19 Sep 2011

ADVICE FOR THE MINISTER

CSEC ISSUES

ISSUE: Why is the government putting national security at risk with the LTA project by hiring contractors to work at CSEC? Why is the government allowing the loss of more than 90 Public Service positions by hiring contractors rather than full-time public servants? Why was Plenary Properties, a foreign-owned Australian company, selected to construct the new facility for Canada's most secret intelligence organization? What is the government doing to ensure that Government of Canada computers and information are protected from cyber-attacks?

IF PRESSED ON IMPACT OF LONG-TERM ACCOMMODATION (LTA) PROJECT ON NATIONAL SECURITY

- **National security is in no way at risk as a result of this project. All CSEC staff, including contractors, are subject to the appropriate security screening process and clearance level.**
- **Any private contractor hired for the new facility who will have access to sensitive information will be designated as a Person Permanently Bound to Secrecy and subject to the *Security of Information Act* in the same manner as CSEC employees.**
- **Contractors have been employed by CSEC for many years. At any given time, there are more than 100 contractors working at CSEC. All contractors have the appropriate security clearances, have sworn the appropriate oaths of secrecy and have signed the appropriate documents to be employed by CSEC.**

IF PRESSED ON IMPACT OF LTA PROJECT ON CSEC EMPLOYEES' JOB SECURITY

- **No CSEC employee will lose employment as a result of this public private partnership.**
- **The Chief of CSEC is fully committed to ensuring that any employee whose job is affected by the move to the new facility four to five years from now is guaranteed another position at CSEC or elsewhere within the federal public service.**
- **In fact, this project will create jobs – approximately 4000 construction jobs will be created as a result of this project.**

IF PRESSED ON PLENARY GROUP (CANADA) AND CANADIAN BUILDER PCL CONSTRUCTION

- **Plenary Group, the Plenary Properties consortium lead, is a Canadian company with offices in Toronto, Vancouver and Edmonton.**
- **Plenary Group has an Australian sister company with industry-leading experience in Australian-based public-private-partnership projects; however, this company is not involved in the project.**
- **Plenary Group has a proven track record of creating Canadian jobs. This project is expected to generate upwards of 4,000 jobs for Canadians, 99 percent of which are expected to be Canadian.**
- **With a project of this size and complexity, it is only reasonable to expect that the consortium would be Canadian-led and multinational in nature.**

IF PRESSED ON CYBER COMPROMISES OF GOVERNMENT OF CANADA COMPUTER SYSTEMS

- **CSEC provides the Government of Canada, departments and agencies advice, guidance and services on the protection of electronic information and infrastructures.**
- **CSEC is recognized as a key partner in Canada's *Cyber Security Strategy*.**
- **While the Government does not comment on the specific operational details of security-related incidents, I can assure you that CSEC continues to work with departments in addressing unauthorized attempts to access their networks.**

IF PRESSED ON OCSEC ANNUAL REPORT, 2010-11

- **As the Communications Security Establishment Commissioner confirmed in his annual report, CSE activities that he examined this past year were all in compliance with the law, ministerial requirements, and CSE policies and procedures.**
- **The Commissioner made a small number of recommendations, and expressed satisfaction that CSEC addressed deficiencies identified in previous annual reports.**

IF PRESSED ON CSEC COLLECTION OF CANADIANS' PERSONAL INFORMATION

- **CSEC does not target the communications of Canadians anywhere and has legislative measures in place for the protection of the privacy of Canadians.**
- **As the CSE Commissioner has noted in his 2010-2011 report, the focus of CSEC activity is foreign intelligence.**
- **The CSE Commissioner highlighted that all reviewed CSEC activities were authorized and carried-out in accordance with the law, ministerial requirements and CSEC's policies and procedures.**
- **In his report, the Commissioner highlights the degree of transparency and cooperation displayed by CSEC, as well as CSEC's genuine concern for protecting the privacy of Canadians.**

BACKGROUND: CSEC ISSUES

- On 6 June 11, media reported that classified information was stolen from two federal government departments during a cyber-attack originating from China in January 2011. The attacks hit Treasury Board, Department of Finance and DND. The breaches, first reported in February, targeted financial records.

PLENARY GROUP CONSORTIUM

- The consortium includes 11 companies, 7 of which are wholly Canadian and 4 are incorporated in Canada.
- Plenary Properties earned the highest score in all sections of the evaluation criteria.
- Plenary Properties received a bond rating of A, the highest grade of any PPP ever awarded in Canada.

CYBER SECURITY

- The Communications Security Establishment Canada has a mandate to provide advice, guidance, and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada.

- In October 2010, the Government released *Canada's Cyber Security Strategy*. The *Strategy* has three pillars:

    - Secure government systems;
    - Partnering to secure vital cyber systems outside the federal government; and,
    - Helping Canadians to be secure online.

- CSEC is a key player in the pillar to Secure Government Systems.

- Budget 2010 included an investment of $90 million over five years to implement the *Strategy*.

- The *Strategy* states that with its unique mandate and knowledge, CSEC will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems.

- The *Strategy* states that Public Safety will coordinate implementation of the Strategy.

OCSEC ANNUAL REPORT 2010-11

- The Commissioner's 2010-2011 Annual Report noted that "when other means have been exhausted, CSEC may use information about Canadians when it has reasonable grounds to believe that using this information may assist in identifying and obtaining foreign intelligence."

- Citing the above, a 29 July 2011 Globe and Mail article referred to CSEC using "information about Canadians… in identifying and obtaining foreign intelligence."

- The story noted these activities were halted and resumed after "major changes."

- The suspension was initiated by the Chief of CSEC, in order to make absolutely certain that the activities in question were compliant with Canadian privacy laws as well as with CSEC's own policies and procedures.

- In consultation with the Department of Justice an internal review determined that these activities were indeed in compliance with the law but it was felt that certain CSEC policies should be clarified. This was done and CSEC resumed these activities.

- As an independent organization, the Office of the Communications Security Establishment Commissioner can review all activities carried out by CSEC for lawfulness, and must review all activities carried out under Ministerial Authorizations.

Responsible Principal(s): CSEC
Contact: Adrian Simpson, Spokesperson, CSEC, 613-949-2218

Sarah Pacey (D Parl A 2-2), 995-8331
19 September 2011

30 Jan 2012

ADVICE FOR THE MINISTER

CSEC ISSUES

ISSUE: Why is the government putting national security at risk with the LTA project by hiring contractors to work at CSEC? Why is the government allowing the loss of more than 90 Public Service positions by hiring contractors rather than full-time public servants? Why was Plenary Properties, a foreign-owned Australian company, selected to construct the new facility for Canada's most secret intelligence organization? What is the government doing to ensure that Government of Canada computers and information are protected from cyber-attacks?

IF PRESSED ON IMPACT OF LONG-TERM ACCOMMODATION (LTA) PROJECT ON NATIONAL SECURITY

- **National security is in no way at risk as a result of this project. All CSEC staff, including contractors, are subject to the appropriate security screening process and clearance level.**
- **Any private contractor hired for the new facility who will have access to sensitive information will be designated as a Person Permanently Bound to Secrecy and subject to the *Security of Information Act* in the same manner as CSEC employees.**
- **Contractors have been employed by CSEC for many years. At any given time, there are more than 100 contractors working at CSEC. All contractors have the appropriate security clearances, have sworn the appropriate oaths of secrecy and have signed the appropriate documents to be employed by CSEC.**

IF PRESSED ON IMPACT OF LTA PROJECT ON CSEC EMPLOYEES' JOB SECURITY

- **No CSEC employee will lose employment as a result of this public private partnership.**
- **The Chief of CSEC is fully committed to ensuring that any employee whose job is affected by the move to the new facility four to five years from now is guaranteed another position at CSEC or elsewhere within the federal public service.**
- **In fact, this project will create jobs – approximately 4000 construction jobs will be created as a result of this project.**

IF PRESSED ON PLENARY GROUP (CANADA) AND CANADIAN BUILDER PCL CONSTRUCTION

- **Plenary Group, the Plenary Properties consortium lead, is a Canadian company with offices in Toronto, Vancouver and Edmonton.**
- **Plenary Group has an Australian sister company with industry-leading experience in Australian-based public-private-partnership projects; however, this company is not involved in the project.**
- **Plenary Group has a proven track record of creating Canadian jobs. This project is expected to generate upwards of 4,000 jobs for Canadians, 99 percent of which are expected to be Canadian.**
- **With a project of this size and complexity, it is only reasonable to expect that the consortium would be Canadian-led and multinational in nature.**

IF PRESSED ON CYBER COMPROMISES OF GOVERNMENT OF CANADA COMPUTER SYSTEMS

- **CSEC provides the Government of Canada, departments and agencies advice, guidance and services on the protection of electronic information and infrastructures.**
- **CSEC is recognized as a key partner in Canada's *Cyber Security Strategy*.**
- **While the Government does not comment on the specific operational details of security-related incidents, I can assure you that CSEC continues to work with departments in addressing unauthorized attempts to access their networks.**

IF PRESSED ON OCSEC ANNUAL REPORT, 2010-11

- **As the Communications Security Establishment Commissioner confirmed in his annual report, CSE activities that he examined this past year were all in compliance with the law, ministerial requirements, and CSE policies and procedures.**
- **The Commissioner made a small number of recommendations, and expressed satisfaction that CSEC addressed deficiencies identified in previous annual reports.**

IF PRESSED ON CSEC COLLECTION OF CANADIANS' PERSONAL INFORMATION

- **CSEC does not target the communications of Canadians anywhere and has legislative measures in place for the protection of the privacy of Canadians.**
- **As the CSE Commissioner has noted in his 2010-2011 report, the focus of CSEC activity is foreign intelligence.**
- **The CSE Commissioner highlighted that all reviewed CSEC activities were authorized and carried-out in accordance with the law, ministerial requirements and CSEC's policies and procedures.**
- **In his report, the Commissioner highlights the degree of transparency and cooperation displayed by CSEC, as well as CSEC's genuine concern for protecting the privacy of Canadians.**

IF PRESSED CSEC'S PLACE IN GOVERNMENT

- **The Communications Security Establishment Canada (CSEC) provides critical foreign signals intelligence and information technology security support to the Government of Canada.**
- **CSEC has doubled in size since its legislative mandate was established in 2001 to address a growing number of security threats to Canada and Canadians.**
- **This administrative realignment maintains the association of CSEC with the National Defence Portfolio and establishes a reporting structure similar to comparable large agencies. There is no impact on the mandate or operations of CSEC.**

BACKGROUND

PLENARY GROUP CONSORTIUM

- The consortium includes 11 companies, 7 of which are wholly Canadian and 4 are incorporated in Canada.
- Plenary Properties earned the highest score in all sections of the evaluation criteria.
- Plenary Properties received a bond rating of A, the highest grade of any PPP ever awarded in Canada.

CYBER SECURITY

- The Communications Security Establishment Canada has a mandate to provide advice, guidance, and services to help ensure the protection of electronic information and information infrastructures of importance to the Government of Canada.

- In October 2010, the Government released *Canada's Cyber Security Strategy*. The *Strategy* has three pillars:

    - Secure government systems;
    - Partnering to secure vital cyber systems outside the federal government; and,
    - Helping Canadians to be secure online.

- CSEC is a key player in the pillar to Secure Government Systems.

- Budget 2010 included an investment of $90 million over five years to implement the *Strategy*.

- The *Strategy* states that with its unique mandate and knowledge, CSEC will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems.

- The *Strategy* states that Public Safety will coordinate implementation of the Strategy.

OCSEC ANNUAL REPORT 2010-11

- The Commissioner's 2010-2011 Annual Report noted that "when other means have been exhausted, CSEC may use information about Canadians when it has reasonable grounds to believe that using this information may assist in identifying and obtaining foreign intelligence."

- Citing the above, a 29 July 2011 Globe and Mail article referred to CSEC using "information about Canadians… in identifying and obtaining foreign intelligence."

- The story noted these activities were halted and resumed after "major changes."

- The suspension was initiated by the Chief of CSEC, in order to make absolutely certain that the activities in question were compliant with Canadian privacy laws as well as with CSEC's own policies and procedures.

- In consultation with the Department of Justice an internal review determined that these activities were indeed in compliance with the law but it was felt that certain CSEC policies should be clarified. This was done and CSEC resumed these activities.

- As an independent organization, the Office of the Communications Security Establishment Commissioner can review all activities carried out by CSEC for lawfulness, and must review all activities carried out under Ministerial Authorizations.

PLACE IN GOVERNMENT

- The CSEC place in government has changed with the security and intelligence posture of the Government of Canada. CSEC was originally established during the Cold War as a branch of the National Research Council. CSEC has been part of the National Defence portfolio since 1975.
- Through the 2001 *Anti-terrorism Act* amendments, the mandate of CSEC was established in legislation. Since that time, the agency has nearly doubled in size to almost two thousand employees.
- Until recently, CSEC reported to the Minister of National Defence through two deputy heads – the National Security Advisor on policy and operations and the Deputy Minister of National Defence on financial and administrative matters.
- Effective 16 November 2011, CSEC will be established as a stand-alone agency reporting directly to the Minister of National Defence with the Chief, CSEC as Deputy Head.

- This change is to be implemented through an Order in Council designating CSEC as a department, for the purposes of the *Financial Administration Act* by being added to Schedule 1.1 as a branch of the federal public administration. This thereby designates the position of Chief as the Deputy Head for CSEC.

This administrative realignment has no impact on the mandate or operations of CSEC. There is also no impact on the role of the CSE Commissioner. The new CSEC reporting structure is similar to that of other large agencies, such as CSIS.

MEDIA BACKGROUND

- On 26 Sep 11, media reported that the Government was warned prior to the cyber compromises of January 2011 that a hacking attempt could possibly occur. According to this reporting, documents obtained by The Canadian Press say the Treasury Board Secretariat and Finance departments were notified of "harmful activity" on 24 Jan by the agency that oversees communications security in Canada.

- On 21 Oct 11, media reported that the Chief of CSEC, Mr. John Adams, is expected to step down from his post in early 2012. Media reported that no replacement has been named at this time.

- On 31 Oct 11, media reported on the relationship between CSE and CSIS. Coverage noted that CSIS works very closely with CSE and that while CSE's intelligence provides CSIS with investigative leads, information collected in the course of CSIS investigations enhances CSE's ability to respond to cyber-threats.

- On 13 Jan 12, media reported that John Forester has been appointed as the new Chief of CSEC.

Responsible Principal(s): CSEC

Contact: Adrian Simpson, Spokesperson, CSEC, 613-949-2218

Sarah Pacey (D Parl A 2-2), 995-8331
30 Jan 2012

27 July, 2011

MEDIA RESPONSE LINES/RÉPONSE AUX MÉDIAS

ISSUE/ENJEU: The Globe & Mail intends to publish a story based on Section 4 of the CSE Commissioner's 2010-2011 Annual Report, which refers to CSEC using "information about Canadians…in identifying and obtaining foreign intelligence."

Media Query/Demande: Produced in anticipation of media queries

Reporter/Journaliste: Colin Freeze/Globe & Mail

Date: 27 July, 2011

Deadline/Échéance: 27 July, 2011

OVERVIEW/APERÇU

CSEC has received a request for comment about the CSE Commissioner's reference in his 2010-2011 Annual Report to the use of "information about Canadians…in identifying and obtaining foreign intelligence."

The reporter has also noted that the Commissioner suggests that these activities were suspended a few years ago for fear of possible privacy violations but have subsequently resumed under "major changes". There was no new ministerial directive.

It is important to note that the CSE Commissioner found that all CSEC activities reviewed were authorized and carried out in accordance with the law, ministerial requirements and CSEC's policies and procedures.

QUESTIONS AND ANSWERS/QUESTIONS ET RÉPONSES

Q1) What sort of "information about Canadians" does CSEC use, and how is it used?

While I cannot comment on specific operational activities, I would point out that the CSE Commissioner highlighted, and I quote "…that CSEC's activities were authorized and carried out in accordance with the law, ministerial requirements and CSEC's policies and procedures."

The suspension was initiated by the Chief of CSEC, in order to make absolutely certain that the activities in question were compliant with Canadian privacy laws as well as with CSEC's own policies and procedures.

In consultation with the Department of Justice an internal review determined that these activities were indeed in compliance with the law but it was felt that certain CSEC policies should be clarified. This was done and CSEC resumed these activities.

As noted in the Report, CSEC is prohibited from directing its activities at Canadians, anyone in Canada or Canadians anywhere in the world.

CSEC is extremely diligent when it comes to the privacy of Canadians, and I think this is clearly demonstrated in the caution we took in this instance by self-regulating our activities, strengthening our policies and procedures when a question arose in-house and by informing the Commissioner that we were doing so.