Parliamentary Review of the *Anti-Terrorism Act*
Special Senate Committee
Chief CSE Appearance – 11 April 2005
Speaking Notes

INTRODUCTION

Madam Chair, Honourable Senators, thank you for inviting me to appear before you today as Chief of the Communications Security Establishment. I welcome this opportunity to talk with you about the impact the *Anti-Terrorism Act* has had on CSE.

Before I begin, I would like to introduce three members of my senior executive management team who are here to assist me.

On my right is Barb Gibbons, who is CSE's Deputy Chief, Corporate Services. Beside me, on my left, is John Ossowski, Director General, Policy and Communications. And beside him, David Akman, who is CSE's Director of Legal Services.

ROLE AND MANDATE OF CSE

Clearly, the brutal terrorist attacks of September 11th 2001 changed forever the way we deal with security issues in North America.

These events were a wake up call for Canada and a turning point for CSE. The *Anti-Terrorism Act* that was proclaimed into law in December 2001

impacted CSE in two important ways: it provided CSE with a legislated mandate and it filled an authority gap that enabled CSE to engage in the war on terrorism.

Under its legislated mandate, CSE engages in three broad areas of activity: collection of foreign intelligence, protection of electronic information, and assistance to federal law enforcement and security agencies.

I would like to take a moment to elaborate more fully on these three elements of CSE's mandate.

First, CSE uses high-technology methods to acquire foreign communications in order to provide the Government of Canada with foreign intelligence. CSE's job is to precisely locate communications that contain valuable foreign intelligence, acquire them, process them to understand the information they contain, and pass that information to the people who need it.

In line with the priorities approved by Cabinet, CSE provides intelligence to hundreds of clients across the federal government. This intelligence helps them to better understand global issues. It informs their decisions. It contributes to the development of our foreign and defence policies. And most importantly, it helps to protect the security of our country and its citizens.

In support of the commitments outlined in the *National Security Policy*, CSE has greatly increased its focus on security issues. CSE now devotes the

majority of its foreign intelligence efforts to gathering and reporting intelligence on issues such as terrorism, proliferation and cyber threats. CSE also supports deployed Canadian Forces operations abroad.

Second, under its IT Security program, CSE provides advice, guidance and services to help ensure the protection of electronic information.

This program is carried out amidst a growing recognition that our country's security and prosperity depend on the security of its most important information. There is also a growing awareness of the very real threat posed by cyber attacks, which are happening on a continuous basis.

In response, CSE analyzes threats and vulnerabilities to determine where protection needs to be strengthened.

We also work with other Government organizations to predict and prevent cyber attacks, and help develop and approve the secure communication systems and devices that protect the Government's most sensitive information.

Consistent with the objectives of the *National Security Policy*, CSE is focusing ever more sharply on helping the Government protect its most critical information and networks.

Third, CSE provides support to federal law enforcement and security agencies. This is a natural extension of CSE's technical expertise in areas like cryptology and IT security.

It is crucial to understand here that, under this third element of our mandate, CSE may provide technical and operational assistance to our federal partners only within the parameters of their own authorities and limitations.

If, for example, CSE provides operational assistance to CSIS under this part of our mandate, we do so under the authority of CSIS, and under its supervision, rules and procedures.

DECLINING EFFECTIVENESS

Let me turn now to the significant legislative gaps in CSE's authority structure that were addressed by the *Anti-Terrorism Act*.

Throughout the 1990s, as CSE moved further away from its Cold War focus, the pace of change in the telecommunications world shifted from evolutionary to revolutionary. New technologies proliferated. The volume, variety and velocity of communications increased exponentially. The routing of messages became unpredictable – "anything could be anywhere" in the new communications landscape.

In this context, however, CSE still had to operate within a legal framework that had been developed to protect the privacy of Canadians in a communications environment very different from, and much less complex than, what exists today.

In this new environment, the absolute prohibition against intercepting "private communications" contained in Part Six of the *Criminal Code* was increasingly scripting CSE out of its basic mission – to collect foreign communications.

To appreciate this impact, it is important to understand that the *Criminal Code* definition of a private communication includes any communication with a reasonable expectation of privacy that originates or terminates in Canada.

This *Criminal Code* provision affected CSE in two ways.

First, it prevented CSE from intercepting communications that an intelligence target abroad sent to or received from Canada. So, for example, CSE could not provide intelligence on a known terrorist group abroad if it was communicating with a member or an accomplice in Canada.

Second, this provision prevented CSE from intercepting any communications that might contain private communications. The difficulty here was that, in this new technological environment where "anything could be anywhere" in virtually endless communications haystacks and electronic highways, it was impossible for CSE to prove, before it acquired a communication, that both ends of the communication would be foreign.

The result was that, as technologies continued to evolve, CSE was increasingly unable to access valuable intelligence sources.

By the time the events of 9/11 took place, all of CSE's key international partners – the US, Britain, Australia and New Zealand – had already found ways to deal with this issue. CSE was being left behind.

With respect to its protection mandate, CSE's ability to protect electronic information and systems was being similarly eroded.

In the new cyber environment, CSE needed to monitor activity on Government of Canada networks, and to sample messages that have characteristics associated with viruses or other malicious code.

Yet the *Criminal Code* prohibition against intercepting private communications also prevented CSE from undertaking these essential protection activities.

As a result, the essential tools of information protection were rapidly moving beyond CSE's reach as well.

ANTI-TERRORISM ACT – IMPACT ON CSE

Nothing could have highlighted more clearly the limits of CSE's authorities than the events of September 11th 2001.

In the aftermath of these events, the CSE provisions in the *Anti-Terrorism Act* were designed to ensure CSE's authorities reflected both the requirements of the new security environment and the realities of modern communications, as well as the obligation to protect the privacy of Canadians.

Specifically, steps were taken to exempt CSE from Part Six of the *Criminal Code* where CSE could demonstrate that it needed this to fulfill its mandate.

The *Act* thus created a mechanism – an authorization by the Minister of National Defence – which allows CSE to intercept private communications when directing its activities against foreign entities located abroad.

I want to be very clear about the activities that the Minister of National Defence may authorize.

Under the legislation, CSE is prohibited from directing its activities against Canadians or anyone within the 12-mile limit that defines Canadian territory. CSE is also prohibited from directing its activities at Canadians abroad, defined in the *Act* as Canadians or permanent residents.

However, under Ministerial authority, when directing its activities at foreign entities abroad, CSE can now conduct operations even if doing so risks acquiring private communications as well. When this occurs, the *Act* allows CSE, in cases where a strict set of conditions is met, to use and retain these communications. Otherwise, upon recognition, they are deleted.

Similarly, CSE may now obtain a Ministerial Authorization to carry out essential IT Security activities that run the risk of intercepting private communications.

In practice, with respect to both foreign intelligence and IT Security, CSE requests Ministerial Authorizations to ensure legal protection against what would otherwise be a *Criminal Code* offence of intercepting private communications that may be

incidentally acquired by CSE in the course of carrying out specific collection and protection activities.

Equally important, such "activities or class of activities", to use the legislative phrase, are only permitted once the Minister is satisfied, following an in-depth review by the Department of Justice, that the specific legislative conditions have been met.

CSE'S EVOLUTION SINCE THE *ANTI-TERRORISM ACT*

I would now like to explain the results CSE has specifically achieved from its new authorities.

Under its foreign intelligence program, Ministerial Authorizations have allowed CSE to significantly increase its ability to identify and collect communications that yield high-value foreign intelligence.

Obviously, I cannot go into detail about CSE's foreign intelligence successes in this public forum. I can say, however, that intelligence provided by CSE has been directly responsible for helping to protect Canadian troops in Afghanistan from terrorist attack. I can also say that CSE has provided intelligence on foreign terrorist targets used to protect the safety and interests of Canadians and our closest allies. This was intelligence that CSE would not have been able to acquire without the *Anti-Terrorism Act*.

Similarly, CSE's IT Security program has used Ministerial Authorizations to ensure that Government of Canada computer systems and networks are better protected from cyber attack.

PROTECTING THE PRIVACY OF CANADIANS

Let me now turn to the critically important measures CSE has in place to protect the privacy of Canadians.

Before providing a Ministerial Authorization, the Minister must be satisfied that, among other things, the interception will not be directed against Canadians or anyone in Canada, and that satisfactory measures are in place to protect the privacy of Canadians.

In this regard, CSE has in place comprehensive procedures to ensure its activities respect the *Charter* right to privacy in letter and spirit. This obligation is taken very seriously by all CSE employees, who receive extensive direction and training in this area.

In addition, CSE has instituted new procedures for activities conducted under Ministerial Authorization to ensure CSE's activities are directed at foreign entities abroad and that they will only be used or retained if they are essential to international affairs, defence or security.

CSE also works closely with an on-site legal team assigned from the Department of Justice to ensure its practices and procedures satisfy all legislated requirements.

As far as external review is concerned, the role of the CSE Commissioner, former Chief Justice of the Supreme Court of Canada the Right Honourable Antonio Lamer, who operates independently, was formalized in the *Anti-Terrorism Act*. The Commissioner has a mandate to review CSE's activities to ensure they are lawful. He has unfettered access to all CSE personnel, information and documentation.

The Commissioner is required by the *Act* to report to the Minister of National Defence annually on his review of CSE's activities. The Minister then tables this report in Parliament. The Commissioner also provides classified reports to the Minister on a regular basis. These focus on specific programs or issues.

Allow me to note here that since the office was established in 1996, the Commissioner has consistently confirmed that all CSE activities reviewed were lawful.

In addition, I note that since the *Anti-Terrorism Act* was enacted, the Office of the Privacy Commissioner has examined CSE's activities conducted under its new mandate. No issues of concern were identified.

CONCLUSION

In short, I believe the authorities granted to CSE under the *Anti-Terrorism Act* provide the right foundation for the organization's activities while protecting the privacy of Canadians.

The *Act* responded to an urgent need to update CSE's authorities, allowing the organization to address new threats and to keep pace with a rapidly changing communications environment.

These new authorities are now absolutely essential to CSE's operations, its ability to successfully overcome formidable technical obstacles, and ultimately its ability to contribute to Canada's security and other national interests.

Indeed, in the current strategic and technological environment, CSE could not function effectively without them.

Three years ago, the Minister of National Defence and I explained to Parliament what CSE needed to help protect the security of Canadians. Parliament had the more difficult task of ensuring the right balance between protecting the privacy rights of Canadians and protecting the nation's security.

In the end, it provided CSE with the critical authorities it needed to be effective in the new strategic and technical environment. And it is my hope that Parliament will continue to support CSE with an authority structure that will allow us to address the very serious national security challenges facing our country.

Thank you. I would be happy to respond to any questions you may have.