Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

P.O. Box 9703
Terminal
Ottawa, Canada
K1G 3Z4

C.P. 9703
Terminus
Ottawa, Canada
K1G 3Z4

Our file Notre référence
A-2014-00012

Mr. Colin Freeze
Globe and Mail
444 Front St. West
Toronto, Ontario M5V 2S9

Dear Mr. Freeze:

This is further to your request submitted under the *Access to Information Act* received on April 23, 2014 for:

"Q&A prepared for the Chief in advance of his early February 2014 appearance at a Senate Security Committee"

Enclosed please find all requested records that could be located using the Department's best efforts, within the restraints of the *Act*.

Please be advised that you are entitled to file a complaint with the Office of the Information Commissioner concerning the processing of your request within sixty days of the receipt of this notice. In the event that you decide to avail yourself of this right, your notice of complaint should be addressed to:

Office of the Information Commissioner of Canada
30 Victoria Street
Gatineau, Quebec
K1A 1H3

Should you require any additional information or assistance regarding this request, please contact the CSEC ATIP Unit at (613) 991-8443.

Yours sincerely,

Dominic Rochon
Access to Information and Privacy Coordinator

Enclosure: 87 pages

Canada

Q.1 If your business is foreign intelligence, why would you collect Canadian metadata or look at travellers in Canada?

- Metadata is technical information used to route communications, and not the contents of a communication.

- CSEC cannot and does not single out Canadian metadata for collection. The internet is large and complex, involving 3.5 billion users and 1800 petabytes of information that travel the globe each day, ignoring geographic and national boundaries. This complexity of global communications networks means that Canadian communications are comingled with international communications. In this context it is impossible for CSEC to collect exclusively foreign metadata.
- Metadata is required to ensure our activities are directed at foreign targets outside of Canada. For example, we must be able to use metadata to know when one of our foreign targets may be entering Canada. In which case, we must cease any intelligence coverage and, through intelligence reporting, advice the RCMP and CSIS so they can conduct any further follow-up.
- More importantly, metadata is essential to fulfill our mandate to collect foreign intelligence. CSEC uses metadata analysis techniques, such as those described in the presentation, to develop an understanding of the global networks used by our foreign intelligence targets.
- Foreign terrorist targets actively seek to hide in plain sight, to disguise their communications in the bustle and noise of urban life in order to evade detection
- It is essential for any foreign intelligence agency to be able to better understand the types of networks foreign targets use and how their behaviours might appear on those networks.
- For this reason, metadata is also used to build models to understand how networks operate in order to locate our legitimate foreign intelligence targets outside Canada.
- Without moving into operational specifics, I can state that the model illustrated in the presentation has been used in CSEC's efforts to gather foreign intelligence related to foreign terrorist targets. Within the last 12 month period, I am aware of at least 2 cases where this model has been used to identify foreign terrorist threats affecting Canadian and allied interests.

Q.2 How can you say that Canadians were not tracked?

- If CSEC were to track anyone, as we do with legitimate foreign targets outside Canada:
    - We would need to know who they are;
    - We would need to actively locate and find the individual; and
    - We would need to monitor their movements in real time.

- That was not the purpose or the result of this exercise.
- The goal was to build an analytical model of typical patterns of network activity around a public internet access point, like an airport, so that CSEC could then apply this model for the purpose of gathering foreign intelligence.
- This work involved a snapshot of historical metadata collected from the global internet.
- We did not use this data to identify any individual Canadian or person in Canada.
- The data was only used to paint a picture of the pattern of network use in certain types of facilities with public internet access. This is what you see in the presentation, patterns of dots.

Q.3 How can you say that this activity was legal when the law says you cannot direct your activities at Canadians or persons in Canada?

- CSEC is authorized to acquire information in order to provide foreign intelligence under the *National Defence Act*.
- To fulfill this mandate, CSEC is authorized to collect and analyze metadata from the global information infrastructure.
- We use metadata to understand global communications networks so that we can find our targets in a vast sea of communications. Global communications networks are complex, vast, borderless and rapidly changing, and foreign and Canadian communications are intermingled.
- CSEC collects and analyses metadata, so that we can better understand these networks, and so that we can ensure we are only directing our foreign intelligence activities at foreign targets outside of Canada.
- Foreign intelligence reveals the motivations, intentions and capabilities of our foreign targets. To find our foreign targets, we first need to understand the global network, how it operates, and then how our targets operate on that global network.
- That's what this exercise was about: analyzing a snapshot of historical metadata from the global internet to build an analytical model of typical network activity patterns around a public access point – like an airport.
- We did not use this data to identify any individual Canadian or person in Canada.
- The sole purpose of the model was to better understand what these patterns look like so that we can more effectively and quickly direct our foreign intelligence activities at legitimate foreign targets, such as terrorists and hostage-takers.
- This use of metadata is authorized under the *National Defence Act* and subject to conditions established under a Ministerial Directive. We recognize that metadata may contain information that has a privacy interest and we take strict measures to protect the privacy of Canadians and persons in Canada.

Q.4 How can you assure Canadians that their privacy was not violated through this activity?

- CSEC did not collect the content of any private communications.
- In this case, metadata, which does not include the content of a communication, was analysed for the sole purpose of developing an analytical model of patterns of network communication. This model was developed for application in identifying foreign threats.
- We did not use this data to identify any individual Canadian or person in Canada.
- All of CSEC's activities, including analytic activities involving the use of metadata in this exercise, include measures that protect the privacy of Canadians as well as the privacy of persons in Canada. These include conditions imposed by a Ministerial Directive, and which have been clearly articulated in CSEC policy.
- The independent CSE Commissioner has reviewed out metadata activities multiple times. He has never found CSEC to have acted unlawfully. In fact, he has specifically noted our culture of lawful compliance and genuine concern for protecting the privacy of Canadians.
- We recognize and acknowledge that many of our activities have privacy implications and we take this seriously. For that reason within CSEC there are multiple structures in place to ensure the privacy of Canadians is strictly protected. These include:
    - Active **monitoring of internal processes** and an internal audit and evaluation function;
    - A dedicated group of CSEC personnel focused exclusively on the development and implementation of operational policies and procedures, as well as embedded **policy compliance teams** in our operational areas;
    - **Executive control and oversight;**
    - An on-site **legal team** of 8 lawyers from the Department of Justice that works closely to provide independent legal advice to CSEC staff; and
    - **External review** by the CSE Commissioner as well as the Privacy Commissioner.

If pressed on how the personal information was protected

- While metadata is largely used to manage and route communications, we recognise that metadata may contain information that has a privacy interest.
- Under the *National Defence Act* and consistent with our other legal obligations CSEC must take steps to protect the privacy of Canadians and persons in Canada in its use and retention of information. This includes not only private communications but other information that has a privacy interest

- We do this through concrete steps such as implementing strict controls on the use, retention, sharing and access to this information.
- The multiple structures we have in place for process monitoring, policy compliance, executive control, legal advice and external review ensure that these measures to protect privacy are followed.
- The CSE Commissioner reviews our measures to protect privacy in every single review he undertakes.

Q.5 Who approved this operation?

- Let me clarify that this was not an operation.
- This was an exercise using a snapshot of historical metadata to build a mathematical, analytical model. It was not subject to ministerial approval.
- CSEC's use of metadata is authorized under the *National Defence Act* and is subject to conditions set out in a Ministerial Directive that was signed in 2011.
- The independent CSE Commissioner regularly reviews CSEC activities, including our activities involving metadata.

Q.6 I hear that CSEC conducted this activity as a trial run for the NSA and other international partners?

- CSEC conducts its foreign intelligence activities in accordance with intelligence priorities set by the Government of Canada.
- CSEC did not conduct this activity on behalf of the NSA or any other partner agency. This was a CSEC effort to develop a mathematical analytic model that can refine CSEC's understanding of communication networks and identify foreign targets.
- While we work closely with our allies to address threats that affect our common interests, no foreign partner can ask another to do something it cannot legally do itself.
- CSEC does not take direction from any outside organization. We are accountable to the Minister of National Defence, the Government of Canada and Parliament.

Q.7 Is this "trial run" now a fully operational program?

- Contrary to media speculation, the subject of this slide presentation is an analytical model. It does not represent an operational program not is it directed at Canadians. It only illustrates a validation exercise of an analytic technique for application in directing our lawful activities at foreign entities outside Canada, such as foreign terrorist targets.

Q.8 How did you obtain this data about travellers at the airport? Who or what is your "special source"?

- No data was collected through any monitoring of the operations of any airport.
- To provide more specific details than those already released by the press would reveal highly classified techniques and capabilities. Since this could cause further injury to Canada's national security, I am not permitted under the law to disclose any further details.

If pressed on any particular slide detail

- I would be happy to discuss and clarify for the committee the overall nature of the exercise and the analytical model described in the document.
- However, I cannot provide any more specific details that could cause further injury to Canada's national security. That would be contrary to the law.
- While the document has been published, it has been released without proper authorization and still contains highly classified details about techniques and capabilities.

CSE Questions and Answers for Appearances

Table of Contents

I. HOT BUTTON ISSUES

Value of CSE

Q.1 What is the value of CSE?

- Let me emphasize that the **foreign intelligence activities of CSE are critical to the ongoing protection of Canadians and Canadian interests**, specifically against terrorism, human smuggling, foreign espionage, illegal arms proliferation, cyber attacks and attacks on our embassies.
- **CSE's operations have also been critical to support Canadian military operations**, such as our mission in Afghanistan, where they helped protect our armed forces against threats from insurgents.
- Further, **CSE's efforts have revealed plots to attack Canadian and allied personnel overseas before these plans could be executed.**
- **CSE has also uncovered foreign-led efforts to attract, radicalize and train individuals to carry out attacks in Canada.**
- Foreign signals intelligence also is critical to support activities taken to **defend and secure government and other IT infrastructure** from foreign cyber threats which can pose a threat to the financial security of Canadians, the intellectual property of Canadian businesses and the privacy of Canadians.
- Under our cyber protection mandate, **CSE leads the coordination of cyber threat incident response across the government** through our Government of Canada Cyber Threat Evaluation Centre – known as GC CTEC.
- Finally, CSE also supports the efforts of the Government to **protect Canadian critical infrastructure from cyber threats**. CSE shares cyber threat information and mitigation advice with the Canadian Cyber Incident Response Centre – known as the CCIRC – at Public Safety for further dissemination to the private sector.

Q.2 What has been the historic value of foreign intelligence?

- Foreign intelligence in all its facets has for centuries been **crucial to the security of nations**, be it their people, their borders, or their prosperity.

- In **times of war** the value of foreign intelligence is often more obvious. It is used in determining the military capabilities of enemies, locating enemy forces on the field, predicting force movements and plans of attack, and even estimating the resources available to the enemy for sustaining conflict. This was as true in Canada's first signals intelligence efforts in World War Two, from which CSE traces its origins, as it was on the field in Afghanistan, where CSE played a significant role in protecting our troops.
- **Today, we face vastly different threats** to our security than an adversary at war or a Cold War superpower. As a result, intelligence agencies have been expected to rapidly adapt. The use of foreign intelligence in times of peace is increasingly important as **terrorism frequently circumvents our conventional means of protection**. Now more than ever intelligence is indispensable in discovering these **threats to the security of Canada**, which rely on blending in with the everyday to evade detection. At the same time, intelligence agencies in democratic countries like Canada have integrated **ever-improving systems of statutory limits, privacy protection and review**.
- Historically all states have also used foreign intelligence to serve a broad range of national interests. In Canada, **foreign signals intelligence exists to support the Government in the pursuit of its national interests within the scope of defence, security and international affairs**. This includes economic interests because in any state a strong economy is integral to national security. For instance, intelligence on economic matters can provide us early warning of impending international financial crises, or provide insight into terrorist financing.
- However, it should be clearly understood that **Canada's foreign signals intelligence activities are NOT used to provide Canadian private companies with any competitive advantage**. Private businesses, here in Canada or anywhere, should compete fairly in the global marketplace on the merits of their own offerings, without any assistance provided by state intelligence capabilities.

CSE Lawfulness, Review, Accountability and Oversight

Q.3 How does the public know that CSE is lawful?

- A fully independent CSE Commissioner—a series of retired judges, including a former Chief Justice of the Supreme Court and other notable federal court judges—has regularly reviewed CSE activities for compliance with the law and made helpful recommendations to improve CSE programs. The **Commissioner and his staff of eleven full time employees and two external subject-matter experts have full access** to all CSE personnel, systems and documents.
- CSE fully respects the legal parameters and authorities under which it operates. **Under the *National Defence Act*:**
    - CSE is specifically **required to protect the privacy of Canadians** in the execution of its foreign intelligence and IT security activities, which is our most important operational consideration.
    - In its foreign intelligence and cyber protection activities, CSE is **prohibited by law from directing its activities** at Canadians anywhere in the world or at any person in Canada.
    - When CSE provides **assistance** to Canadian federal law enforcement and security agencies it does so **under their lawful authorities**, including any applicable court warrants.
- CSE also adheres to all applicable federal legislation, including the *Canadian Charter of Rights and Freedoms*, the *Privacy Act* and the *Criminal Code of Canada.*
- In his 2012-2013 Annual Report, Commissioner Décary acknowledged the leadership of CSE in its commitment to lawfulness and the protection of the privacy of Canadians. **The Commissioner's 2012-13 report specifically noted that "the protection of the privacy of Canadians is, in the eyes of CSE and its employees, a genuine concern" and lauded CSE's "culture of compliance".**
- To date the Commissioners' review reports have contained **140 recommendations.** CSE has **accepted and addressed 92%** of these recommendations. All recommendations related to privacy have been implemented and CSE is in the process of implementing those from recent reviews.

Q.4 What external review, oversight or parliamentary control exists for CSE?

- **CSE operates under a statutory regime established by Parliament in the *National Defence Act***. CSE is also subject to legislated privacy protections such as the *Charter* and the *Privacy Act.*
- **All CSE activities are subject to review for lawfulness by the independent CSE Commissioner**, whose report is tabled in Parliament on an annual basis and who may be called to appear before parliamentary committee.
- **CSE is subject to access to information and privacy legislation**, is included in the regular financial reporting to Parliament, such as the *Public Accounts* and the parliamentary estimates process, and may be called to appear before parliamentary committee.
- Like many departments, **CSE is subject to external review and audit** by Agents of Parliament (e.g. Auditor General, Privacy Commissioner, and Information Commissioner). As a stand-alone agency, CSE has also established a Departmental Audit Committee composed of external members as required under Treasury Board policy.

Q.5 How can one person effectively monitor all your agency's activities?

- The CSE Commissioner's office has a staff of **eleven full time employees and two external subject-matter experts**. This is comparable to other government oversight and review bodies, given the Commissioner's mandate and the size of CSE.
- **Unlike many other government oversight and review bodies, the CSE Commissioner is focussed solely and squarely on the review of one organization: CSE. In fact, the Commissioner's equivalent in Australia reviews six agencies with the same number of staff.**
- **As Commissioner Plouffe testified in December, he feels that the resource levels of his office are sufficient to carry out his mandate.**
- **The Commissioner and his staff** may review all aspects of CSE activities for lawfulness. They **have full access** to CSE facilities, databases and staff at all stages of review.
- While their main office is off-site, the Commissioner's staff have office space within CSE buildings and are supported in their review efforts by a dedicated team of CSE employees who extend every effort to ensure the Commissioner's staff have timely access to complete information.
- I would also note that the position of **CSE Commissioner** has some of the most exacting qualifications of any federal oversight body. As **a supernumerary or**

retired judge of a federal or superior court, the CSE Commissioner has the legal experience and acumen necessary to fully assess the lawfulness of CSE's activities. In fact **one of our past Commissioners was a retired Chief Justice of the Supreme Court of Canada.**

- I can speak from experience that former Commissioner Robert Décary directed his staff with extreme diligence in the conduct of in-depth reviews during his time in office. He worked to increase the level of detail and clarity in his annual public report and was always available to be called before Parliament.
- **I look forward to continue working with the new Commissioner, Jean-Pierre Plouffe**, and as always will place the highest priority on my agency's continued cooperation with his office as they work to fulfill the important role of assuring the Minister, parliamentarians and Canadians that CSE continues to act lawfully.

Q.6 How do OCSEC and SIRC compare?

- **Both OCSEC and SIRC are external and independent review bodies which provide reports to Parliament** on the operations of CSE and CSIS respectively, and provide assurance to Parliament that CSE and CSIS respectively are complying with the law, policy, and Ministerial directions. Similarly, both OCSEC and SIRC have the ability to review all activities, documents, and interview the personnel of CSE and CSIS respectively.
- The CSE Commissioner has all the powers of a commissioner under Part II of the Inquiries Act. Each CSE Commissioner has been a **retired or supernumerary judge** of a federal or superior court, providing the position with **the legal experience and acumen necessary to fully assess the lawfulness of CSE's activities.**
- The CSE Commissioner's office has a staff of eleven full-time employees and two external subject-matter experts. This is comparable to other government oversight and review bodies, given the Commissioner's mandate and the size of CSE.
- Comparatively, **SIRC is a committee comprised of three-five Privy Councillors**, who are selected so as to be representative of the three major federal political parties. The committee members are supported by 17 full-time staff.
- **While both OCSEC and SIRC have a public complaints function, SIRC's complaints function has a much higher demand requiring more staff to manage.** SIRC also has a somewhat higher budget which reflects the higher costs they have in travel related to the number of board members and the

regional nature of CSIS operations. All CSE and OCSEC staff are located in the NCR.

Q.7 Commissioner Plouffe mentioned in his last appearance that he is currently working part-time as the Commissioner. Can you clarify the time commitment of the CSE Commissioner and how it compares to other review bodies?

- While I believe that this question would be best answered by the Commissioner himself, I can provide you with my view.
    - Based on my numerous interactions with the Commissioner today, I certainly believe that **he is fully engaged and applying his vast legal experience and acumen as a judge to his role as Commissioner.**
    - Additionally, I know that the staff he directs are engaged full time in the review of CSE activities, with almost a dozen ongoing reviews at this very time.

Q.8 What do you think of the creation of a parliamentary oversight committee for the review of CSE's operations?

- It is the **purview of the Government and Parliament** to establish any further legislative or other measures with respect to review or oversight.
- One of our great challenges is that CSE has been a largely unknown organization for decades. To meet this challenge we are committed to becoming more transparent within the confines of national security. We believe that transparency is crucial to ensuring that there is public trust in what we do.
- I can say that CSE is **currently subject to a robust review regime** led by the independent CSE Commissioner, a supernumerary or retired federal judge. The Commissioner's report is tabled in Parliament on an annual basis and he may be called to appear before parliamentary committee. I should note that the Commissioner and his staff **focus squarely on the activities of CSE**, unlike other bodies such as the Office of the Auditor General, which can examine over 100 Government of Canada organizations. The **Commissioner and his staff also have full access** to all CSE information holdings, systems and staff.
- CSE operates under a statutory regime established by Parliament in the *National Defence Act*, and **adheres to all applicable federal legislation, including the *Privacy Act***. In the pursuit of fulfilling our mandates, CSE's internal policies adhere to the legal framework of its legislation and Canadian law.

- CSE is **subject to access to information and privacy legislation**, is included in the **regular financial reporting to Parliament**, such as the *Public Accounts* and the parliamentary estimates process, and our **officials may be called to appear before parliamentary committee**.
- **CSE is additionally subject to external review and audit** by Agents of Parliament such as the Auditor General and the Privacy Commissioner. We also may be called upon to appear before commissions of inquiry, such as the Air India Inquiry.

Q.9 What do you think of the proposals for joint reviews among domestic intelligence review bodies, or a structure that would put all intelligence review bodies under one umbrella?

- We strongly believe that due to the highly technical and specialized nature of CSE's work, as well as that of our domestic partners, that the review bodies of the Canadian security and intelligence agencies need to reflect that specialization.
- In his 2012-2013 Annual Report the **CSE Commissioner stated that he believed some collaboration among review bodies is "possible under existing legislation,"** and recommended that if any legislative change is made it should encourage and authorize cooperation.
- In his most recent appearance before this Senate Committee, Commissioner Plouffe noted several ways in which his office has shared information with SIRC.
- Reflecting on the idea of an over-arching structure that would group review bodies under a single umbrella, as proposed by the Arar Commission of Inquiry, the CSE Commissioner has stated that before creating a "super-bureaucracy" – with its associated burden and costs – existing review bodies should be optimized and their collaboration should be further facilitated.
- Furthermore, **Justice O'Connor who led the Arar Inquiry** stated in that same report that **"the Office of the CSE Commissioner functions very well and that [he] sees no reason to interfere with that operation."**
- CSE is supportive of the previous Commissioner's position and would always act in support of any Government of Canada effort to optimize cooperation between existing security and intelligence review bodies in order to maintain the confidence of Canadians in the diligence and lawfulness of our activities.

Q.10 What do you think about the Privacy Commissioner's recommendations for increasing CSE's reporting requirements, including tabling an annual report in Parliament?

- It is the **purview of the Government and Parliament** to establish any further legislative or other measures with respect to accountability.
- CSE does produce **an annual classified report for the Minister** that is shared with the CSE Commissioner.
- Currently, the **independent CSE Commissioner** can review all activities carried out by CSE and provides a public report to Parliament annually.
- **CSE also appears in the Public Accounts** and the **parliamentary estimates** process. CSE is also subject to external audit and review by the Auditor General, the Privacy Commissioner, the Information Commissioner and Commissions of Inquiry.
- As a note, **CSIS *voluntarily* produces a useful public annual report** on the threat environment. It is not a legislated requirement.

Unauthorized Disclosure of the Metadata Deck

Q.11 What were you doing in the project described in this deck?

- This was not and is not an operational surveillance program. The purpose was to build an analytical model of typical patterns of network activity around a public internet access point, like an airport – which is what you see in the document: patterns of dots.
- This work relied on metadata. Metadata is data about a communication, not the contents of a communication itself. It is used by computers to manage or route communications over global networks. This was the data we were using in this exercise.
- This exercise involved using a snapshot of historical metadata collected from the global internet. No data was collected through any monitoring of the operations at any airport.
- The goal was to build a mathematical, analytical model. The end result of this work was formulas, algorithms, software. The reason we did this was to develop a model to help us find legitimate foreign targets – terrorists, hostage takers, foreign intelligence agents – in a sea of billions and billions of communications.

Q.12 How was the data that was collected used?

- The collection and use of metadata to analyze and understand the global internet is authorized under the *National Defence Act*. This work was conducted under conditions set out in a Ministerial Directive on metadata.
- The data was used to build an analytical model of typical patterns of network activity around a public internet access point, like an airport.
- This analytical model can help us in two ways:
    - It helps us to narrow our search in a foreign remote region or large city – filtering from millions of possibilities to a few.
    - Terrorists or hostage takers will often use public places to access the internet because they are trying to hide in plain sight. This model, which helped to identify typical patterns, helps us to identify where that contact may be coming from – a café, a hotel, an airport.
- Further, this model can save time and work during an incident where time is critical. It increases our chance of success. I am aware of at least 2 cases where this model has been used in the past year to help identify foreign terrorist threats.

- No Canadians' private communications were targeted, collected or used. We did not use this data to identify any individual Canadian or person in Canada. As with all of our activities, measures were in place and applied to protect the privacy of Canadians.

Q.13 How does this model apply to your mandate?

- CSE's role is to collect information on legitimate foreign targets from the global information infrastructure – the Internet. To do this, we need to understand how the millions of communications networks that comprise it function, how they change (which is constant), and how foreign targets make use of them.
- The collection and use of metadata to analyze and understand the global internet is authorized under the National Defence Act. This work was conducted under conditions set out in a Ministerial Directive on metadata. The first Ministerial Directive, which included this kind of network analysis, was signed in 2005. A new Ministerial Directive was submitted by my predecessor and signed by the Minister in 2011. This work was done under the conditions set out in those directives.
- Our collection and use of metadata, including network analysis, has been reviewed by successive Commissioners five times since 2003, the most recent in 2011, and were found to be lawful. The Commissioner has approved in 2012 a new review of metadata. Metadata is the kind of topic that the Commissioner regularly looks at and we are happy to cooperate with him in that review.
-

Q.14 If your business is foreign intelligence, why would you collect Canadian metadata or look at travellers in Canada?

- Metadata is technical information used to route communications, and not the contents of a communication.
- CSE cannot and does not single out Canadian metadata for collection. The internet is large and complex, involving 3.5 billion users and 1800 petabytes of information that travel the globe each day, ignoring geographic and national boundaries. This complexity of global communications networks means that Canadian communications are comingled with international communications. In this context it is impossible for CSE to collect exclusively foreign metadata.
- Metadata is required to ensure our activities are directed at foreign targets outside of Canada. For example, we must be able to use metadata to know when one of our foreign targets may be entering Canada. In which case, we must

cease any intelligence coverage and, through intelligence reporting, advice the RCMP and CSIS so they can conduct any further follow-up.

- More importantly, metadata is essential to fulfill our mandate to collect foreign intelligence. CSE uses metadata analysis techniques, such as those described in the presentation, to develop an understanding of the global networks used by our foreign intelligence targets.
- Foreign terrorist targets actively seek to hide in plain sight, to disguise their communications in the bustle and noise of urban life in order to evade detection
- It is essential for any foreign intelligence agency to be able to better understand the types of networks foreign targets use and how their behaviours might appear on those networks.
- For this reason, metadata is also used to build models to understand how networks operate in order to locate our legitimate foreign intelligence targets outside Canada.
- Without moving into operational specifics, I can state that the model illustrated in the presentation has been used in CSE's efforts to gather foreign intelligence related to foreign terrorist targets. Within the last 12 month period, I am aware of at least 2 cases where this model has been used to identify foreign terrorist threats affecting Canadian and allied interests.

Q.15 Why did you develop this model in Canada? Why not an airport in another country?

- In order to fulfill our mandate on the collection of foreign signals in accordance with government intelligence priorities, we need to understand where our foreign targets are and how they communicate on global networks. In order to understand the global network, and in particular foreign networks, we develop models. These models enable us to conduct network analysis, for which we require the use of metadata.
- This analysis took a snapshot of routine global metadata and then was used to develop algorithms to capture the patterns of public access behaviours on the Internet. This enables us to understand how networks operate outside of Canada in order to locate our legitimate foreign intelligence targets, also outside Canada.
- The development of this model was done using a data set that we had collected, as authorized under the law, from the global Internet.
- In order to develop an accurate and complete model we needed a thorough understanding of the network of a public area. We used information from a geographic location where we had a good understanding of the local context.

- This way, when we use the model in a foreign country, where we know little about the conditions, we can be confident that we have been able to validate the model properly, and ensure that it is robust and reliable.
-

Q.16 How can you say that Canadians were not tracked?

- The independent CSE Commissioner has recently looked into this issue and has publicly noted that this analysis did not involve "mass surveillance" or tracking of Canadians or persons in Canada. No CSE activity was directed at Canadians or persons in Canada,
- If CSE were to track anyone, as we do with legitimate foreign targets outside Canada:
    - We would need to know who they are;
    - We would need to actively locate and find the individual; and
    - We would need to monitor their movements in real time.
- That was not the purpose or the result of this exercise.
- The goal was to build an analytical model of typical patterns of network activity around a public internet access point, like an airport, so that CSE could then apply this model for the purpose of gathering foreign intelligence.
- This work involved a snapshot of historical metadata collected from the global internet.
- We did not use this data to identify any individual Canadian or person in Canada.
- The data was only used to paint a picture of the pattern of network use in certain types of facilities with public internet access. This is what you see in the presentation, patterns of dots.

Q.17 How can you say that this activity was legal when the law says you cannot direct your activities at Canadians or persons in Canada?

- The independent CSE Commissioner has recently looked into this issue and has publicly noted that this analysis did not involve "mass surveillance" or tracking of Canadians or persons in Canada. No CSE activity was directed at Canadians or persons in Canada,
- CSE is authorized to acquire information in order to provide foreign intelligence under the *National Defence Act*.
- To fulfill this mandate, CSE is authorized to collect and analyze metadata from the global information infrastructure.
- We use metadata to understand global communications networks so that we can find our targets in a vast sea of communications, and direct our activities at these

legitimate foreign intelligence targets outside Canada in order to better understand their capabilities and intentions.

- These communications networks are complex, vast, borderless and rapidly changing, and foreign and Canadian communications are intermingled.
- As a result, CSE collects and analyses metadata, so that we can better understand these networks, and so that we can ensure we are only directing our foreign intelligence activities at foreign targets outside of Canada
- That's what this exercise was: analyzing a snapshot of historical metadata from the global internet to build an analytical model of typical network activity patterns around a public access point – like an airport.
- The purpose of the model was solely to better understand what these patterns look like so that we can more effectively and quickly direct our foreign intelligence activities at legitimate foreign targets, such as terrorists and hostage-takers.
- This use of metadata is authorized under the *National Defence Act* and subject to conditions established under a Ministerial Directive. We recognize that metadata may contain information that has a privacy interest and we take strict measures to protect the privacy of Canadians and persons in Canada.

Q.18 How can you assure Canadians that their privacy was not violated through this activity?

- The independent CSE Commissioner has recently looked into this issue and has publicly noted that this analysis did not involve "mass surveillance" or tracking of Canadians or persons in Canada. No CSE activity was directed at Canadians or persons in Canada,
- CSE did not collect the content of any private communications.
- In this case, metadata, which does not include the content of a communication, was analysed for the sole purpose of developing an analytical model of patterns of network communication. This model was developed for application in identifying foreign threats.
- We did not use this data to identify any individual Canadian or person in Canada.
- All of CSE's activities, including analytic activities involving the use of metadata in this exercise, include measures that protect the privacy of Canadians as well as the privacy of persons in Canada. These include conditions imposed by a Ministerial Directive, and which have been clearly articulated in CSE policy.
- The independent CSE Commissioner has reviewed out metadata activities multiple times. He has never found CSE to have acted unlawfully. In fact, he has specifically noted our culture of lawful compliance and genuine concern for protecting the privacy of Canadians.

- We recognize and acknowledge that many of our activities have privacy implications and we take this seriously. For that reason within CSE there are multiple structures in place to ensure the privacy of Canadians is strictly protected. These include:
    - Active **monitoring of internal processes** and an internal audit and evaluation function;
    - A dedicated group of CSE personnel focused exclusively on the development and implementation of operational policies and procedures, as well as embedded **policy compliance teams** in our operational areas;
    - **Executive control and oversight;**
    - An on-site **legal team** of 8 lawyers from the Department of Justice that works closely to provide independent legal advice to CSE staff; and
    - **External review** by the CSE Commissioner as well as the Privacy Commissioner.

If pressed on how the personal information was protected

- While metadata is largely used to manage and route communications, we recognise that metadata may contain information that has a privacy interest.
- Under the *National Defence Act* and consistent with our other legal obligations CSE must take steps to protect the privacy of Canadians and persons in Canada in its use and retention of information. This includes not only private communications but other information that has a privacy interest
- We do this through concrete steps such as implementing strict controls on the use, retention, sharing and access to this information.
- The multiple structures we have in place for process monitoring, policy compliance, executive control, legal advice and external review ensure that these measures to protect privacy are followed.
- The CSE Commissioner reviews our measures to protect privacy in every single review he undertakes.

Q.19 Who approved this operation?

- Let me clarify that this was not an operation.
- This was an exercise using a snapshot of historical metadata to build a mathematical, analytical model. It was not subject to ministerial approval.
- CSE's use of metadata is authorized under the *National Defence Act* and is subject to conditions set out in a Ministerial Directive that was signed in 2011.

- I am also required to report to the Minister of National Defence on an annual basis, including providing him with a report on private communications that CSE has incidentally intercepted, and how they were used and disposed. The independent CSE Commissioner regularly reviews CSE activities, including our activities involving metadata.

Q.20 I hear that CSE conducted this activity as a trial run for the NSA and other international partners?

- CSE conducts its foreign intelligence activities in accordance with intelligence priorities set by the Government of Canada.
- CSE did not conduct this activity on behalf of the NSA or any other partner agency. This was a CSE effort to develop a mathematical analytic model that can refine CSE's understanding of communication networks and identify foreign targets.
- While we work closely with our allies to address threats that affect our common interests, no foreign partner can ask another to do something it cannot legally do itself.
- CSE does not take direction from any outside organization. We are accountable to the Minister of National Defence, the Government of Canada and Parliament.

Q.21 Is this "trial run" now a fully operational program?

- Contrary to media speculation, the subject of this slide presentation is an analytical model. It does not represent an operational program. It only illustrates a validation exercise of an analytic technique for application in directing our lawful activities at foreign entities outside Canada, such as foreign terrorist targets.
- The independent CSE Commissioner has looked into this activity and issued a public confirmation that no activity was directed at Canadians or persons in Canada.

Q.22 How did you obtain this data about travellers at the airport? Who or what is your "special source"?

- No data was collected through any monitoring of the operations of any airport.
- To provide more specific details than those already released by the press would reveal highly classified techniques and capabilities. Since this could cause further injury to Canada's national security, I am not permitted under the law to disclose any further details.

If pressed on any particular slide detail

- I would be happy to discuss and clarify for the committee the overall nature of the exercise and the analytical model described in the document.

- However, I cannot provide any more specific details that could cause further injury to Canada's national security. That would be contrary to the law.
- While the document has been published, it has been released without proper authorization and still contains highly classified details about techniques and capabilities.

Metadata

Q.23 What is metadata?

- Metadata is **technical and descriptive information** associated with a communication that is **used to identify, manage or route communications**, and the means by which it was transmitted.
- Metadata **does not include any content** of a communication or any information or part of information that could reveal the content of a communication.
- As **an analogy**, when **a digital camera takes a photograph, many pieces of information, or metadata,** that are associated with, but not part of the actual photograph, are recorded.
    - This includes information such as: **the date and time** the photo was taken, image resolution, size of the file, the make of the camera taking the photo, the type of lens used, the location, the shutter speed setting and flash use. This type of metadata provides useful information about a photograph, but does not in any way include the actual subject of the photograph.

Q.24 If CSE is a foreign intelligence agency, why would CSE collect Canadian metadata?

- CSE is prohibited by law from directing its foreign intelligence activities at Canadians anywhere in the world or at any person in Canada. **CSE targets only foreign entities outside Canada** unless assisting law enforcement or security agencies under their lawful authorities, such as any applicable court warrants.
- The technical information in metadata helps CSE **ensure we are not targeting Canadians, by distinguishing foreign communications from those of Canadians**. This data also assists us in our efforts to better **understand the increasingly complex global information infrastructure and to identify foreign cyber threats**.
- Given the interconnectedness of telecommunications networks and systems, and the dynamic nature of global communications routing, Canadian and international metadata are often co-mingled within the same circuits. Thus when we collect information under our lawful mandate we have no way of knowing what is foreign and what is Canadian until we look at the metadata.
- Basically, by looking at metadata you know much more about what the territory looks like, so when you go looking for foreign intelligence you can do so with

greater discretion and precision, avoiding the communications of Canadians whenever possible and protecting the privacy of that information.

Q.25 How does CSE use metadata?

- Metadata, which never includes the content of a communication, is needed to ensure that CSE is not targeting Canadian communications. **It allows CSE to identify foreign communications of relevance to Government of Canada intelligence priorities.**
- CSE uses metadata to better **understand the increasingly complex global information infrastructure** from which foreign communications are collected in order to better fulfill its mandate and direct its foreign intelligence activities.
- Metadata can also be used to detect malicious cyber-activity and helps protect information and networks of importance to the Government of Canada.
- In its use of metadata **CSE applies measures to protect the privacy of Canadians**, as verified by the independent CSE Commissioner and his staff. Metadata does not include any content of a communication.

Q.26 What is the scope and scale of CSE's metadata collection?

- Metadata is critical to CSE operations.
- CSE collects metadata as necessary to deliver on our mandates, including metadata required to understand global networks, to find our foreign targets, and to detect cyber threats,
- Metadata helps ensure that CSE is directing its foreign intelligence activities at foreign targets located outside Canada, and not Canadians or anyone in Canada.
- Metadata is also used to protect information infrastructures of importance to the Government.

If pressed:

- CSE cannot provide details on the volume or types of metadata collected as that would reveal capabilities, methods and techniques which, under the *Security of Information Act*, we are prohibited from doing.

Q.27 How long does CSE retain metadata that it collects?

- To help ensure the protection of privacy, **CSE has strict operational policies dictating limits on the retention of metadata**. Given the quantity of information transiting cyberspace daily, this technical data is frequently overwritten prior to the end of its retention period.

Q.28 Are there Ministerial Directives related to metadata?

- Since 2005, a **Ministerial Directive** has been in place that **outlines the obligations of CSE with respect to the collection and use of metadata** for its foreign intelligence program.
- The Minister's direction also includes strict measures to protect the privacy of Canadians.

Q.29 Why was the 2005 Ministerial Directive on Metadata needed?

- Prior to 2005, metadata analysis was being conducted under another Ministerial Directive that applied to broader activities. As communication technologies evolved, the Minister issued more specific direction to CSE, in the form of a separate Ministerial Directive on metadata.
- **The 2005 Directive clearly defines metadata and specifies that metadata collection and use must protect the privacy of Canadians** or any other expectation or condition that the Minister may wish to impose.

Q.30 What did revisions to the 2011 Ministerial Directive on metadata address?

- **The 2011 Ministerial Directive on metadata** updated and replaced the 2005 Directive to **reflect changes in the current security threat environment.** The strict provisions to protect the privacy of Canadians from the 2005 Directive were retained.
- **Ministerial Directives do not grant CSE any new powers or authorities, nor are they used to circumvent the law.** Ministerial Directives serve to provide guidance and parameters for our operations, as well as reporting requirements.

Q.31 What did the CSE Commissioner say about CSE's metadata activities?

- **In 2008**, then-Commissioner Gonthier recommended that **CSE review the authorities under which metadata had been analysed.**
- Based on this recommendation, the Chief of CSE at that time **voluntarily suspended the specific analytical activity** in question and CSE updated its operational policy and practices accordingly.
- Following another in-depth review of these activities, former CSE Commissioner Robert Décary has stated that CSE has addressed previous findings and recommendations related to metadata.

- In his **2011 annual report** to Parliament, Commissioner Décary found that **CSE's activities related to metadata "were authorized and carried out in accordance with the law, ministerial requirements and CSE's policies."**
- He also found that **sufficient measures were in place to protect the privacy of Canadians** and lauded CSE's culture of compliance with the law.

If pressed on Commissioner's reference to continuing review from Dec. 9/13

- I think it is quite reasonable that the Commissioner continues to look at this important issue so that Canadians feel certain that our activities are lawful.
- As always, CSE looks forward to any recommendations the Commissioner may have that could further improve our mechanisms to protect the privacy of Canadians.

Q.32 What is the legal basis for CSE's collection of metadata?

- CSE acquires and analyses Metadata pursuant to its mandate as set out in the *National Defence Act.* It is subject to all of the restrictions of the Act, including the restrictions on directing activities at Canadians or any person in Canada and the requirement to have measures in place to protect the privacy of Canadians.
- A communication that originates or terminates in Canada in which the originator has a reasonable expectation of privacy is considered a private communication. **The interception of these private communications is prohibited under Part VI of the *Criminal Code*.**
- Metadata is information about a communication that is used to manage or route communications on a global network .It does not include the content of the communication.
- Nevertheless, CSE recognizes that there are still privacy considerations related to metadata, so any metadata related activities are subject to applicable Ministerial directives and various other policies and procedures put in place to provide comprehensive protection for the privacy of Canadians and persons in Canada.

Other Unauthorized Disclosures of CSE Information

Q.33 IF ASKED TO CONFIRM OR DENY ANY SPECIFIC OPERATIONAL ACTIVITY OR DETAIL IN PUBLISHED DOCUMENTS

- It would be inappropriate to comment on the classified activities or capabilities of Canada or our allies (e.g. targets, capabilities, operations or methods)
- I want to emphasize that **CSE's foreign intelligence activities are lawful, are not directed at Canadians or persons in Canada and are essential to Canada's national security interests.**

Q.34 How have the unauthorized disclosures affected the operations of CSE?

- It is reasonable for one to expect that continuation of the disclosures of specific aspects of intelligence capabilities of CSE or our allies could have a cumulative detrimental effect on our operations.
- **CSE has observed our foreign targets discussing changes to their communications security** as a result of the disclosures. Canada's allied partners have also publically stated that they have observed terrorist groups and other threat actors changing their methods of communications in an effort to hide their planning efforts from intelligence gathering capabilities that were revealed through the unauthorized disclosures.
- CSE is challenged by the complexities of our target environment and the rapid pace of change in telecommunications technology.
- Our **success** is hard won and **is dependent on our targets being unaware of the methods and technologies that we use against them.**
- It stands to reason that the recent unauthorized disclosures have diminished the advantage we may have had, both in the short term but more worryingly in the long term.

Q.35 Has CSE been conducting industrial espionage on behalf of Canadian companies?

- **CSE does not share foreign intelligence with Canadian companies for their commercial advantage.**
- **I can state with confidence that all of CSE's foreign intelligence activities are lawful.**

- All of CSE's activities are reviewed by the independent **CSE Commissioner, who has never found CSE to have acted unlawfully. In fact, he has specifically noted our culture of lawful compliance** and genuine concern for protecting the privacy of Canadians.
- CSE's participation in briefings to critical infrastructure sectors is always in our cyber protection role to help pass on threat information to protect Canada's critical infrastructure from cyber intrusions.
- We do not comment on specific foreign intelligence collection activities or capabilities.

Q.36 What was CSE's involvement in the NSA's surveillance at the 2010 G20 Summit?

- We do not comment on the operations or capabilities of Canada or our allies.
- **CSE cannot ask our international partners to act in a way that circumvents Canadian laws nor can we do anything that would allow a foreign partner to circumvent Canadian laws.**
- All of CSE's activities are reviewed by the independent **CSE Commissioner, who has never found CSE to have acted unlawfully. In fact, he has specifically noted our culture of lawful compliance** and genuine concern for protecting the privacy of Canadians.

Q.37 Why is CSE targeting friendly nations like Brazil?

- I cannot comment on specific intelligence collection activities or capabilities.
- Foreign intelligence is defined in the *National Defence Act* and includes information or intelligence about the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group, as they relate to international affairs, defence or security.
- **CSE is mandated through legislation to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence.** By law, **all CSE foreign intelligence activities must be in accordance with Government of Canada intelligence priorities.**
- Given the classified nature of the activities that CSE undertakes as part of its foreign intelligence mandate, **I cannot comment on our methods, operations or capabilities.** For me to do so would risk a violation of the *Security of Information Act* and would undermine CSE's ability to carry out its mandate.

Q.38 Does CSE have a STATEROOM program that uses diplomatic facilities to conduct foreign intelligence as noted in released documents?

- **I cannot comment on our methods, operations or capabilities.** This would be contrary to the *Security of Information Act* and could unintentionally provide an advantage to foreign terrorists or other threat actors.
- I can confirm that all CSE's foreign intelligence activities are lawful, are not directed at Canadians or persons in Canada, and are in line with Government of Canada intelligence priorities.

Q.39 Can you comment on President Obama's recommendations for policy changes related to NSA operations?

- While CSE works closely with our allies, including the United States, **each country has their own capabilities and programs and each country's agency operates within its own laws and policies.** Also, one country cannot ask a partner agency to do something that it cannot legally do itself.
- The measures announced by President Obama are primarily focused on enhancing the checks and balances related to the activities of the US National Security Agency (NSA). These changes are expected to have a minimal impact on CSE's relationship with the NSA.
- All of CSE's activities are reviewed by the independent **CSE Commissioner, who has never found CSE to have acted unlawfully. In fact, he has specifically noted our culture of lawful compliance** and genuine concern for protecting the privacy of Canadians.

If pressed for our opinion of NSA operations

- It would be inappropriate to comment on the operations or capabilities of our allies.

If pressed on whether CSE will continue to retain metadata

- CSE uses metadata to better **understand the increasingly complex global information infrastructure** from which foreign communications are collected in order to better fulfill its mandate and direct its foreign intelligence activities.
- Metadata can also be used to detect malicious cyber-activity and helps protect information and networks of importance to the Government of Canada.
- CSE strives to maintain a proper balance between security and privacy. **We respect and comply with Canadian law.**

Privacy Protection

Q.40 What kind of measures do you take to protect the privacy of Canadians?

- CSE is **prohibited by law from directing its foreign intelligence or cyber defence activities against Canadians anywhere or any person in Canada.**
- CSE only targets foreign entities outside Canada unless **assisting law enforcement or security agencies under their lawful authority**, such as court warrants.
- Given the complex and global nature of cyberspace and telecommunications, **CSE may**, when targeting foreign entities outside Canada, **incidentally intercept the private communications of Canadians**.
    - As the CSE commissioner stated in his 2012-2013 Annual Report, the proportion of CSE's intercepted communications that are private communications is **very small**, and **CSE destroys most of them**.
- When an incidental interception does occur there are structures in place to ensure the privacy of Canadians is strictly protected. These include:
    - **Executive control and oversight;**
    - A dedicated group of CSE personnel focused exclusively on the development and implementation of operational policies and procedures, as well as embedded **policy compliance teams** in our operational areas;
    - An embedded **legal team** from the Department of Justice that works closely with and provides legal advice to CSE staff;
    - Active **monitoring** of internal processes and an internal audit and evaluation function; and
    - **External review** by the CSE Commissioner as well as the Privacy Commissioner.
- There are also **strict measures in place to ensure that the privacy of Canadians is protected.**, such as:
    - **Limits on the use or retention** of private communications, including regular reporting to the Minister of National Defence;
    - Full **adherence to Canadian** law concerning the use and retention of information about Canadians and personal information.

Q.41 What happens if Canadian communications are incidentally collected?

- CSE directs its foreign intelligence activities at foreign entities. **If a foreign intelligence target is communicating with a Canadian, CSE may incidentally acquire that communication, under authorities outlined in the *National Defence Act*.**
- **All foreign intelligence** collected by CSE, including any incidental collection that may relate to a Canadian, **is authorized in law and subject to strict measures for privacy protection.**
- CSE retains information according to the following principles:
    - With respect to **foreign intelligence, information will only be used or retained if it is essential to international affairs, defence or security**.
    - Regarding **IT security**, only information that is **essential to identify, isolate or prevent harm** to Government of Canada networks will be used or retained.
- The CSE Commissioner reviews CSE activities, including the privacy measures applied, and has **consistently publicly reported that these were carried out in accordance with the law**.

Q.42 What happens to any private communications that CSE intercepts?

- **A private communication** that is incidentally intercepted by CSE, despite the fact that we only target foreign entities outside Canada, **will only be used or retained if it meets requirements specified in our legislation**.
    - That is, the private communication must be determined to be essential to foreign intelligence or cyber defence.
    - If CSE retains or uses the private communication, additional measures are taken to protect the privacy of any Canadians involved in the communication.
- The use and retention of any recognized private communication **is reported to the Minister of National Defence** in accordance with the requirements outlined in the applicable Ministerial Authorization.
- The **CSE Commissioner reviews** all CSE activities to ensure that the **privacy** of Canadians **is protected**.
    - As in previous reports, in his **2012-2013** Annual Report, the Commissioner stated that **"CSE retained only those private communications essential to international affairs, defence or security."**

- The most recent annual report of the Commissioner also states that **the office can and does review every one of the small number of private communications** that CSE retains and uses.

Q.43 Given the extent of CSE's assistance to federal law enforcement agencies, why doesn't CSE publish more information about these requests, as recommended in the Privacy Commissioner's 2014 report, to assure Canadians that their privacy rights are protected?

- We welcome the recommendations of the Privacy Commissioner, and have taken them into consideration. CSE does produce **an annual classified report for the Minister,** which includes this information. This report is shared with the CSE Commissioner.
- **All CSE technical and operational assistance is undertaken in accordance with the mandate and authorities of the agency requesting support and under warrant**, as applicable. We are bound by and respect any limits in those authorities.
- Under such circumstances, CSE **activities are subject to review** by the CSE Commissioner.
- **Everything that CSE does**, including assisting other Canadian law enforcement and security agencies, **is consistent with Canadian law**. There are also **strict measures in place to ensure that the privacy of Canadians is protected.**
- Detailed disclosure of requests for technical and operational assistance by federal law enforcement and national security agencies could compromise our **operational capabilities** or those of our federal partners.

Domestic and International Partners and Information Sharing

Q.44 When can CSE provide assistance to the RCMP and CSIS?

- Under the *National Defence Act* and upon request, CSE may provide technical and operational assistance to law enforcement and security agencies in the performance of their lawful duties.
- When CSE provides this **assistance to the RCMP or CSIS, we do so under their specific legal authorities** – for example, any applicable court warrant. We are bound by and respect any limits in those authorities.
- Under such circumstances, CSE activities are subject to review by the CSE Commissioner.

Q.45 What happens to CSE information shared with Five Eyes partners? Is it protected?

- Information shared with the Five Eyes partners is governed by a principle known as **originator control**. This means that **CSE sets and retains privacy controls** on any information we generate.
- Further, **CSE applies strict privacy rules** to protect the identities of Canadians when sharing intelligence reporting.
- International partners have agreed to strictly respect each other's privacy requirements and obligations.
- In his **2012-2013 Annual Report, the CSE Commissioner stated that he found that CSE does take effective measures to protect the privacy of Canadians in what it shares with international partners.**

Q.46 What measures does CSE take to protect privacy when sharing information with domestic and international partners?

- **When foreign intelligence includes any information about a Canadian** person, corporation, or organization, **the reference is altered in such a way that it is impossible to identify the Canadian.** Any Canadian identity information – such as a name, phone number, email address, or IP address – is removed and replaced with a generic reference, for example, a Canadian phone number.
- CSE's Government of Canada partners and **core allies may request and receive Canadian identity information only if they have both the authority**

and an operational justification to receive the information. All requests are assessed on a case-by-case basis and sharing must be in accordance with the standards outlined in the *Privacy Act*.

- Broadly speaking, CSE will only share Canadian identity information, if the information is essential to support the lawfully-mandated activities of the requestor, will not jeopardize Canadian domestic security efforts and will not cause undue harm to the Canadian. CSE may also attach conditions to how the information can be used.
- In accordance with Government of Canada direction, **CSE has clear measures in place to govern the sharing of information** including, where applicable, assessment of the potential for any privacy impacts and/or any potential of mistreatment. CSE also applies an escalating level of approval, depending on the information being requested and the recipient.
- The CSE Commissioner has reviewed CSE's information sharing and has confirmed that CSE takes measures to protect the privacy of Canadians in what it shares with international partners.

Q.47 What measures does CSE take to ensure the information it shares with foreign partners does not lead to mistreatment of individuals?

- CSE's **sharing of information is always undertaken in accordance with our legal obligations**, including the prohibitions on mistreatment, torture or other forms of cruel, inhuman or degrading treatment or punishment.
- CSE has put **policies and processes in place that fulfill the Government of Canada's obligations under domestic law and international conventions** to prevent mistreatment or torture.
    - These internal policies and processes ensure that the risks and associated mitigation measures are assessed prior to a decision to share information. The final decision to share information is based on a total risk assessment, including the application of mitigation measures.
- CSE must carefully manage relationships with foreign entities, assisted by policies that guide information sharing practices, to ensure that the sharing of information does not give rise to a substantial risk of mistreatment.

- Examples of possible mitigation measures, including additional caveats imposed by CSE, assurances provided by the foreign agency, or other proposed

measures to mitigate the risk, wherein CSE must address the likelihood that these measures would be successful.

Q.48 Does CSE have access to the US PRISM program?

- The former Minister of National Defence responded to this question in Parliament and noted that **CSE does not have access to data from PRISM**.

Q.49 Does CSE have a program similar to PRISM?

- **CSE cannot comment on its methods, operations or capabilities.**
- CSE is required by law to have strict measures in place to protect the privacy of Canadians.
- The CSE Commissioner has reviewed our activities and has noted in each of his annual reports that CSE acts in full compliance with Canadian law.

Mosley Decision

Q.50 Did CSE mislead the court or act in any way unlawfully in relation to this case?

- Justice Mosley has noted that **the testimony of CSE officials in answering his follow-up questions has been candid. No concerns about the lawfulness of CSE activities have been raised** in his decision or in the CSE Commissioner's review of these activities.
- CSE's technical and operational assistance to CSIS in relation to the targets covered by this warrant and any other statutory authority that CSIS may have is in keeping with the legal limits on our assistance activities under the *National Defence Act*.

SIRC Report

Q. **Can you comment on the statements about CSE in the recent SIRC report that mentions concerns about information sharing with allies through CSE?**

a. I have seen the report issued by SIRC, which is of course the review body for CSIS and not CSE.

b. **The independent CSE Commissioner** has reviewed and addressed the issue of information sharing with allies in his 2012-2013 report. He **concluded that CSE conducts its activities in accordance with the law and in a manner that includes measures to protect the privacy of Canadians.**

- CSE also operates by the principle of originator control in all its information sharing with allies, which means that Canada sets and retains privacy controls on any information shared.

c. **International partners have agreed to strictly respect each other's privacy requirements and obligations.**

Insider Threats

R. **What is the Government of Canada doing to protect sensitive information from insider threats**

a. The Government of Canada is committed to safeguarding sensitive information and is continuously assessing security measures in place to protect classified facilities and systems.

b. Issues related to safeguarding sensitive information are a priority for the Government of Canada, and represent a regular topic of discussion amongst senior Government of Canada officials focused on national security.

c. **Specifically, CSE constantly reviews, revises, and updates the measures in place to ensure the security of the information entrusted to us**, and the security of Government networks, especially as new information arises.

d. In our cyber protection role CSE manages Canada's Top Secret Network on behalf of the federal security and intelligence community, to ensure the continued security of the Government's most sensitive information.

S. **What has CSE done to make sure that a breach of security, such as Snowden, does not happen in Canada?**

a. CSE **continues to work closely with our allies to share best practices, and to identify measures to improve how we safeguard** all forms of classified information.

b. As part of a longstanding and continuous process, the entire 5-Eyes community (Canada, US, UK, Australia and New Zealand), has been reviewing and updating the measures used to safeguard classified information.

c. Unauthorized disclosures of classified information that have occurred in a number of allied countries over the last few years underline the importance of continual efforts to analyse our networks and implement upgrades. **We learn from every incident how to improve our information and personnel security**.

d. CSE, and many of our partners, are examining and implementing measures to minimize any potential vulnerability.

e. You may already be aware that **CSE has stringent measures in place for the clearance of employees and contractors. This includes psychological assessment and polygraph examination.**

f. With the focus on Snowden in the media, you may have heard that his system administrator access played a large role in his ability to pull such a large amount of classified information. CSE is currently reviewing all systems accounts that provide privileged access to ensure proper use and validity. CSE has increased its ability to monitor and detect potentially suspect behaviour.

T. **What measures does CSE take to protect whistleblowers or otherwise allow employees to raise concerns without fear of reprisal?**

- CSE is, by nature of its separate employer status and the sensitivity of its work, excluded from the definition of "public sector" in the *Public Servants Disclosure Protection Act* (PSDPA). However, the Act does require that CSE develop its own procedures, similar to the provisions found in the PSDPA.
- **CSE had developed a procedure to allow employees to raise concerns without fear of reprisal prior to the introduction of the PSDPA in 2005.** The procedure designates **a senior officer to whom wrongdoing can be reported** with protection from reprisal located within our audit and evaluation section. This senior officer reports directly to my office. Since 2005, we have updated the process to ensure that it provides similar protections to those offered to all public servants under the PSDPA.
- **All new employees are given training with regard to the process**, the procedures are posted on the organizational website and a hotline is being established.
- Employees also have the option of reporting any concerns to the CSE Commissioner, who has the investigation of complaints as part of his mandate.

CSE's Long-Term Accommodation

U. **Why does CSE require a new headquarters?**

a. There is an undisputed requirement for a new CSE facility given that there is no further possibility of expansion of our current facilities.

b. The current CSE campus is designed to support only half of the CSE workforce. This puts a tremendous strain on power and utilities which are already at a breaking point.

c. The Long-Term Accommodations project is on time and on budget.

V. **Why is CSE's new facility being built using a Private-Public Partnership?**

a. The Public-Private Partnership (P3) approach was found to be the most viable solution for the Long-Term Accommodations Project.

b. This approach allows the public sector to leverage private sector innovation and efficiency to deliver major public infrastructure projects. Advantages include greater certainty of on-time delivery, access to private-sector capital, and the transfer of certain risks, such as financial and schedule overrun.

c. The P3 approach also provides significant value-for-money. **The estimated savings are expected to be in the range of $176 million over the life of the contract.**

d. The construction of this facility is expected to result in the creation of up to 5,000 jobs in the Ottawa area and has already created 3,000 jobs to date. The private partner consortium in this project, led by Plenary Properties and PCL, estimates that 99 percent of the jobs created by this project will be Canadian.

W. **What is the cost of the Long-Term Accommodation Project?**

a. The design, construction and financing cost of the Long-Term Accommodation (LTA) project is $880 million.

b. The estimated savings from using the Public-Private Partnership approach are expected to be in the range of $176 million over the life of the contract.

c. Initial funding for the LTA was announced in 2009. Since then, there have been references in multiple federal budgets to the LTA P3 model and funding has been and will continue to be sought through the estimates process.

d. In line with the P3 approach, the **largest payment to the private contractor will be due following delivery of the building and appear in the 2014-15 Main Estimates**, with ongoing payments to be made thereafter and included in CSE reference levels until the end of the contract period in **2044-45**.

If pressed:

e. As reported on our public website and in the Public Accounts, **the total cost of the contract is $4.1 billion**, which includes the design, construction and financing of the LTA as well as **30 years of maintenance**.

X. **I've heard it said that the new CSE building will cost either $880M or $1.1B. What is the actual cost of the building?**

a. The **cost of the building is $880M**—this is the capital cost including design and construction. The capital cost remains **unchanged and construction is on time and on budget.**

b. As reported in the Public Accounts, the **full design, build and finance contract** with the **private partner is $1.1 billion and includes financing charges** that are related to the Public-Private Partnership approach to this project.

c. When the Government builds a new building it covers these financing costs and they would not be included in the cost estimate of the building. However, the Government would then also bear the risk of any increases due to changes in construction costs or schedule overruns.

d. The Public-Private Partnership approach is a special method of procurement that ensures that private partner is responsible for these risks and that taxpayers do not bear these unanticipated costs that may arise during construction.

e. The **estimated savings from using the Public-Private Partnership approach** are expected to be in the range of **$176 million over the life of the contract** to design, build, finance and maintain the building over 30 years.

Y. **I heard about a fire at your new building. How much damage was done and will the project budget or schedule change?**

a. The fire was **very minor** and the private partner estimates that the repair costs associated with the fire are under **$5000.**

b. The fire will have **no effect on the cost of the building, its security or the deadline** for completion of the project. CSE is still scheduled to move into the building in the fall of 2014.

c. Since this is a Public-Private Partnership, **the building and site are under the ownership and responsibility of the private partner**. The Government has not taken possession of the building as construction is still ongoing.

CSE Personal Information Banks

Z. **Why does CSE collect personal information on Canadians and why was this not reported before?**

- CSE does not target Canadians at home or abroad in its foreign intelligence activities, nor do they target anyone in Canada. That is prohibited by law and protecting the privacy of Canadians is CSE's most important principle.
- **CSE has always fulfilled its reporting requirements under the *Privacy Act.*** Previously, CSE personal information banks were previously listed in *Info Source* under the Department of National Defence. With the establishment of CSE as a stand-alone agency, responsibility for administration of the *Access to Information Act* and the *Privacy Act* was transferred from DND to CSE, effective April 1, 2013.
- **Through its website, CSE posted its first *Info Source* publication, which contains a listing of its personal information banks**. This information was posted in October 2013, ahead of the December 2013 Treasury Board deadline.
- Personal information banks apply to both Canadians and non-Canadians. Given CSE's foreign signals intelligence mandate, the vast majority of the information in CSE personal information banks related to foreign intelligence pertains to non-Canadians.
- **CSE is subject to robust independent external review by the CSE Commissioner** who has consistently found CSE protects the privacy of Canadians as required by law.

AA. **Why are certain Personal Information Banks exempt from publication?**

- CSE has three separate and institution-specific Personal Information Banks. One is related to foreign intelligence and the other two are related to cyber protection and employee mentoring.
- **Since 1984, the Foreign Intelligence PIB has been designated as exempt from disclosure as the information in that bank is related to international affairs and defence**. This exemption is in accordance with sections 18 and 21 of the *Privacy Act.*

II. AUTHORITIES / LEGAL ISSUES

Privacy and Accountability

BB. **What safeguards are in place to ensure that CSE's activities are legal and respect the privacy of Canadians?**

a. **CSE operates within all Canadian laws**, including the *Charter of Rights and Freedoms*, the *Human Rights Act*, the *Privacy Act* and the *Criminal Code*.

b. CSE also **has in-house legal counsel** from the Department of Justice who provide expert legal advice on proposed operations prior to their implementation.

c. In addition, **the independent CSE Commissioner reviews CSE's activities to ensure that they comply with the law**. The Commissioner produces an annual public report on his findings, and this report is tabled in Parliament.

d. Like all other government organizations, CSE is subject to periodic review by the Auditor General, the Privacy Commissioner and the Information Commissioner.

- As a stand-alone agency, CSE has also established a Departmental Audit Committee composed of external members as required under Treasury Board policy.

CC. **In sharing intelligence with your foreign partners, can CSE guarantee that the private information and identities of Canadians are protected?**

a. **CSE is required by law to have strict measures in place to protect the privacy of Canadians**. These measures extend to the sharing of information with allies, which must be in accordance with the *Privacy Act*.

b. Moreover, we are always working to ensure that we only collect required information. The **CSE Commissioner** reviews our activities and **in every case where the Commissioner has reached a conclusion he has always found CSE to be lawful.**

Ministerial Authorizations

DD. **What are Ministerial Authorizations?**

- A communication that originates or terminates in Canada in which the originator has a reasonable expectation of privacy is considered a private communication. **The interception of these private communications is prohibited under Part VI of the *Criminal Code*.**
- However, technological changes, including the shift to digital networks, the widespread adoption of the internet and the development of new communications technologies, have significantly altered how communications are transmitted.
- In this environment of new technology, **CSE may risk the inadvertent interception of private communications when targeting foreign entities**. This risk occurs because we have no way of knowing in advance, let alone controlling, who our foreign targets will communicate with, including persons in Canada.
- **Therefore, the Ministerial Authorization regime was established** in the 2001 amendments to the *National Defence Act*.
- Express authorization by the Minister of National Defence is required to protect CSE from criminal liability if it unintentionally intercepts private communications while conducting its mandated intelligence and protection activities.
- **Ministerial Authorizations are vital legal instruments that enable CSE to fulfill its mandate**. Without them, the organization would be unable to collect the data that it requires to obtain foreign intelligence or protect the information infrastructures of importance to the Government of Canada.

EE. **What are the conditions for Ministerial Authorizations?**

- **For the sole purpose of obtaining foreign intelligence**, the Minister may only issue an authorization to intercept private communication if
  - The interception will be directed at foreign entities, located outside Canada;
  - The information to be obtained could not be reasonably obtained by other means;
  - The expected foreign intelligence value of the information that would be derived from the interception justifies it; and
  - Satisfactory measures are in place to protect the privacy of Canadians and to ensure that private communications will only be used or retained if they are essential to international affairs, defence or security.
- **For the sole purpose of protecting the computer systems or networks of the Government of Canada**, the Minister must be satisfied that:
  - The interception is necessary to identify, isolate or prevent harm to the Government of Canada computer systems or networks;
  - The information could not reasonably be obtained by other means;
  - The consent of persons whose private communications may be intercepted cannot reasonably be obtained;
  - Satisfactory measures are in place to ensure that only information that is essential to identify, isolate or prevent harm to Government of Canada computer systems or networks will be used or retained; and
  - Satisfactory measures are in place to protect the privacy of Canadians in the use or retention of that information.
- **Structures are in place to ensure strict compliance with these conditions**. These include:
  - Executive control and oversight;
  - A dedicated group of CSE personnel focused exclusively on the development and implementation of operational policies and procedures, as well as embedded policy compliance teams in our operational areas;
  - An embedded legal team from the Department of Justice that works closely with and provides legal advice to CSE staff;

- Active monitoring of internal processes and an internal audit and evaluation function; and
- An external review by the CSE Commissioner as well as the Privacy Commissioner.

FF. **Why doesn't CSE require judicial warrants?**

- **Canadian warrants apply only to Canadians or persons in Canada.**

If pressed:

- **Warrants are court ordered and allow security and police agencies to target the private communications of specific individuals.**
- In contrast, **Ministerial Authorizations do not relate to specific individuals, rather they authorize an activity or class of activities that may risk intercepting private communications.** Any interception of a private communication is inadvertent and incidental to the objective of an operation.
- Further, Ministerial Authorizations require CSE to protect the privacy of Canadians and its activities are subject to review by the CSE Commissioner to ensure their lawfulness.

Interception of Private Communications/Lawful Access

GG. **Does CSE use "lawful access"?**

a. Under its assistance mandate, **CSE provides technical assistance to federal law enforcement and security agencies in the performance of their lawful duties**.

b. **All CSE actions are undertaken in accordance with the mandate and authorities of the agency requesting support and under warrant**, as applicable.

c. If, for example, the RCMP wanted our assistance with an investigation, then that assistance would be provided under the legal authorities that apply to the RCMP, such as any applicable warrant.

HH. **What happens to any private communications that CSE intercepts?**

a. A private communication that is incidentally intercepted by CSE, despite the fact that we only target foreign entities outside Canada, will **only be used or retained if it meets requirements specified in our legislation. That is, the private communication must be determined to be essential to foreign intelligence or cyber defence**. If CSE retains or uses the private communication, additional measures are taken to protect the privacy of any Canadians involved in the communication.

b. The use and retention of any recognized private communication **is reported to the Minister of National Defence** in accordance with the requirements outlined in the applicable Ministerial Authorization.

c. The **CSE Commissioner reviews** all CSE activities to ensure that the **privacy** of Canadians **is protected**.

- As in previous reports, in his **2012-2013** Annual Report, the Commissioner stated that **"CSE retained only those private communications essential to international affairs, defence or security."**
- The most recent annual report of the Commissioner also states that **the office can and does review every one of the small number of private communications** that CSE retains and uses.

II. **Under what circumstances would data collected from an incidental intercept be retained?**

a. With respect to foreign intelligence, information will only be used or retained if it is essential to international affairs, defence or security.

b. Regarding IT security, only information that is essential to identify, isolate or prevent harm to Government of Canada networks will be used or retained.

III. CYBER ISSUES

The Role of CSE in Cyber

JJ. **What is CSE's role in protecting Canada's critical infrastructure from a possible cyber attack?**

a. CSE is mandated to help ensure the protection of information and information infrastructures of importance to the Government of Canada. CSE's foreign intelligence reporting also provides valuable information on cyber threats to Canada.

b. **As you know, cyber security is a shared responsibility.**

c. **Public Safety has the lead for emergency response and critical infrastructure protection**, including responding to a major cyber incident outside the Government of Canada.

d. At the same time, **other federal agencies contribute their expertise** to a coordinated whole-of-government approach to cyber issues.

- **Working with other federal partners, CSE leads the coordination of cyber threat incident response across the government through our Government of Canada Cyber Threat Evaluation Centre** – known as GC CTEC.

KK. **What is CSE's role with respect to private sector engagement?**

a. **We support Public Safety's outreach and partnership efforts** with critical infrastructure owners and operators.

b. CSE is mandated to help ensure the protection of information and information infrastructures of importance to the Government of Canada, which can include the private sector.

c. **CSE shares cyber threat information and mitigation advice with the Canadian Cyber Incident Response Centre** – known as the CCIRC – at Public Safety for further dissemination to the private sector.

d. CSE has provided or supported threat briefings to the private sector so they can similarly protect their networks.

e. We also share information if we discover in the course of our mandated activities that a company has been the victim of a cyber attack.

f. In addition, CSE provides advice and guidance for the Government of Canada on our website that is applicable to the private sector.

LL. **What are the mechanisms CSE uses to disseminate information about cyber threats to Government departments and agencies?**

a. The Government of Canada Cyber Threat Evaluation Centre – known as GC CTEC – is part of CSE and produces a comprehensive suite of reports on cyber threats.

b. **GC CTEC's goal is to keep our clients informed** about the current cyber threat situation, any specific threats they should be defending against, and specific technical mitigation advice they should be adopting.

c. These reports are tailored for use by specific Government departments or for dissemination to all departments for broader adoption across the Government.

d. In this effort we partner closely with Shared Services Canada and the Treasury Board Secretariat's Chief Information Officer Branch.

MM. **What role does CSE have in ensuring increased GC IT security awareness, education, and best practices?**

a. As a lead security agency, **CSE provides advice, guidance, and training to departments on a wide range of IT security issues**. Implementing that advice and adhering to policies is the responsibility of each individual department.

b. In addition to this general advisory role, **CSE also supports an IT Security Learning Centre** that offers 38 courses annually to about 1,500 IT professionals per year from across the federal government.

NN. **What are the "systems of importance to the Government" identified in CSE's information protection mandate?**

a. Generally speaking, "systems of importance" to the Government include all of the Government's systems, as well as the non-government systems the Government depends on for the function of:

i. its own infrastructure, or

ii. the national economy or to safeguard the security of Canadians, such as the sectors identified in the Government of Canada's *National Strategy for Critical Infrastructure*.

OO. **Can you provide us with more detail as to how CSE helps to protect the Government's computer systems and networks?**

a. The **IT Security program at CSE provides products and services that help prevent, detect, and defend against IT security threats and vulnerabilities.**

b. **We work with other government departments**, including the Treasury Board of Canada Secretariat's Chief Information Officer Branch, with Public Works and Government Services Canada, and with Shared Services Canada.

c. **We develop technical standards and guidance**, in order to help federal departments and agencies to strengthen their IT systems and prevent cyber incidents.

d. With the additional cooperation of CSIS, the RCMP, and Public Safety Canada, **we track the activities and methods of IT security threat actors** seeking to steal or do harm to information systems of importance to the Government of Canada.

e. Our unique and highly specialized technical expertise and capabilities **complement and build on the commercial security technologies that are already being used to protect federal IT systems.**

f. **CSE monitors federal government network traffic**, in order to detect and defend against those IT security threats that are not in the public domain.

g. If a government system is the victim of a sophisticated threat, **CSE offers assistance for a focused and quick response to mitigate the incident, and to help prevent it from recurring.**

h. When appropriate, **CSE will also share the technical information on an incident with other government IT departments** so that they can take appropriate action to protect their networks from similar threats.

i. **Our technical information is also shared with our partners** at Public Safety Canada, who in turn distribute it through their partnerships outside the federal government, as appropriate.

j. In addition, **we work with our partners to share comprehensive cyber threat information and intelligence with the private sector** so they can similarly protect their networks.

OAG Fall 2012 Cyber Report

PP. **How has CSE responded to the Auditor General's findings in his report, *Protecting Canada's Critical Infrastructure from Cyber Threats*?**

- The Auditor General's concern that **CSE was not consistently providing the Canadian Cyber Incident Response Centre – known as CCIRC – with timely and complete information about threats** to Government of Canada information systems has been addressed.
- CSE has taken action to facilitate more frequent and secure communication between the two organizations.
- Specifically, **we have integrated an official from CCIRC into the Government of Canada Cyber Threat Evaluation Centre** at CSE two days a week since September 2012. This individual has full access, ensuring the timely sharing of information on cyber threats.
- This increased communication further enhances Government of Canada efforts to protect Canada's critical infrastructure.

QQ. **What is CSE doing to ensure that it is providing important information in a timely fashion and in an appropriate manner to all IT security partners?**

- Since 2011, **CSE has had standard operating procedures for sharing specific incident information and mitigation advice** in a timely and secure manner with government IT security partners.
- The Government of Canada Cyber Threat Evaluation Centre – known as **GC CTEC** and which is part of CSE – **provides cyber threat information to all Government of Canada departments and briefs senior government executives, chief information officers and departmental security officers regularly.**
- Our partners include Shared Services Canada, which is mandated to deliver IT services to all government departments and agencies in an effort to improve the efficiency, reliability and security of the government's IT infrastructure.
- In addition, **CSE routinely shares cyber threat information and mitigation advice with the Canadian Cyber Incident Response Centre** – known as CCIRC – at Public Safety. CCIRC passes this information and advice on to other levels of government and the private sector, as appropriate.

- Finally, **we are working to facilitate more frequent and secure communication with CCIRC** by integrating an official from CCIRC into GC CTEC two days a week, which can increase if required.

RR. **How has CSE spent the $570 million the Auditor General says it has received for cyber security?**

a. The Auditor General report states that CSE has been granted $570 million in funding approvals over the last ten years. However, **these funds were not exclusively allocated to cyber security**.

b. Rather, **they were meant to support a range of initiatives**, including building capacity in our Signals Intelligence and IT Security programs, a modernization program for computers, facilities, corporate services and research and development.

c. CSE supports cyber security efforts through its regular operations. The advice, guidance and services we provide through CSE's IT Security program are contributing to safeguarding electronic information belong to the Government of Canada and others.

d. IT Security is one component of our overall budget, with a budget of $157.1 million for FY2013-14. The other key program area – Signals Intelligence – has a budget of $286.6 million.

If pressed:

- For national security reasons, CSE does not provide specific funding details that might reveal its capabilities.

SS. **Now that CSE is responsible for monitoring cyber threats to the Government of Canada, does CSE do such monitoring on a 24/7 basis?**

a. Specialized automated equipment works constantly to detect and protect government networks from cyber threats.

b. Procedures are in place to ensure that cyber threats are detected and dealt with in a rapid and coordinated manner.

c. CSE is, by nature, a 24/7 operational organization and maintains a full-time operational coordination centre.

The Relationship between CSE and Other Government Departments

TT. **What is CSE's relationship with other key cyber units in the Government of Canada?**

- **Public Safety is the overall policy lead for cyber security** for the Government of Canada and it acts as the primary interface between the government, the private sector and the public.
- Included within CSE is the Government of Canada Cyber Threat Evaluation Centre – known as GC CTEC. Since 2011, **GC CTEC has been responsible for detecting and coordinating the Government of Canada's response to malicious cyber activity on its internal networks.**
- Since October 2013, this work is carried out **in collaboration with the newly created Government of Canada Cyber Incident Response Centre in Shared Services Canada (GC-CIRT).**
- **CSE monitors federal government network traffic** in order to detect and defend against those IT security threats not in the public domain.
- If a government system is the victim of a sophisticated threat, **CSE offers assistance for a focused and quick response to mitigate the incident, and prevent it from recurring.**
- When appropriate, **CSE will also share the technical information on an incident with other government IT departments** so that they can take appropriate action to protect their networks from similar threats.
- **The same information will be shared with Public Safety's Canadian Cyber Incident Response Centre, as appropriate,** for dissemination to its partners outside the federal government.

UU. **What is the difference in the roles and mandates of CSE, CCIRC and the new GC CIRT?**

a. **CSE is one of 3 federal organizations that have a role in cyber threat incident monitoring and incident response.**

b. **CSE's Cyber Threat Evaluation Centre (CTEC) monitors and defends against cyber threats to Government of Canada networks** that could potentially affect the confidentiality, integrity, or availability of federal government networks. CSE detects, analyses and defends against cyber security incidents.

c. Public Safety Canada is the national incident response coordination body. It has a unit called the Canadian Cyber Incident Response Centre, or **CCIRC, which acts as the national coordinator of cyber security incidents outside the federal level**, including incidents affecting the private sector, sub-national governments, or other critical infrastructure.

d. Shared Services Canada, the federal agency that is charged with consolidating and operating Government of Canada IT infrastructure, has a relatively new unit called the Government of Canada Cyber Incident Response Centre (**GC-CIRT**) since October 2013 which **assumes the first line tasks for responding to and mitigating cyber incidents on federal government networks**. CSE works closely with the GC-CIRT.

e. Generally speaking, GC-CIRT responds to cyber incidents on federal government networks, and CCIRC responds to those on other critical infrastructure networks in Canada. CTEC enhances the activities of both the GC-CIRT and CCIRC by developing and sharing cyber threat information, analysis, and mitigation advice which augment what those organizations already have.

VV. **What is the role and relationship between CSE and Shared Services Canada (SSC) now that the latter is leading the consolidation of federal government IT systems?**

a. **Shared Services Canada – or SSC – is working to consolidate government networks, data centres, and e-mail systems up to the SECRET level**, in order to establish a common security baseline across the government.

b. **CSE works closely with SSC** by helping it develop security requirements for information technology in the Government of Canada to strengthen IT security and resilience.

c. Since October 2013, much of CSE's work is carried out **in collaboration with the newly created Government of Canada Cyber Incident Response Centre in Shared Services Canada (GC-CIRT)**.

d. **CSE monitors federal government network traffic**, in order to detect and defend against those IT security threats not in the public domain.

e. CSE also contributes to SSC's efforts to track the activities and methods of cyber threat actors by using our unique technical expertise, capabilities, and classified information to complement the commercial security technologies already available and in use by federal IT security practitioners.

f. If a government system should fall victim to these sophisticated threats, **CSE offers assistance for a focused and quick response to mitigate the incident**, and prevent it from recurring.

g. When appropriate, **CSE will also share the technical information on an incident with other government IT departments** so that they can take appropriate action to protect their networks from similar threats.

h. It should also be noted that the Chief Information Officer Branch of the Treasury Board of Canada Secretariat is responsible for setting overall IT Security Policy and Standards for the government with CSE support and expertise.

WW. **What role does CSE have in evaluating and testing proposed equipment and systems related to Shared Services Canada's initiatives, such as Requests for Proposals?**

a. **CSE provides leading-edge guidance and strategic advice on IT security to the Government of Canada, including to Shared Services Canada throughout the development of Requests for Proposal related to security requirements for federal systems and networks.**

If pressed:

b. CSE will not comment on particular equipment suppliers, nor on the bidders, for these Requests for Proposal.

XX. **What is the CF's relationship with CSE in cyber matters? How do the two organizations work together?**

- **CSE provides intelligence and expert technical advice, guidance, and services to the Canadian Forces** to help protect and defend the Department of National Defence's systems against sophisticated cyber threats.
- CSE also provides the sophisticated cryptographic technology the Canadian Forces rely upon to keep military communications secure.
- **Support for these operations is a high priority for CSE.**

Cyber Threats

YY. **What is the risk that Canada faces in terms of cyber threats? I've heard some refer to the fact that we need to be ready for a "Cyber Pearl Harbour"?**

a. In general, I would say that, over the past few years, policy makers in Canada and elsewhere are coming to understand both the opportunities and the vulnerabilities inherent in the increasingly interconnected nature of our world.

b. **As information systems are connected to the Internet, they become vulnerable to malicious actions.** Previously, threat actors needed physical access to a system. Now any Internet-connected system is theoretically vulnerable to compromise by anyone with access to the Internet.

c. **We are aware of this risk and are taking prudent steps to better protect key systems.** The implementation of *Canada's Cyber Security Strategy* and the work that Public Safety is doing with critical infrastructure is an important step in that direction.

d. That being said, **the government is limited to providing guidance and advice to the private sector, which owns and operates 90% of Canada's critical infrastructure.**

ZZ. **How many compromises have there been?**

a. For national security reasons, CSE does not comment on security-related incidents.

AAA. **What was the role of CSE in response to the alleged Chinese cyber attacks against TBS and the Department of Finance in early 2011?**

a. CSE provides advice, guidance, and services to the Government of Canada and others to protect electronic information and infrastructure and is a key partner in *Canada's Cyber Security Strategy*.

b. While the Government does not comment on the specific operational details of security-related incidents like the ones that occurred in early 2011, **CSE has worked with, and continues to work with, Government of Canada departments to improve the security of their networks.**

BBB. **What was the impact of the alleged Chinese cyber attacks against TBS and the Department of Finance in early 2011?**

a. For national security reasons, the Government does not comment on the specific operational details of security-related incidents.

CCC. **What countries/states are targeting Canada most aggressively for intelligence?**

a. For security reasons, I cannot comment on which countries are targeting Canada.

DDD. **What about the Mandiant report? Is China hacking the networks of the Canadian government and Canadian businesses?**

a. I cannot comment on the alleged actions of any specific state or actor.

EEE. **Does equipment sold by some telecommunications equipment vendors pose any threats to the Canadian government's computer infrastructure? Is there any software or hardware in such equipment that could assist in spying on the Canadian government?**

a. **CSE is mandated in legislation to provide advice, guidance, and services to the Government of Canada and others to** protect electronic information and infrastructure of importance to the government.

b. To that end, **CSE works closely with government departments and agencies to raise awareness** and increase the IT security posture of their networks.

c. While I cannot comment on specific vendors or equipment, I can say that **CSE provides advice and security evaluation of products for the Government of Canada** on products regardless of vendor.

d. **We also have unclassified advice on our public website** that includes guidance on the technology supply chain.

Canada's Cyber Security Strategy

FFF. **What is CSE's role in *Canada's Cyber Security Strategy*?**

- The three key objectives of the Strategy are to:
  - Strengthen the CAPABILITY of the Government of Canada to protect itself;
  - Build CREDIBILITY for the Government of Canada as a trusted partner with the private sector, critical infrastructure sectors, academia, the provinces and territories, and international allies; and
  - Promote AWARENESS among Canadians, helping them to protect themselves online.
- CSE contributes to the first objective – strengthening the CAPABILITY of the government to protect itself – by **enhancing its analytic capacity and providing more comprehensive cyber threat information to key partners.**
- Our efforts to protect Government of Canada networks have **secondary benefits in terms of information sharing with the private sector so they can similarly protect their networks.**
- This approach aligns with Canada's key allies and the cyber security capabilities of their respective cryptologic agencies. This demonstrates that Canada, like its allies, recognizes the importance of cyber.

GGG. **Did CSE receive any part of the $155 million funding announced in October 2012 by the Government to improve cyber security? If so, what is CSE doing with those funds?**

a. The **first dedicated investment for cyber security was $90 million over five years** provided for *Canada's Cyber Security Strategy* in October 2010. These resources were **shared among nine Government of Canada departments, including CSE.**

b. There has since been **an additional government investment of $155 million** to further bolster the cyber defences of the Government, a portion of which was given to CSE.

c. The additional funding will help CSE contribute to Securing Government Systems, which is the first pillar of *Canada's Cyber Security Strategy.*

d. The details of specific CSE operations and capabilities are classified to ensure that no unintentional advantage is provided to Canada's adversaries.

e. However, the purpose of the funding is consistent with our existing mandate to provide advice, guidance and services to help ensure the protection of electronic information, information infrastructure of importance to the Government of Canada and foreign intelligence on cyber threats.

IV. GENERAL QUESTIONS

The Establishment of CSE and Its Role

HHH. **When was CSE established?**

a. CSE was formally established, by an Order-in-Council, in 1946 as the Communications Branch, National Research Council.

b. In 1975, it was renamed the Communications Security Establishment and moved to the Department of National Defence.

c. **In November 2011, it was established as a stand-alone agency** with the status of a department within the National Defence portfolio.

III. **What is CSE's role within the Government?**

- **CSE provides foreign intelligence to a number of Government of Canada departments and agencies**, including the Privy Council Office, Foreign Affairs, National Defence/Canadian Forces, CSIS, the RCMP, CBSA, CIC and Transport Canada, in accordance with Government of Canada intelligence priorities.
- In addition, **CSE works with other federal partners**, most notably Public Safety, Shared Services Canada, and Treasury Board **to ensure that the government's communications are secure**.
- **CSE also provides assistance to federal security and law enforcement agencies** – such as the RCMP and CSIS - in the performance of their lawful duties.

JJJ. **How does CSE handle information about Canadians?**

- **CSE adheres to all Canadian laws concerning the use, retention, sharing and disclosure of information about Canadians.**
- The *National Defence Act* mandates that CSE shall have measure to protect the privacy of Canadians. CSE has implemented detailed policies and procedures, reviewed by the Department of Justice, to abide by its commitments in this area.
- CSE is subject to review by both the Information and the Privacy Commissioners and is reviewed regularly by the CSE Commissioner, who has specifically noted our culture of lawful compliance and genuine concern for protecting the privacy of Canadians.

KKK. **Does CSE monitor the Internet? Does CSE monitor social networks?**

a. CSE collects foreign signals intelligence from the global information infrastructure and provides services to help protect electronic information and systems of importance to the GC. Beyond this, **we cannot discuss specific activities.**

The CSE Commissioner and Annual Report

LLL. **Who is the CSE Commissioner and what role does he play?**

- The independent CSE Commissioner, **a supernumerary or retired judge**, can **review all activities carried out by CSE and provides a public report to Parliament annually** to ensure CSE compliance with the law including and the protection of the privacy of Canadians.

MMM. **How many reviews has the CSE Commissioner conducted on CSE activities?**

- **Since 1997**, CSE Commissioners have submitted **75 classified review reports to the Minister of National Defence**. The Commissioner also submits an unclassified annual report to the Minister; this is then tabled in Parliament.
- The Commissioners' review reports have contained **140 recommendations**. **CSE has accepted and implemented or is currently addressing 92% of these recommendations**. Each review provides helpful feedback to CSE so that we can further strengthen our strict measures to protect the privacy of Canadians.

NNN. **Why does the Commissioner say in his most recent report that you may have directed your activities at Canadians?**

- For the past 16 years, CSE Commissioners have reported that CSE continues to act lawfully in the conduct of its current activities.
- In the 2012-2013 Annual Report, **the Commissioner noted that he did not have any concerns or recommendations with the vast majority of CSE activities that were reviewed**.
- In a single historical review of a small number of records gathered in the early 2000s, the Commissioner reported that he was unable to reach a definitive conclusion regarding activities directed at a remote location outside Canada.
- This conclusion does *not* indicate that CSE has acted unlawfully. It indicates that certain historical material upon which the Commissioner would have relied for his assessment was incomplete or not available for a number of reasons.

- Since this particular review, CSE has upgraded several of its systems to store and retain historical information to satisfy the Commissioner's review requirements.
- Of note, **again this year the Commissioner commended me as the Chief of CSE for instilling, within the organization, a culture of respect for the law and for the privacy of Canadians.**

OOO. **Has CSE broken the law?**

- No. In every case where the Commissioner has reached a conclusion, CSE activities have always been found to be in compliance with the law.

PPP. **Has CSE directed its activities at Canadians?**

- CSE is prohibited by the *National Defence Act* from directing its foreign intelligence activities at Canadians and it respects this prohibition.
- The **Commissioner's report confirms that CSE employees are well aware of policies and procedures regarding the protection of the privacy of Canadians,** and staff members repeatedly demonstrate their knowledge of their responsibilities in these areas.

QQQ. **What does the CSE Commissioner have to say about your intelligence sharing with allies?**

- The independent CSE Commissioner has reviewed and addressed the issue of information sharing and has concluded that CSE conducts its activities in accordance with the law and in a manner that includes measures to protect the privacy of Canadians.

CSE Targeting Issues

RRR. **Does CSE target Canadians in its foreign intelligence activities?**

- No. **CSE, in carrying out its foreign intelligence mandate, is prohibited by law from directing its activities at Canadians** located anywhere or any person in Canada. CSE has rigorous procedures in place to ensure it adheres to this prohibition.
- When supporting Federal law enforcement and security agencies, CSE operates under the requesting agency's authorities, which include any applicable court-issued warrants.

SSS. **In carrying out its foreign intelligence mandate, does CSE target the citizens of its closest allies?**

- There is a longstanding convention in policy among CSE and its closest international partners not to target each other's citizens.

TTT. **Do CSE's closest allies target Canadian citizens?**

- CSE is prohibited by law from directing its activities at Canadians or any person in Canada. **It would never ask its international partners to act in a way that circumvents this restriction.**

If pressed:

- There is a longstanding convention in policy among CSE and its closest international partners not to target each other's citizens.

UUU. **How does CSE determine who and what to target?**

- Legislation requires that CSE's foreign signals intelligence activities are linked directly to intelligence priorities. These are determined by the Government of Canada.

CSE Relationships

VVV. **What is the relationship of CSE with Internet Service Providers?**

- **CSE has a broad range of partnerships** with various government departments and agencies, as well as with industry that helps improve security in products and services provided to the GC. Beyond this, we cannot discuss specific partnerships.

WWW. **How does CSE provide technical and operational assistance to federal law enforcement agencies?**

- Our unique technical capabilities are a resource that is helpful to federal law enforcement and security agencies in the performance of their lawful duties.
- Such **assistance would leverage the authorities and restrictions of the requesting agency**, which may include instruments like judicial warrants. Assistance is only provided upon request.

XXX. **What is the nature of CSE's assistance to its federal partners?**

- Through its legislation, **CSE has been mandated to support federal law enforcement and security agencies** such as CSIS and the RCMP.
- This **support is always provided under our partners' authorities and under warrant**, as applicable. It is also always of a technical or operational nature. For example, CSE has developed technical solutions to assist CSIS and the RCMP in their efforts to lawfully access information in the course of their investigations.
- To abide by the limits outlined in the *National Defence Act*, **CSE requires that the requesting agency first demonstrate that they have legal authority**, such as a warrant, to conduct the activities. CSE is subject to the same laws and limitations that govern the agency it is assisting.
- In reviewing CSE activities to assist federal law enforcement and security agencies, **the CSE Commissioner verifies that CSE complies with any limitations imposed by law on the requesting agency**, for example, any conditions imposed by a judge in a warrant.

YYY. **Who are your foreign partners? What do you share with them?**

- For over 65 years, **CSE has maintained its closest partnerships with allied agencies** in the US National Security Agency, Great Britain's Government Communications Headquarters, the Australian Signals Directorate) and New Zealand's Government Communications Security Bureau. This partnership is referred to as **the Five Eyes.**
- CSE receives and shares intelligence with the Five Eyes and we jointly address technological challenges and collaborate on issues such as counter-terrorism and cyber security.
- **CSE also has important relationships with NATO members through existing signals intelligence and IT security fora.** Cooperation covers several areas, including intelligence sharing, communications security and technical collaboration.

ZZZ. **Does CSE have any direct knowledge of, or has it at any time been involved with, NSA's alleged 'domestic surveillance program'? Does CSE have a similar program?**

- CSE has no direct knowledge of or involvement with such a program.
- CSE does not direct its foreign intelligence activities at Canadians or any person in Canada.

Cryptography and SIGINT

AAAA. **What is cryptology?**

- **Cryptology is the art and science of making codes and ciphers and breaking them.** Traditionally, cryptology is composed of two disciplines: cryptography (making our using codes and ciphers) and cryptanalysis (breaking codes and ciphers).

BBBB. **What is signals intelligence, or SIGINT?**

- SIGINT refers to **signals intelligence – the foreign electronic emissions collected and exploited by CSE.** SIGINT is used to produce the intelligence reporting that responds to Canadian government requirements.
- The success of the SIGINT process is founded on our understanding of the key technologies used within the global information infrastructure.

Our Place in Government

CCCC. **What are the implications of CSE's change in its place in government?**

- CSE was previously part of the Department of National Defence (DND) and became a stand-alone agency on November 16, 2011.
- As a stand-alone agency, **CSE is directly accountable to the Minister of National Defence.**
- This change in status had **no impact on the CSE mandate to provide foreign intelligence, advice and guidance on systems of importance to the Government and support to law enforcement and security and intelligence organisations.**
- There was no cost to the taxpayer and no new funding associated with this change. Existing funding for CSE activities has been transferred from the Department of National Defence to CSE.
- **Our activities continue to be subject to independent, external, and public review** by the CSE Commissioner, Auditor General, Privacy Commissioner, Information Commissioner, and Parliamentary committees and Commissions of Inquiry, amongst others.
- Prior to becoming a stand-alone agency, information regarding CSE was included in broader DND reporting.
- Since becoming a stand-alone agency, CSE now appears in the Main and Supplementary Estimates, as well as in the *Public Accounts.*
- CSE is required to produce documents which are reviewed by the Treasury Board Secretariat to ensure accountability, but not all of which can be made public, due to reasons of national security.

DDDD. **What is the impact of the change in CSE's status on its role and relationship with the CF?**

- On November 16, 2011, CSE was established as a stand-alone agency. This was principally an administrative change. **The Chief of CSE now reports directly to the Minister of National Defence**, rather than through the National Security Advisor and the Deputy Minister of National Defence.

- This change has no impact on the mission, mandate or operations of CSE. The ongoing collaborative relationship between CSE and the Canadian Forces is not affected by this change.

Recent Terrorist Attacks and Radicalization

EEEE. **Was CSE involved in responding to the January 2013 Algerian terror attacks or the April 2013 bombings in Boston?**

- In the event of a terrorist attack, we work closely with Canadian and allied partners to support a coordinated response.
- **Under the CSE assistance mandate, we provide technical and operational support to Canadian investigations**, in accordance with the mandate and authorities of the agency requesting support and under warrant, as applicable.
- Under the CSE foreign intelligence mandate, **CSE may provide intelligence related to the activities of foreign terrorist networks and their operational and organizational plans.**

If pressed:

- For national security reasons, CSE does not comment on operations.

FFFF. **What is the role of CSE in combatting the radicalization of Canadians?**

- **Under the CSE assistance mandate, we provide technical and operational support to Canadian investigations**, in accordance with the mandate and authorities of the agency requesting support and under warrant, as applicable.
- **Under the CSE foreign intelligence mandate, CSE may provide intelligence related to the activities of foreign terrorist networks** and their operational and organizational plans.

If pressed:

- For national security reasons, CSE does not comment on operations.

GGGG. **Did CSE play a role in the arrest of two Canadians accused of planning to derail a passenger train in Toronto?**

- Under the CSE assistance mandate, we provide technical and operational support to Canadian investigations, in accordance with the mandate and authorities of the agency requesting support and under warrant, as applicable.

If pressed:

- For national security reasons, CSE does not comment on operations.

V. FINANCIAL/RESOURCE/ACCOMMODATIONS ISSUES

General CSE Finances

HHHH. **What is CSE's current budget?**

- **Our total budget combining the 2013-14 Main Estimates and Supplementary Estimates to date is $443.7 million.**
- This is split between two program areas, IT Security and Signals Intelligence with budgets of $157.1 million and $286.6 million respectively.

IIII. **Does CSE have the necessary resources to fulfill its mission?**

- **CSE is satisfied with our current level of resources**, we continue to align our resources to our highest priorities.

JJJJ. **Why is there no additional detail concerning the spending of CSE?**

- **CSE does not publicly disclose details of its budget for reasons of national security and to protect operational integrity. This information could compromise operational capabilities and put the safety of our employees at risk.**
- Similar to CSIS and other allied intelligence agencies, CSE carefully monitors any disclosure of information in unclassified settings that may unintentionally provide a cumulative picture of the Government of Canada's foreign intelligence and IT security capabilities.
- However, **when it became a stand-alone agency in 2011, CSE began to appear in the Main and Supplementary Estimates, as well as in the *Public Accounts*.**
- CSE's exemption from quarterly financial reporting ensures that the status of CSE as a stand-alone agency does not create new requirements that would risk unintentional disclosure of information to Canada's adversaries on the operational capabilities of CSE.

KKKK. **What cutbacks did CSE undertake as part of the deficit reduction measures included in Budget 2012?**

- **As of 2013, CSE is providing $13.7 million in ongoing savings** as part of the Government's Deficit Reduction Action Plan announced in Budget 2012.
- This will be achieved through internal reallocations and improved efficiencies.
- These savings will have no negative implications to the continued fulfilment of our operating activities or our accountability and review mechanisms.
- **There will be no employment losses for CSE staff** as a result of the implementation of the savings.
- Further, when part of the financial administration of the Department of National Defence CSE also received a budget reduction of $9.8M as a result of the DND's overall Strategic Review Process.

Supplementary Estimates B

CSE's Budget Increase

LLLL. **Why does CSE's budget continue to escalate at a time when other departments are being cut back?**

- The **CSE funding envelope increased substantially following the events of 9/11 as the federal government made significant investments in the areas of security and intelligence.**
- Moreover, in recent years CSE funding has also been **increased in order to meet targeted Government of Canada priorities, particularly those related to cyber security and securing Government of Canada systems and information from threats.**
- Additionally, there have been administrative transfers of funding related to the establishment of CSE as a stand-alone agency.
- Like all departments, CSE participated in the Deficit Reduction Action Plan and, starting in 2012-2013, CSE is providing $13.7 million in ongoing annual savings.
- Further, when part of the financial administration of the Department of National Defence CSE also received a budget reduction of $9.8M as a result of the DND's overall Strategic Review Process.
- Our total budget combining the 2013-14 Main Estimates and supplementary estimates to date is $443.7M.

If pressed on specific examples

- **CSE has received additional resources for its important role in supporting *Canada's Cyber Security Strategy*.** CSE plays a central part in Pillar 1 of the Strategy – securing Government systems;
- One-time investments have been needed to maintain CSE's current buildings and to support the initial stages of CSE's long-term accommodations project, a Public-Private Partnership that will enable CSE to continue to deliver on its mandate and deliver $176 million in savings over the life of the contract.

- Since becoming a stand-alone agency, CSE has also received administrative transfers of funds related to CSE activities from the Department of National

Defence funding envelope. As a specific example, CSE is receiving transfers from DND to complete the implementation of the Canadian Cryptographic Modernization Program, a CSE-led project since 2005 for which DND is the main beneficiary;

- Like many Government of Canada departments, CSE has received targeted funding in order to continue its support of Government of Canada efforts to deter known human smuggling ventures since the arrivals of the migrant vessels *Ocean Lady* and *Sun Sea*.

CSE's Reporting Detail

MMMM. **Why is there no additional detail in these estimates concerning the spending of CSE?**

- **CSE does not publicly disclose detailed budget information for reasons of national security and to protect operational integrity. This information could compromise operational capabilities and put the safety of our employees at risk.**
- Similar to CSIS and other allied intelligence agencies, CSE needs to carefully consider the disclosure of information in unclassified settings that may unintentionally provide a cumulative picture of the Government of Canada's foreign intelligence and IT security capabilities.
- When it became a stand-alone agency in 2011, CSE began to appear in the parliamentary estimates as well as in the *Public Accounts*.
- CSE's financial reporting in the estimates is organized under its two main programs, foreign Signals Intelligence and Information Technology Security.
- A proportional share of the internal services to support these activities is reflected under each program.

Funding for Modernizing Canada's Top Secret Network (CTSN)

NNNN. **Why is CSE receiving funding for modernizing the CTSN?**

- The Government of Canada is committed to ensuring that its computer networks are robust and defended against all types of security threats.
- As part of its mandate, CSE works to provide advice and services to ensure the protection of electronic information and systems of importance to the Government of Canada, such as the Canadian Top Secret Network.
- With this funding CSE will implement system and collaborative tool upgrades, as well as life cycle maintenance that will ensure the continued security of the Canadian Top Secret Network and the Government's most sensitive information.
- This is the first year of funding for this time-limited project, which will require **$44.6 M to implement with $9.6M ongoing to fund the life cycle operation and maintenance of the network.**

OOOO. **What is the CTSN?**

- The Canadian Top Secret Network is used by a number of Government of Canada departments for the exchange of information at the TOP SECRET level.
- It is separate from standard government networks provided by Shared Services Canada.
- In our cyber protection role and using our unique expertise, CSE manages the network on behalf of the federal security and intelligence community.

PPPP. **Are these security upgrades intended to address leaks of information by people like Snowden and Delisle?**

- This effort is not a direct result of any specific incident.
- CSE constantly reviews, revises, and updates measures in place to ensure the security of the Government information and networks.
- We also work closely with our allies to share best practices, and to identify measures to improve how we safeguard all forms of classified information.

- As part of a longstanding and continuous process, the entire allied community (Canada, US, UK, Australia and New Zealand), has been reviewing and updating the measures used to safeguard classified information.
- Unauthorized disclosures of classified information that have occurred in a number of allied countries over the last few years underline the importance of continual efforts to analyse our networks and implement upgrades.

QQQQ. **What is the current status of this project? Are classified documents at risk because these upgrades have not been made?**

- While in the early stages of this project, CSE is on track with our plans to make modern system upgrades that will ensure the continued security of the Government's most sensitive information.
- **The current network is robust and subject to significant and continual efforts focused on maintaining its security.** This funding supports a concentrated effort to modernize specific aspects of the network's infrastructure that will support advanced security and technical features now and in the future.

Funding for Wage and Salary Increases

RRRR. **Why is CSE receiving funding for wage and salary increases?**

- In anticipation of a new collective bargaining agreement for CSE employees, this amount reflects a re-profile of funding previously set-aside in CSE's budget to cover the estimated retroactive pay that would be due to employees. We hope to reach an agreement this fiscal year.

SSSS. **Can you provide a status update on CSE's collective bargaining?**

- Following, the last set of negotiations between on October 10, 2013, the Public Service Alliance of Canada made a request on November 7th for a Public Interest Commission to assist in resolving a number of outstanding issues.
    - CSE has provided their position on all outstanding issues (13) as well as 3 additional issues.
- As a result, the Public Service Labour Relations Board will establish a conciliation board over the next couple of weeks and then set a hearing date sometime in April or later.
- CSE anticipates a report before the end of the summer with recommendations to the parties.
- Once a report is issued with recommendations, the parties will be expected to return to the table to resolve the issues. In the interim the union will likely solicit direction from the employees on a potential strike.

Funding to Combat Human Smuggling

TTTT. **Why is CSE receiving funding to combat human smuggling?**

- The amount in the Supplementary Estimates (B) reflects time limited funding to CSE as it continues to support Government of Canada efforts to deter known human smuggling ventures.
- The funding level is consistent with allocations in past estimates since the arrival of the migrant vessels *Ocean Lady* and *Sun Sea*. [$700K annually]

If pressed on specifics of CSE's support

- CSE's support to this Government of Canada effort is consistent with our mandate as the Government's foreign signals intelligence agency.
- As you may be aware, the details of specific CSE operations are of a classified nature.

Transfer from National Defence for the Canadian Cryptographic Modernization Program (CCMP)

UUUU. **Why is CSE receiving a transfer of funding for the CCMP?**

- CSE is committed to maintaining the security of our most sensitive information.
- **This transfer continues the implementation of a program underway since 2005 to modernize the infrastructure used to secure classified communications**, such as those essential to the safety of our military personnel in the field and Canadians at missions abroad.
- This is not new funding, but a transfer of allocations for an existing program for which CSE is the program lead.
- CSE is now a stand-alone agency, financially separate from the Department of National Defence. However, the Department of National Defence is the primary user of cryptographic equipment and the main beneficiary of this program.

VVVV. **What is this money for the CCMP used to do?**

- Initiated in 2005, the Canadian Cryptographic Modernization Program (CCMP) is an $839M multi-year omnibus project led by CSE.
- Funding under this program is used to modernize the cryptographic equipment and infrastructure that the Government uses to safeguard classified information. This is critical to maintaining Canada's ability to establish secure communications both nationally and internationally and to the safety of military and other deployed Canadian personnel around the world.
- In the new reality that is cyberspace, it is critical for the government to continue to stay ahead, ensuring our most classified information can be communicated in a secure manner.

PSAT Funding

WWWW. **Can CSE account for how it spent the funding received for the Public Security and Anti-Terrorism (PSAT) Initiative?**

- CSE can account for the funding received to support activities under the Public Security and Anti-Terrorism (PSAT) Initiative and has reported to Treasury Board, as required.
- All CSE expenditures have been reported annually to Parliament through the Estimates process and Public Accounts.
- **The Auditor General found that CSE had spent PSAT funding on projects consistent with the broad objectives of the Initiative.**

If pressed:

- CSE does not publicly disclose details of its budget for reasons of national security and to protect operational integrity. This information could compromise operational capabilities and put the safety of our employees at risk.

OAG Spring 2013 Report on the Policy on Safeguarding Government Assets and Information in Contracting

XXXX. **What were the results of the Auditor General's findings outlined in his Spring 2013 report, *Safeguarding Government Assets and Information in Contracting*?**

- The Auditor General found that **CSE was fully compliant with the Policy on Government Security and has policies in place that provide assurances beyond the levels required**. CSE has implemented a quality assurance program and has an approved Departmental Security Program.
- **CSE requirements for firm clearance**, also known as Facility Security clearances, **exceeded the requirements in the Policy on Government Security.**
- In some cases, contracts were awarded to firms before Facility Security clearances had been granted to the organization.
    - For example, for an urgent plumbing issue, CSE would accept a contractor with a lower clearance and provide an escort while the work was completed.
    - While these contracts did not meet the requirements contained in CSE's internal guidelines, Government of Canada minimum standards were exceeded and risk mitigation measures were in place.
- The Auditor General's report also provides a positive review of security practices for contractors working at the new Long-Term Accommodation project.

YYYY. **How has CSE responded to the Auditor General's findings in his report, *Safeguarding Government Assets and Information in Contracting*?**

- CSE has accepted the Auditor General's recommendation to ensure that security requirements are fully met before a contract is awarded and has updated internal policy accordingly.

ZZZZ. **What did the report recommend to CSE?**

- The Auditor General recommended that CSE should ensure that contract security requirements are met before the awarding of a contract.

AAAAA. **What were the findings of the Audit, specific to the CSE Long-Term Accommodation Project?**

- The Audit found that security has been well considered in CSE Long-Term Accommodation Project.
- Until firms and contractors were appropriately cleared, no site access was granted and no work was permitted.
- CSE took several additional precautions, including:
  - ensuring firms providing construction materials were only granted access to specific sections of the work site as necessary;
  - restricting access to drawings of the building and the building site; and
  - establishing verification procedures to ensure that there were no unobserved breaches of security.