Canadian Association of Petroleum Producers (CAPP) Presentation
Director, Richard B. Fadden

Slide 1 - Title Page

The Canadian Security Intelligence Service

An Overview

Speaking Points

-In preparing for this meeting I learned that your industry group has been around since 1927 in one form or another. That is impressive. Equally impressive is that your member companies produce more than 90 per cent of Canada's natural gas and crude and have annual revenues of about $100 billion-a-year.

-You represent an important economic sector, and in today's globalized world, economic and security interests are closely related. I'm delighted to meet with you and it's a relationship I'd like to develop.

Slide 2 – Who We Are

- Canada's National security intelligence agency
- *CSIS Act* (1984)
- CSIS is a civilian organization
- No power to arrest or detain

Speaking Points

-CSIS is Canada's national security intelligence agency. We were created in 1984 by an Act of Parliament based upon the findings of the MacDonald Commission. The Commission recommended that security intelligence functions be separated from law enforcement and given to a civilian agency subject to strict review.

-CSIS is that civilian agency and we were provided a broad operational scope. We are responsible for investigating activities that aren't necessarily illegal but could still be detrimental to Canadian interests. As a consequence, we don't require the powers of arrest or detention. We are also subject to a great deal of public review and scrutiny. Two-thirds of our founding legislation is dedicated to oversight.

Slide 3 – CSIS Operations

- CSIS investigates, collects, analyses and reports – to government – information about threats to Canada and Canadian interests

- The primary focus of CSIS activities are on:

  - Terrorism
  - Espionage and Foreign Interference
  - Information Security Threats
  - Proliferation of Weapons of Mass Destruction

- CSIS operates mainly inside Canada but also maintains a significant international presence

Speaking Points

-Our mandate is to collect, analyse and report -- to government -- information about threats to Canada and Canadian interests at home and abroad.

- Security threats to Canada can originate from anywhere. The most immediate security threat facing Canada, the one that consumes the majority of our resources, is terrorism - and that is a phenomenon without borders. As a result, while we operate mainly inside Canada, we must also maintain an international presence. We follow the threat.

Slide 4 – Terrorism

- Al Qaeda and Its Affiliates
- Radicalization and "Home-grown" Terrorism

Speaking Points

- So let's talk about terrorism. Despite the death of Osama Bin Laden, Al Qaeda (AQ) remains one of the most dangerous terrorist groups in the world. Even if AQ leadership, or what we sometimes call AQ Core, has been weakened, the organization is a many-headed hydra, with affiliates in different parts of the world

-There's Al Qaeda in the Arabian Peninsula, which is known for its creative operational planning. The notorious underwear bomber and the printer cartridge plots were hatched by AQAP; there's Al Qaeda in the Islamic Maghreb (AQIM), a vicious group that has kidnapped and murdered westerners across North Africa. And of course there's the Al Qaeda ideology, which has a life of its own beyond any one group or terrorist leader.

-One of the issues that preoccupies us and other intelligence services is the phenomenon of radicalization, the process whereby individuals move from holding moderate, mainstream beliefs towards adopting extremist political or religious ideologies. It is generally fuelled by the adoption of significant grievances against Western governments, their societies and way of life, as well as the conviction that the Muslim world is under attack and needs defending through the use of violence. The influence of a charismatic ideologue and the abundance of Internet-based lectures and propaganda supporting a radical cosmology also contribute to the process.

-Even if Al Qaeda and other groups have been diminished they have learned that so-called small arms attacks are equally effective at terrorizing a population. The actions of a single terrorist with simple weapons can spread profound fear and disrupt our way of life, as the recent events in the French city of Toulouse showed.

Slide 5- Domestic extremism

- Energy sector as an attractive target.
- From peaceful to violent protest

Speaking notes

- Canada's energy infrastructure poses an attractive target for both international and radicalized "home-grown" terrorists, as well as single-issue and domestic extremists groups. Small improvised explosive devices (IEDs) detonated near strategically vulnerable sites can cause large-scale damage and injury.

-As we all learned in the recent bombings of Encana pipeline assets in British Columbia, even relatively small IED targeting of pipeline infrastructure has significant disruptive effects on the targeted company, its work force and the local community.

-In Europe, a radical and violent reaction to the economic downturn is expected to continue. Those who are frustrated with economic uncertainty typically express themselves non-violently, at least in Canada, but that's not always the case. The 2010 firebombing of a Royal Bank branch in Ottawa represented a serious case of politically motivated violence against the financial sector.

-The grievances harboured by those who oppose issues such as the perceived oppressive effects of capitalism are likely to continue and may trigger additional acts of serious violence.

-The potential for violent confrontation in 2012 could well coalesce around opposition to natural resource development such as the shale gas development in New Brunswick and British Columbia, and the Northern Gateway pipelines project.

-Canadian domestic extremists are increasingly sharing techniques to secure their communication and prevent exposure of their activities. Needless to say, this emerging "security culture" makes it more difficult to identify extremists.

Slide 6 – Espionage and Foreign Interference

- CSIS investigates clandestine activities by foreign governments in Canada that may be detrimental to Canadian interests

- Why is Canada a target?

  - Expertise
  - Support global acquisitions and investments
  - Support state-owned enterprises (SOEs)

Speaking Points

- Espionage is an unfortunate reality in the post-Cold War era where economic and strategic competition is both global and intense. Canada is a particularly attractive target to hostile foreign powers owing to our status as a world leader in communications, mineral and energy extraction, aerospace and other areas. The consequences for Canada can be measured in lost jobs, in lost tax revenues and in an overall diminished competitive advantage.

-A related security issue is one of foreign investment. Canada is a trading nation. Our wealth, advanced infrastructure and vast potential make us an attractive prospect for foreign investors. While the vast majority of foreign investment in Canada is carried out in an open and transparent manner, certain state-owned enterprises (SOEs) and private firms with close ties to their home governments have pursued opaque agendas or received clandestine intelligence support for their pursuits here.

-When foreign companies with ties to foreign intelligence agencies or hostile governments seek to acquire control over strategic sectors of the Canadian economy, it can represent a threat to Canadian security interests. National security concerns related to foreign investment in Canada will continue to materialize, owing to the prominent role that SOEs are playing in the economic strategies of some foreign governments.

-Canada is also a target for our political and military intelligence. Canadians sometimes make the mistake of underestimating the relevance -- to foreign governments -- of the information we have. We are a founding member of NATO, a signatory to a number of other multilateral and bilateral defence agreements, and a close strategic partner of the United States -- all of which makes us an attractive target for espionage.

Slide 7 – Information Security Threats

- CSIS defines a cyber-related attack as the use of information systems or computer technology as either weapon or target

- Threats to Canada's soft energy critical infrastructure can emanate from foreign states, terrorists, hacktivists and others

Speaking Points

-Computer technologies are in a constant state of development, and the moment they are developed, they are adopted -- by both the public and private sectors. This rapid process of adoption does not come without risk. The pace of technological advancement affords new opportunities for cyber attackers as it exposes new vulnerabilities and creates new victims.

-Consider the Stuxnet computer virus, which reportedly sabotaged Iran's nuclear program in 2010. What was so ingenious about the Stuxnet is that –according to open source reports – it was programmed to disguise the sabotage as it occurred. Now, we might not be so alarmed in this particular instance because the target was Iran, not exactly a friend of the West. But technologies themselves don't discriminate between good guys and bad. What if a similar attack were aimed at Alberta's energy infrastructure?

- Or consider the blackout of August 2003. It affected some 50 million people across Ontario and much of the northeastern US – and it was not even the result of a deliberate attack. It did, however, highlight the vulnerability of technologically advanced societies.

-With the right technology, someone or some foreign power can disrupt our way of life in profound ways, stealing our knowledge or sabotaging our infrastructure, without ever coming into our country or even near our shores.

Slide 10 – What can we do?

- Education
- Partnership

Speaking Points

-Today's presentation is part of a larger effort at CSIS to engage important sectors such as yours. We like to say that just because we are the keeper of secrets doesn't mean we have to be a secret organization. It's important for us to talk about who we are and the work we do, and to help Canadians identify their -- our -- shared security interests.

-We have established a Liaison Awareness Program that is administered out of our regional offices, and it covers a broad range of security issues. The program is designed in part to provide corporate partners with information on the risks that they face and that, in turn, the country faces. We can provide security awareness briefings that address specific concerns about business travel. And where appropriate we work with other government departments to brief private sector representatives on threats such as terrorism, espionage and weapons proliferation.

-We can share with you some of the most common covert methods used by those engaging in economic espionage, and we also can talk about threats to information security. By using recent examples of computer intrusions we can illustrate the danger posed to computer and telecommunications systems.

-These developing relationships, we hope, will not be a one-way dialogue. We feel we also can benefit from the insight and experience of our partners. The entrepreneurial or private sector community has its own considerable expertise in risk assessment, and has much to contribute to the dialogue about threat management and mitigation.

There are many ways for us to work together, both in Canada and in theatre, which would be of benefit not just to my organization and your industry, but to Canada generally.

-Thank you again for the invitation and I'm happy to take any questions.

PROTECTED
520-301-21
2007 07 11

POST-CONFERENCE REPORT:
Unclassified Security Briefing for the Canadian Association of Petroleum Producers

SUBJECT

On 2007 03 06, in Calgary, Alberta, the Canadian Association of Petroleum Producers (CAPP) hosted an unclassified security briefing forum. In order to faciliate this forum, CAPP requested the Energy Infrastructure Protection Division (EIPD),Natural Resources Canada, to cosponsor and assist in the delivery of various presentations.

CSIS was represented by

DISCUSSION

Panel Discussions:

- The International Geo-Politics of Energy Vulnerabilities, Risks and Protective Security by Prof. Martin Rudner, Director, Canadian Centre of Intelligence and Security Studies (CCISS), The Norman Paterson School of International Affairs, Carleton University.
- Radicalization: Homegrown Terrorism in Canada by Ms. Angela Gendron, Senior Fellow at CCISS.

CSIS Comment:
Rudner / Gendron presented a brief history of Al Qaeda based on "Penetrating Terror Threats - Counter Intelligence as Counter Terrorism: 1) evolution of AlQaeda; 2) Al Qaeda's 20 years strategic plan; 3) Al Qaeda's Intelligence Manual; 4) Penetrating Adversaries; and 5) Lessons that need to be learned. Although the audience indicated they were aware of some of these issues, they did appreciate receiving a complete package approach.

- The Relationship Between Law Enforcement, Intelligence and the Private Sector by Phil Murray, Retired Commissioner, RCMP.

Presentations:

Presentations were given by the RCMP, CSIS, ITAC, SIM, PSEPC, NEB and the EUB on issues dealing with oil and energy security issues as they relate to each organization. CSIS notes are contained herein.

General Comment:
This was an excellent forum to meet members of the Canadian Association of Petroleum Producers. It opened doors and facilitated a better understanding of each other`s concerns.

Prepared by:

PROTECTED
520-301-21
2007 07 11

Canadian Association of Petroleum Producers (2007 03 06) **UNCLASSIFIED**

Facilitated Panel Discussion 1

Roles and Responsibilities

- Good morning and thank you for the opportunity to speak to you on behalf of CSIS.
- Our Director recently addressed the very issue we are here to talk about - the ability of the Canadian Security Intelligence Service to communicate differently and with a range of stakeholders.
- Not just the traditional clients for security intelligence advice - the Privy Council Office, foreign affairs and national defence, the police, the courts, border and immigration officials, and other agencies of the national security community.
- At the Canadian Association for Security and Intelligence Studies (CASIS) meeting last fall, Director Judd identified public communication as one of several critical areas in which CSIS has to adapt or accelerate changes already underway if the Service is to succeed as an innovate business in an increasingly unforgiving security environment.
- Quote - "In the realm of public communications, it is increasingly important for us to be able to explain both what we do, and what we do not do, and how. While there will always be limits on what we can and cannot discuss publicly, there is a clear imperative for a better understanding of an organization such as ours and the misconceptions that often surround our work."
- Key areas of responsibility, concentrating on those pertinent to today's forum.

National security investigations

- Mandated to investigate, analyse, report to and advise the Government of Canada on threats to the security of Canada: espionage, sabotage, clandestine foreign influence and terrorism:
  - investigates activities of foreign governments that engage in economic espionage - use of clandestine, coercive or deceptive means by a foreign government or its surrogates which jeopardize Canadian competitiveness, intellectural property and investments in research and development.
- Advise federal government departments, such as NRCan, one of our key clients.
- Specifically, the Service's "threat and risk assessment program" has a working relationship with the Energy Infrastructure Protection Division, as does Security Screening in the realm of clearances.
- The TRA program, that I manage, has evolved exponentially, post 9/11, which I will address this afternoon.

Security clearances

- CSIS is mandated to provide security assessments, on request, to all federal departments and agencies, with the partial exception of the RCMP, which receives CSIS information,

but conducts its own clearances for RCMP personnel.

- Security assessments are required for all federal employees, who in the course of their duties, will require access to information or assets classified in the national interest.
- Purpose - to appraise the loyalty to Canada, and reliability as it relates thereto, of government employees - assess if a person may represent a security threat.
- Increasingly since 9/11, this government's security clearance function has expanded to include personnel in the private sector who require access to restricted areas, or to information classified in the national interest.
- "Site-access" assessments of individuals seeking employment at airports and nuclear power stations and in the parliamentary precinct:
  - helps to ensure that individuals with terrorist connections do not obtain access to our country's sensitive sites or classified information
  - programs managed by client departments - Transport Canada, the Canada Border Services Agency, the Canadian Nuclear Safety Commission, NRCan for energy sector writ large.
- Assists CBSA and Department of Immigration in preventin the entry to Canada of persons known or suspected of being involved in espionage, proliferation or terrorism.
- Assessments of the risks applicants for status in Canada may pose to the security of Canada are prepared according to standards set by the *Immigration and Refugee Protection Act* and the *Citizenship Act*.

- This is a integral step in ensuring that due diligence has been conducted to safeguard Canadian interests.

Working relationships - our role

- Work closely with members of the security and intelligence community, and with federal, provincial and municipal law enforcement agencies, as well as foreign partners.
- Develop effectuve liaison information sharing arrangements with NRCan, specifically with the Energy Infrastructure Protection Division (EIPD), and portfolio agencies of the department.
- CSIS meets annually with security officials from the Canadian nuclear industry for threat briefings and discussions.
- NRCan's Energy Infrastructure Protection Division (EIPD) coordinates twice-yearly classified briefings (each May and November) for energy stakeholders - oil and gas, nuclear energy, offshore, and electricity, from production to distribution.
- CSIS is an active partner in these briefings, at a SECRET level.
- In Alberta, CSIS regional offices (Calgary, Edmonton) are well positioned to observe and contribute to the information and intelligence sharing arrangements with key regulatory

and intelligence players:

- Alberta Energy and Utilities Board (EUB)
- Alberta Security and Strategic Intelligence Support Team (ASSIST)
- Industry associations such as the CAPP, the National Energy Security Professionals (NESP), and officers within member corporations.

- In Canada, CSIS has memoranda of understanding, and maintains close working relations with the police of jurisdiction.
- In many instances, this means the RCMP, which is the lead agency for criminal investigations of national security offences.
- CSIS may disclose information obtained in the performance of its duties and functions to a police officer of jurisdiction when the information may be used in the investigation or prosecution of an alleged contravention of any law of Canada.
- Just how essential these relationships was evident during the press conferences surrounding the arrests in Toronto last summer: every police force in the greater Toronto area from Durham to Peel had a role in the prevention of terrorist acts.
- Our information sharing with foreign partners is critical to the Service's capacity to deliver on its mandated responsibilities, as well as responding to crises, such as providing intelligence support to the rescue of hostages in Iraq, or evacuating Canadian citizens from Lebanon.
- I have focussed on those roles/responsibilities that directly impact on how the Service relates to the energy sector, which includes you, the stakeholders.
- Although there is a need for intelligence warning, we also need to concentrate on building and nurturing trusted networks.
- From my colleagues in our Edmonton and Calgary offices, I know that you already have good, solid networks and relationships in place.
- The reality of today's global environment will be the driving force in maintaining these.

Additional points (if time allows / panel discussion)

A transformed national security environment

- In recognition of the unprecedented extremist threat to public safety, the Service is a partner in the Integrated National Security Enforcement Teams (INSETs), and Integrated Border Enforcement Teams (IBETs).
- This ensures that intelligence producers and consumers - those who advise on, and those who protect against - terrorist threats have every necessary means of communication and cooperation in implementing their specific responsibilities.
- Under the authority of the Ministers of Public Safety and Foreign Affairs, CSIS has intelligence sharing partnerships, and/or security vetting arrangements, with countries in every sector of the globe.
- The ability to operate outside Canada in support of our core is another of the critical business challenges identified by our Director.
- National borders are only peripherally relevant to the vast majority of threats we now deal with, or the risks to Canadians, either at home or outside Canada.

From national security to critical infrastructure protection

- Among the most significant transformations in the national security community post 9/11, is the transformation from the centralized, top-down, secret and closed world of national security, to the horizontal, multi-partner and increasingly transparent world of critical infrastructure protection.
- On the 'threat-from' side, aka - traditional espionage, the business of intelligence collection would be recognizable to any intelligence officer from the Cold War.
- While the tools of the trade - and the targets - have become more sophisticated, and the scope of the Service's activities more international, our methodology remains basically the same - acquiring intelligence, by necessary and legal means, into the intentions of capabilities of those who pose a threat to the security of Canada.
- It is on the intelligence production side - the 'threats-to' side of the equation that the real transformation is taking place.
- Corporations accustomed to regulation in light of accidents and naturally-occurring hazards are unexpectedly forced to protect their business operations and do their business recovery planning in light of transnational threats to critical infrastructure (their own and others).
- This is fuelling the demand for enhanced information and intelligence sharing - and not just in the energy sector.

Bringing in the private sector

- Critical infrastructure is overwhelmingly in the private sector.
- It is hardly surprising, therefore, that the old intelligence model developed for the Cold War, is under stress as the political executive and key intelligence agencies adapt to a new

world order very different from the one envisaged during the 1990s.

- The 1990s was the decade of the 'peace dividend', during which responsible governments exacted the dividend - often meaning significant cuts to the defence and national security communities.
- In the post-9/11 world, the decade of the 1990s now seems more remote than the Cold War which preceded it.
- As should be evident from recent media coverage, the usual suspects for foreign espionage are as aggressive and active as they have ever been against Canada,

- With all the understandable emphasis on the threat of terrorism, we should not lose sight of the fact that threats of espionage, including theft of intellectual property and attempted theft of classified assets, are serious security concerns to Canada.

Summary

- CSIS works with an extraordinary range of organizations in Canada and abroad to fulfill our mandate.
- This has increased our contact with federal departments and agencies outside the traditional S&I community, other levels of government, and with the private sector.
- None of us should be surprised by the significant expansion of the number of clients on the intelligence distribution lists, or the increased use of Unclassified For Official Use Only reporting as means of getting the intelligence product out as quickly as possible to those with a need to know.
- These developing arrangements are the corollaries from the shift mentioned earlier from the self-contained national security community to critical infrastructure protection.

Canadian Association of Petroleum Producers (March 6, 2007) **UNCLASSIFIED**

Facilitated Panel Discussion 2

What are the real risks to industry?

- Intelligence product is the return on CSIS' investment in collection and analysis, and reflects the Service's own risk management in allocating scare and often specialized resources across competing programs (counter-terrorism vs counter-espionage; security intelligence investigations vs government and immigration screening;) and against specific targets.
- Although I'll speak to terrorism, domestic extremism and espionage threats, ITAC will provide you with an in-depth perspective on the terrorism threats to the energy sector.
- International terrorism is not new - it has been with us now for four decades, beginning with the attacks in 1968 by Palestinian terrorists on civil aviation targets - the hijacking of aircraft and armed assaults on international airports.
- Until 9/11, the bombing of Air India was the most lethal incident of international terrorism.
- The Air India bombing, horrific as it was, did not transform the Canadian security intelligence community or its relations with the private sector - civil aviation had long been a terrorist target of choice, and in this attack Canada was venue for the spillover of terrorist violence from a conflict rooted in the homeland.
- Today, there is a fundamental shift in the nature of the threat.
- We have moved beyond indirect threats of the spillover of violence from conflicts abroad, to a direct - and unprecedented - terrorist threat against Canada, its allies and global interests.
- Al Qaeda's strategic vision includes attacking the energy sector, disrupting US energy supplies and driving up the price of oil.
- Key link between Al Qaeda's strategic vision and homegrown extremism is the Internet.
- Parts of the world wide web offer both basic and advanced degrees in terrorism for free.
- The Internet is a multi-faceted facilitation tool which allows extremists to communicate, proselytize, radicalize, recruit, raise funds, learn how to make improvised explosives and detonators, and collect information on potential targets.
- That there has not been a terrorist attack in North America since 9/11 is no basis for complacence - this is an open-ended conflict against a continually mutating threat.
- It is, however, a positive indicator that North America is a difficult operating environment for terrorists.
- And yes, we have been successful in diffusing several potential threats - the most notable in June 2006 in Toronto.
- Others, we cannot talk about.
- While there is never going to be a 100% surety against an attack taking place, the purpose of the security and intelligence community's outreach to other levels of government and

to the private sector is to ensure that Canada becomes an increasingly difficult operating environment for those who would do us harm, whether it be terrorism, espionage or domestic extremism.

- So much of the discussion tends to be on the issue of terrorism for obvious reasons, however, we should not lose site of security issues that are more likely to be of concern to energy stakeholders.
- Domestic extremists are emerging from their post 9/11 introspection.
- Recall the mass anti-globalization protests in Seattle, Quebec City and Rome.
- In North America, these evaporated and while the extremists never went away, the domestic security environment remained relatively quiescent for some time.
- There are signs this is changing, particularly among aboriginal and environmental extremists, there is a rediscovered militancy.
- This already has been evidenced in Caledonia, Ontario and the impact on Hydro One's operations.
- Energy stakeholders also need to be concerned with national security threats from foreign governments and transnational criminal groups.
- Foreign countries continue to use their intelligence services to covertly achieve their goals in their own national interest.
- Transnational criminal organizations and the illicit funds generated from their illegal activities pose a significant threat to Canada's economic security.

- The Service provides intelligence support to NRCan in
and will work with the private sector as appropriate in countering these threats.
- How do we leverage the operational capacity of an intelligence service and its partners in the federal security and intelligence community into enhanced security of assets in the private sector?
- As an investigative agency, CSIS is focussed on where the threats are coming from.
- For a facility owner-operator, the issue is threats to the facility, including personnel and essential services that enable operations to continue.
- While the Service's 'threats-from' focus will always remain central to our operations, CSIS, the RCMP and other agencies of the S&I community are increasing their knowledge of critical assets at risk, vulnerabilities of concern, and the security counter measures available.
- In this translation of 'threats-from' intelligence analysis into 'threats-to' advice to clients we have the basis of a dialogue between those with the capacity to advise on threat actors' capabilities and intentions, and those with the knowledge and expertise to deliver essential services safely.
- The 9/11 attacks changed the definition of national security to include critical infrastructure.

- CSIS has produced dozens of threat and risk assessments.
- Originally, TRAs were designed under the Government Security Policy to assist departmental security officers to meet heir obligation to protect department assets and personnel.
- Today, the CSIS TRA function responds to requests from departments and agencies for advice on the national security implications of policy decisions and regulations.
- Herein lies the nexus to our rapidly expanding list of clients for the Service's intelligence product and the connection to the private sector.
- Our threat assessments are tactical in scope; current intelligence intended to provide other government departments, the law enforcement and protective security communities of potential threats arising from incidents in Canada or abroad, to Canadian or foreign dignitaries, special events or the potential for violence arising from protests and demonstrations.
- We provide security advice via threat and risk assessments, which includes all threat domains as stated in the *CSIS Act*.
- These are prepared for government departments, thematic issues - such as energy, transportation, health.
- While there has been a great deal of angst about the lack of information sharing, in the case of the recent arrests in Toronto, there was specific information sharing months before the arrests.
- As to the sharing of non-specific information, the Service is represented in a variety of forums involving the private sector in ways entirely unexpected even ten years ago.
- While the Service will always be limited in what it can say publicly, we expect to continue on the path of enhanced liaison and informed discussions with you.
- This morning's session and this panel have allowed me the opportunity to provide you with a very quick tour of the CSIS view of international security environment, transformations affecting the way we do business, insight into how the Service must adapt, not so much in our intelligence operations, as in our public communication, community outreach and building partnerships. I hope you found it useful. Thank you.

Trip Report Summary – Presentations to CAPP May 2011
SUBJECT
Presentation to Canadian Association of Petroleum Producers (CAPP) Chief Information Officer (CIO) Forum
UNIT / SECTION / THEME

ISSUE
On 2011 05 09, provided the CAPP CIO Forum with an unclassified presentation on cyber-related issues in Calgary, Alberta. The meeting involved participation by AltaGas Ltd., Cenovuous Energy Inc., Compton Petroleum Corp., Crescent Point Energy Corp., Devon Canada Corp., Encana Corp., Imperial Oil Resources, Penn West Petroleum, Quick Silver Resources Canada Inc., Spectra Energy Corp., Talisman Energy Corp., and Manager, Health and Safety, CAPP, all of whom were very interested in cyber- and SCADA related issues.

Please find below a summary of discussions / action items out of the Director's visit to PR last week (April 11-13th).
Excerpt:
Meeting with CAPP: The Director left with CAPP President It was noted that CAPP has a Cyber Security network/effort for/between its members.

Energy and Utilities Sector Network Meeting - 2009 11 13
Chair, Mr. Kevin Stringer,
DG Petroleum Resources Branch, NRCan

1. On 2009 11 13, attended the Energy and Utilities Sector Network (EUSN) meeting convened by NRCan under the auspices of the GoC National Strategy and Action Plan for Critical Infrastructure Protection (NSAPCIP). EUSN meetings to energy sector stakeholders, including private sector representatives from the electricity and petroleum sub-sector, their associations and the NRCan portfolio - regulatory agencies. Discussions are unclassified.

2. Energy Sector Network: Within the Public Safety Canada (PSC) - National Strategy for Critical Infrastructure, each of the 10 sectors are to develop a sector network to include key public and private stakeholders. The strategic objective of these networks is to build trusted and sustainable partnerships to support critical infrastructure resiliency. Given NRCan's pre-existing and well established energy sector network,

3. In addition to NRCan officials, representatives were: Canada Newfoundland and Labrador Offshore Petroleum Board; Canadian Association of Petroleum Producers (CAPP); Canadian Gas Association (CGA); Canadian Electricity Association (CEA); North America Electricity Reliability Corporation (NERC); Hydro One; National Energy Board (NEB); Newfoundland Transshipment Limited (NTL); Government of Alberta (via telephone); (Academia); Public Safety Canada; RCMP and CSIS.

4. The meeting was chaired by Mr. Kevin Stringer, DG, Petroleum Resources Branch, NRCan. Mr. Stringer advised that: he was pleased with the Auditor General's report and specifically thanked the RCMP and the private sector for their contributions. NRCan's priorities are mapping and conducting table top exercises.

5.

6.

7.

8.

9.

16.

Annex A:
Strategic Considerations for CSIS Federal Partners in Critical Infrastructure Protection[3]

Strategic Considerations for Sector Networks:

17. CICI participation within the Energy Sector Network is important because: NRCan specifically requested that the RCMP be a permanent member of the Energy Sector Network.

18. Sector Network Meetings are valuable forums to establish a clear delineation of roles, responsibilities, and coordination requirements among industry and government for the investigation and reporting of findings, conclusions, and recommendations related to the identification and mitigation/ recovery efforts for threats and other emergencies affecting Canada's energy infrastructure.

19. CICI attendance within these and the other sector network meetings provides it the opportunity to be briefed on real and or potential threats to Canada's CI; participate in the discussions; and assist in the maintenance of the RCMP/private sector cooperative relations.

20. CICI attendance will permit it the opportunity to be briefed on topics of Canada's energy sector interests.

RECOMMENDATION:

I recommend that CICI continue to participate within the Energy Sector Meetings.

T.A. O'Neil
Senior Criminal Intelligence Research Specialist
Critical Infrastructure Criminal Intelligence

Strategic Considerations for Sector Networks - Public Safety Canada

21. The Strategy recognizes that each responsible jurisdiction, department and agency, as well as private sector infrastructure owners and operators, will exercise their responsibilities as they deem appropriate for strengthening the resiliency of Canada's critical infrastructure. To be effective, however, implementation of the Strategy will require the collaboration of federal, provincial, territorial and private sector partners and the establishment of mechanisms to facilitate this collaboration.

22. The Strategy proposes to establish a sector network for each of the critical infrastructure sectors. This approach would build to the fullest extent possible upon existing coordination and

---

[3] Derived from the RCMP briefing note on the value of the Force's participation in the Energy and Utilities Sector Network.

consultation mechanisms. In recognition of the unique characteristics of each sector, the Strategy does not prescribe the structure of each sector network. At a minimum, the sector networks should support critical infrastructure protection by providing standing fora for discussion and information exchange among partners.

23. Working with these critical infrastructure partners, each lead department would facilitate the development of sector networks to suit the needs of their stakeholders. The Strategy provides a framework for the possible functions of the sector networks, including:

- promotion of timely information sharing;
- identification of issues of national, regional or sectoral concern;
- use of subject-matter expertise from both the public and private sectors to provide guidance on current and future challenges; and
- development of tools and best practices for strengthening the resiliency of critical infrastructure across the full spectrum of prevention/mitigation, preparedness, response and recovery.

24. The sector networks will be composed of relevant federal departments and agencies, provinces, territories and key members of the private and public sectors. Participation in these networks will be voluntary. To facilitate the exchange of information, critical infrastructure partners will collaborate to develop a protocol to safeguard information shared through these networks.

POST-CONFERENCE REPORT:
Unclassified Security Briefing for the Canadian Association of Petroleum Producers

SUBJECT

On 2007 03 06, in Calgary, Alberta, the Canadian Association of Petroleum Producers (CAPP) hosted an unclassified security briefing forum. In order to faciliate this forum, CAPP requested the Energy Infrastructure Protection Division (EIPD),Natural Resources Canada, to cosponsor and assist in the delivery of various presentations.

CSIS was represented by

DISCUSSION

Panel Discussions:

ÿ The International Geo-Politics of Energy Vulnerabilities, Risks and Protective Security by Director, Canadian Centre of Intelligence and Security Studies (CCISS), The Norman Paterson School of International Affairs, Carleton University.

ÿ Radicalization: Homegrown Terrorism in Canada by Senior Fellow at CCISS.

CSIS Comment:

presented a brief history of Al Qaeda based on "Penetrating Terror Threats - Counter Intelligence as Counter Terrorism: 1) evolution of AlQaeda; 2) Al Qaeda's 20 years strategic plan; 3) Al Qaeda's Intelligence Manual; 4) Penetrating Adversaries; and 5) Lessons that need to be learned. Although the audience indicated they were aware of some of these issues, they did appreciate receiving a complete package approach.

ÿ The Relationship Between Law Enforcement, Intelligence and the Private Sector by Phil Murray, Retired Commissioner, RCMP.

Presentations:

Presentations were given by the RCMP, CSIS, ITAC, SIM, PSEPC, NEB and the EUB on issues dealing with oil and energy security issues as they relate to each organization. CSIS notes are contained herein.

General Comment:

This was an excellent forum to meet members of the Canadian Association of Petroleum Producers. It opened doors and facilitated a better understanding of each other`s concerns.

Prepared by:

CAPP Briefing

Presentation by the Director of the
Canadian Security Intelligence Service to the
Canadian Association of Petroleum Producers
April 12, 2012

Who We Are

- Our members come from across Canada and include intelligence officers, analysts, computer scientists, technicians, linguists, and other specialties.
- CSIS was created in 1984 by an Act of Parliament.
- Our mandate is to collect, analyse and report -- to government -- information about threats to Canada and Canadian interests.
- We are a civilian agency. The government conferred on us a broad investigative scope.
- CSIS investigates activities that may on reasonable grounds be suspected of constituting threats to the security of Canada.
- The Service is not a police force and does not collect evidence.

Where Does the Service Conduct its Business?

- CSIS operates mainly inside Canada but in a globalized world the service also maintains an international presence.

- The Service can collect intelligence on threats to the security of Canada anywhere in the world but can only collect political and economic intelligence on foreign governments within Canada.

- CSIS is mandated to collect and analyze this intelligence.

What are the Priority Threats?

- **Terrorism** – investigating the threat or use of violence for the purpose of achieving political, religious or ideological objectives.

- **Espionage and Foreign Interference** - Investigating clandestine activities by foreign governments in Canada that may be detrimental to Canada's technological, economic, cyber, military and commercial interests, as well as classified government information.

- **Information Security Threats** - Investigating threats to Canada's critical information systems and infrastructure directed by foreign countries, terrorist and extremist groups, as well as other private-sector actors .

- **Proliferation of Weapons of Mass Destruction** - Investigating foreign states and terrorist organizations that are developing, producing, or acquiring weapons of mass destruction using Canadian technology and know-how.

CSIS and Threats to Canada's Energy Security

The Service's responsibility for Canada's energy security falls into four categories of threats:

- Threats to hard energy infrastructure assets from terrorism and domestic extremism.
- Threats to soft energy infrastructure assets (i.e. cyber systems) from foreign states, terrorists, domestic extremists and hackers, and proprietary information, know how and business and market information from cyber espionage.
- Threats to Canada's energy industry and markets from clandestine and deceptive foreign influence and interference.
- Threats to Canada's energy industry, assets and personnel abroad.

Al Qaeda Core and its Affiliates

- AQ and the "Single Narrative".
- Global & Local Jihad.

- Encouraging Small-Unit and Lone-Actor Actions.
- Striking abroad: AS, AQI, AQIM, AQAP.

West Africa & the Arabian Peninsula

- Boko Haram in Nigeria.
- AQAP.

Radicalization

- Home-grown;
- Travel to war-zones;
- Increasing role of females.

Domestic Extremism

- Left -Wing Extremism;
- Right-Wing Extremism;
- Aboriginal Extremism.

Cyber and Threats to Critical Infrastructure

- Ubiquitous.
- Connectivity leads to Exploitable Vulnerability
- Force multiplier.
- Anonymous and Hacktivism

Transformation in the Middle East

- Tunisia, Egypt, Libya, Syria, and Yemen.
- "Arab Spring" – Non-ideological, cross-generational movements.
- Not inspired or influenced by Al Qaeda.
- Al Qaeda seeking to exploit the uncertainty.

The Canadian Security Intelligence Service

Protecting Canada and its interests

Who We Are

- Canada's National security intelligence agency
- *CSIS Act* (1984)
- CSIS is a civilian organization
- No power to arrest or detain

CSIS Operations

- CSIS investigates, collects, analyses and reports – to government – information about threats to Canada and Canadian interests

- The primary focus of CSIS activities are on:
  - Terrorism
  - Espionnage and Foreign Interference
  - Information Security Threats
  - Proliferation of Weapons of Mass Destruction

- CSIS operates mainly inside Canada but also maintains a significant international presence

Terrorism

- Al Qaeda and Its Affiliates
- Radicalization and "Home-grown" Terrorism

Domestic extremism

- Energy sector as an attractive target
- From peaceful to violent protest

Espionage and Foreign Interference

- CSIS investigates clandestine activities by foreign governments in Canada that may be detrimental to Canadian interests

- Why is Canada a target?
  - Expertise
  - Support global acquisitions and investments
  - Support state-owned enterprises (SOEs)

Information Security Threats

- CSIS defines a cyber-related attack as the use of information systems or computer technology as either weapon or target

- Threats to Canada's soft energy critical infrastructure can emanate from foreign states, terrorists, hacktivists and others

Transformation in the Middle East

- The uncertainty of forecasting
- Optimists and pessimists

What can we do?

- Education
- Partnership