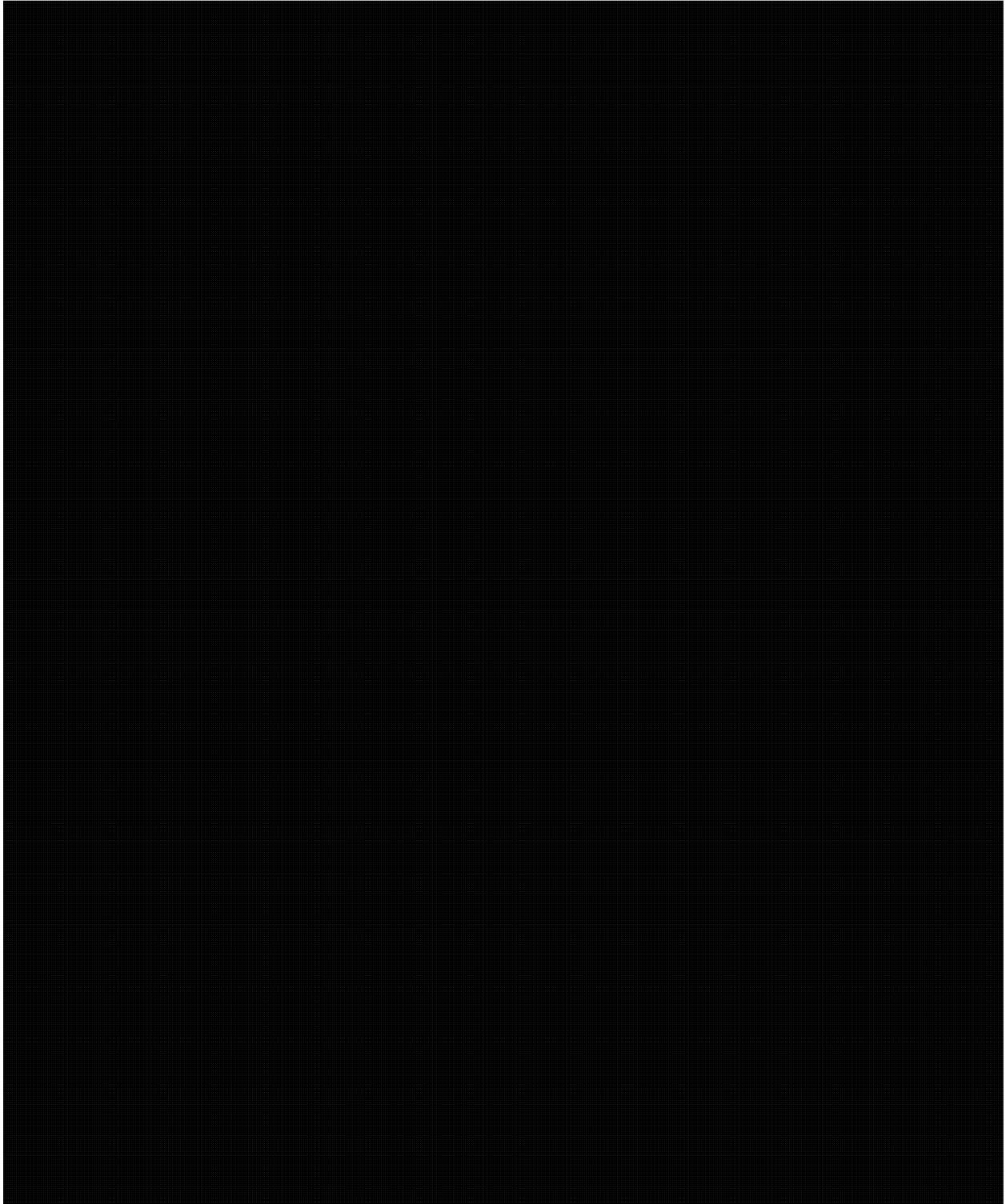
CSEC interaction with the RCMP continued to increase in 2010–2011. [REDACTED]

CSEC made special provision for identity releases [REDACTED] The Chief, CSEC authorized managers under the Director General of Intelligence to release identities to clients in instances where an Operational Policy Advisor was not available within one half-hour. This provision was used only twice, but it was considered to be useful in meeting operational requirement on a timely basis and will likely be considered again in the future.

6. SPECIAL REPORT: [REDACTED]



TOP SECRET//COMINT//CANADIAN EYES ONLY



7. SPECIAL REPORT: INTERNAL SECURITY AND POLYGRAPH TESTING

IRRELEVANT

TOP SECRET//COMINT//CANADIAN EYES ONLY

IRRELEVANT

TOP SECRET//COMINT//CANADIAN EYES ONLY



TOP SECRET//COMINT//CANADIAN EYES ONLY