Government Consulting Services

Services conseils du gouvernement

2008-2009 Summative Evaluation of the National Strategy for the Protection of Children from Sexual Exploitation on the Internet

Prepared for: Public Safety Canada

FINAL REPORT

Project Number: 570-2735
Program Evaluation and Performance Measurement Services

July 2008

Public Works and Government Services Canada
Travaux publics et Services gouvernementaux Canada
Canada

Table of Contents

List of Acronyms

ADM	Assistant Deputy Minister
AICEC	Advanced Internet Child Exploitation Course
C3P	Canadian Centre for Child Protection
CCAICE	Canadian Coalition Against Internet Child Exploitation
CEOP	Child Exploitation Online Protection Centre
CETS	Child Exploitation Tracking System
CANICE course	Canadian Internet Child Exploitation Course
CNA	Customer Name and Address
CWG	Cybercrime Working Group
ERC	Expenditure Review Committee
DOJ	Department of Justice
ESP	Electronic Service Provider
FPT	Federal/Provincial/Territorial
IBCSE	Internet-based Child Sexual Exploitation
IC	Industry Canada
ICAC	Internet Crimes against Children
ICE	Integrated Child Exploitation (unit)
INHOPE	International Association of Internet Hotlines
ISP	Internet Service Provider
IWG	Interdepartmental Working Group
IWGTIP	Interdepartmental Working Group on Trafficking in Persons
KIK	Kids in the Know
KINSA	Kids Internet Safety Alliance
NCECC	National Child Exploitation Coordination Centre
NCMEC	National Centre for Missing and Exploited Children
NGO	Non-government Organization
OCSET	Australian Federal Police Online Child Sex Exploitation Team
OIC	Officer in charge
P2P	Peer to peer
PIPEDA	*Personal Information Protection and Electronic Documents Act*
PS	Public Safety Canada
PSC	Project Safe Childhood
RCMP	Royal Canadian Mounted Police
RMAF/RBAF	Results-based Management and Accountability Framework / Risk-based
Strategy	National Strategy for the Protection of Children from Sexual Exploitation on
TBS	Treasury Board Secretariat of Canada
VIU	Victim Identification Unit
VGT	Virtual Global Taskforce
YCWW	Young Canadians in a Wired World

[*] - In accordance with the Privacy and Access to Information Acts, some information may have been severed from the original reports.

Executive Summary

i) Introduction

The National Strategy for the Protection of Children from Sexual Exploitation on the Internet (hereafter referred to as the Strategy) is a horizontal initiative providing a comprehensive, coordinated approach to enhancing the protection of children on the Internet and pursuing those who use technology to prey on them. A total of $42 million over five years, beginning in 2004-2005, was allocated to three partners to implement the Strategy[1]. The table below lists the Strategy partners and summarizes the funding that was provided for each partner.

Strategy Partner	**Funding Level over Five Years**
Royal Canadian Mounted Police (RCMP)	$34.34 M
Industry Canada (IC)	$3.00 M
Public Safety (PS) and *Cybertip.ca*[2]	$4.70 M
TOTAL	**$42.04 M**

Under the Strategy, the general expectations and desired achievements of each partner were as follows:

- the RCMP was to expand the current capacity of the National Child Exploitation Coordination Centre (NCECC);
- IC was to expand their School Net Program and forge partnerships with industry and Non-government Organizations (NGOs);
- PS was to enter into a contribution agreement with Child Find Manitoba (now the Canadian Centre for Child Protection (C3P)) for the purposes of operating and expanding *Cybertip.ca*, Canada's national tipline for reporting suspected cases of child sexual exploitation and, as the lead department for the Strategy, to coordinate, oversee and evaluate the Strategy.

Under PS lead, and through the collaboration of all partners, a *Results-based Management and Accountability Framework* and *Risk-based Audit Framework* (RMAF/RBAF) was prepared for the Strategy. During the four years since inception, Strategy activities and funding have evolved and expanded in scope leading to a progression of the initiative design that was not anticipated at the outset. For example, the $1 million in each of the fiscal years 2007-08 and 2008-09 that had been profiled for IC for *CyberWise.ca* activities was re-directed to PS, who, in turn, directed some of the funding to *Cybertip. ca*. The Strategy also received an additional $6 million per year in funding, announced in Budget 2007, to enhance existing initiatives to combat child sexual exploitation and trafficking.

[1] The National Strategy itself contained five broad objectives; however, the Strategy received funding for only three objectives. The five objectives of the National Strategy are as follows: *1)* enhance law enforcement capacity; *2)* provide for public education and reporting; *3)* forge partnerships with industry and non-governmental organizations; *4)* ensure relevant legislation and public reporting; *and, 5)* engage in research and analysis. (objectives 4 and 5 were unfunded)

[2] *Cybertip.ca* received funding through a contribution agreement managed by PS.

PS coordinated a formative evaluation of the Strategy in 2006-07[3]. The summative evaluation assesses the continuing relevance of the Strategy; the overall impact and success of the Strategy; cost-effectiveness and alternatives; and aspects of the design and delivery of the Strategy related to governance and progress against the recommendations of the formative evaluation. It covers a four-year period from the receipt of Strategy funding in April 1, 2004 to March 31, 2008.

ii) Summary of Conclusions

The paragraphs that follow summarize the conclusions contained in the body of this report.

1. Overwhelming evidence suggests a continued need for a national strategy to combat Internet-based Child Sexual Exploitation (IBCSE). The problem of IBCSE has not diminished; rather it continues to be prevalent and expanding in Canadian society. Thus, it remains relevant and in the public interest to address this issue. Interviews and studies conclude that the Internet and technology are pervasive in children's lives, and because of this, offenders have increased access to potential victims. Technological advancements have enabled sophisticated methods for offenders to conceal their identities and to continue to offend, leading to the emergence of new forms of IBCSE.

2. The number of IBCSE cases being processed has increased, and *Cybertip.ca* and the NCECC are forwarding more cases to law enforcement. Evidence from interviews suggests that law enforcement at the field level is lacking skilled investigators and forensics support. However, it should be noted that the responsibility for field level resources rests with provincial and municipal governments.

3. The Strategy is built on a partnership approach that involves all levels of government, NGOs and the private sector. The roles and responsibilities, as they are delineated under the Strategy are appropriate. The federal government continues to play an essential role in the fight against IBCSE. Efforts of partners have been well-coordinated by PS, and the central coordinating role of the NCECC is key to a national strategy to combat IBCSE.

4. Original governance mechanisms as laid out in the RMAF/RBAF have evolved. There has been no requirement for the envisioned Assistant Deputy Minister (ADM) Steering Committee. The National Steering Committee is being revitalized and work of the Interdepartmental Working Group (IWG) has been well-coordinated by PS on an as-required basis. PS has also brought a degree of strategic planning to the Strategy through the redesign of the logic model, participation in national and international working groups and the development of cabinet documents to address changing needs. Further advancement of a strategic agenda and continuing to remain abreast of emerging issues is an important role of PS. There is a need for further engagement of the IWG in areas such as communications (public awareness), and research. In addition, there is still work to be done in developing awareness of other groups involved in public education efforts (outside the Strategy) so that the Strategy can realize synergies and avoid duplicating the efforts of others. Working level governance through the Integrated Child Exploitation (ICE) Officer in Charge (OIC)

[3] The final report was dated June 2007.

meetings is functioning very well although some participants would like to see longer meetings because of the significant travelling distance.

5. The Strategy has been successful in increasing the knowledge of target audiences in the areas of investigative challenges, best practices and measures to overcome challenges. This outcome is directly attributable to the efforts of the Strategy. For law enforcement, training and the NCECC Annual Conference are the strongest contributors to success in this area. Raised awareness of judicial partners, such as provincial crown prosecutors, is attributed mainly to participation in the Federal Provincial Territorial (FPT) Cyber-crime Working Group (CWG). Raised awareness among Internet Service Providers (ISPs) is attributed mainly to work on Canadian Coalition against Internet Child Exploitation (CCAICE). Remaining work includes: continued training on trends in sex offender methods, Internet usage among youth and training on investigative techniques for law enforcement; education on the nature of the crime among judicial partners, and continuing awareness efforts on legal issues with ISPs.

6. Law enforcement collaboration and information sharing has been enhanced a great deal through the NCECC Annual Conferences, investigative support from the NCECC, and through the building of international relationships. Information sharing has been well coordinated by the NCECC through the provision of high quality investigative packages. Limited buy-in of the Child Exploitation Tracking System (CETS) by some law enforcement agencies and the fact that the image database has not been implemented is hindering information sharing. The NCECC Technology Section continues to address detracting issues.

7. Through the efforts of the NCECC and the work of *Cybertip. ca*, the Strategy has contributed to coordinated, comprehensive and efficient investigations. NCECC provides a single point of contact from which complete investigative packages are sent to the appropriate jurisdiction. *Cybertip.ca* has also realized efficiencies and taken the burden off of police by triaging complaints and forwarding complaints requiring follow-up directly to local jurisdictions. The NCECC has reduced backlog and is achieving targeted turnaround times. Despite this success, some investigations are being hindered by lack of cooperation from ISPs in providing responses to Customer Name and Address (CNA) requests which renders an investigation un-actionable.
8. The work of the Canadian Centre for Child Protection (C3P) has greatly contributed to enhanced awareness among the general public. This is evidenced by the marked increases in reporting and educational downloads immediately following campaigns. There is evidence that children and parents are being reached because the Kids in the Know (KIK) program is being utilized in most provinces, and 15% of Canadians are now aware of *Cybertip.ca* as the national reporting tipline. In terms of reach, the Billy educational kit has been distributed in Ontario, Alberta, B.C. and Quebec. Evidence indicates that the kit is effective and will be used again by teachers. Limited anecdotal evidence suggests that behaviours have changed as a result of these educational efforts. Educational efforts, geared toward health care professionals and ISPs, are underway but this remains an area that requires continuing improvement. Positive results of a broad-based survey of Canadians would further solidify these findings and provide understanding as to whether awareness activities have resulted in preventative behaviours among target groups.

9. Although PS has recently developed a communication plan with participation from all Strategy partners, it appears that some coordination may still be necessary between the RCMP and *Cybertip.ca* in terms of conducting public awareness activities. Document review indicates that there are two communications plans in existence with similar target audiences, one from the NCECC and the other the joint communication plan for the Strategy.

10. From the information provided, it cannot be fully determined whether the Strategy has enhanced the pursuit of suspects; however, it would appear that some progress has been made. Anecdotal evidence indicates that, because of the Strategy, investigators are now able to complete investigations that may not have been completed prior to the Strategy. The NCECC has contributed to 34 arrests while Cybertip.ca reports contributing to 37 arrests. The NCECC statistics are based mainly on case summaries as the NCECC is not able to report on the actual number of individuals arrested as a result of the information sent to law enforcement agencies. It is probable that the figure significantly under represents the number of arrests, charges and prosecutions because many field investigation dispositions have not been completed. In addition, law enforcement agencies are not reporting back on the results of the information that was sent from NCECC.

11. In terms of prevention efforts, offenders have been prevented from accessing child exploitation material through the shutting down of 2,850 websites by *Cybertip.ca* and through the blocking of access to 11,000 URLs through the efforts of project Cleanfeed. It cannot be determined whether or not these efforts contributed to preventing abuse of children but it can be said that it is possible that offenders and the Canadian public have been prevented from viewing offensive material.

12. Protection of children has been enhanced through the identification of 233 victims. These results are not attributable solely to the Strategy since other Canadian law enforcement agencies have contributed to this result. It is also noted that Strategy partners have provided programs to help children build their self-esteem which helps to reduce their vulnerability of victimization. Protection of children could potentially be enhanced through the implementation of the image database originally envisioned as part of the Strategy, but yet to be implemented.

13. There have been no major negative impacts due to the evolution of the Strategy. As the Strategy has evolved, partners have worked well together to address changing needs as they arise. The exception to this is that work on legislative issues has taken a good deal of time away from the day-to-day work of the NCECC meaning that other work has suffered as a result.

14. From the information provided, it has been demonstrated that the Strategy has provided value for money to some extent. For example, monetary donations and donations in-kind have been added to Strategy resources. In 2007-08, for every dollar spent on *Cybertip.ca*, 41 cents in private sector donations was realized resulting in $725,000 in private sector funding. Interviewees generally believe that value has been provided, and PS and *Cybertip.ca* have maintained the value that was provided by IC through the proactive and efficient transfer of

this file and the associated materials. Without further financial and performance information and comparable benchmarks, it cannot be conclusively stated that the Strategy overall has provided value for money.

15. The Strategy has realized efficiencies. Centralized triaging by *Cybertip.ca* and preparation of investigative packages by the NCECC has made work more efficient for field resources. In quantifiable terms, the work of *Cybertip.ca* is estimated to have saved provinces and municipalities at least somewhere between $600,000 and $1,800,000[4] over the last four years. The NCECC is now meeting its turnaround times. Efficiencies due to targeted research could not be quantified but interview evidence suggests that this has been the case.

16. Spending of resources against budgets by Strategy partners is generally within acceptable limits with the exception of the RCMP, which has under spent its budget since 2004-05 by approximately 40%. Approximately 20% of this amount can be accounted for by the fact that the image database is delayed and funding is re-profiled each year to account for the delay. Another factor that may have contributed to under spending is the challenge of recruitment and retention across the RCMP and law enforcement, in general, and in the child exploitation area, in particular, because it is a psychologically demanding field of law enforcement specialization.

17. From a review of other similar initiatives, it appears that the Strategy is a very appropriate response to the identified need. In terms of a general approach to combating IBCSE, work in other countries involves a law enforcement component and an education and awareness component, similar to the Strategy. Also, a partnership approach appears to be good practice.

18. Of the initiatives studied, CEOP provides a model that may warrant further study because of the apparent benefits of an approach that is further integrated than the Strategy. Following this approach may mean integrating additional partners such as: charities that have credible understanding of victims, victim support, guidance counsellors, social workers, and a youth panel. Benefits to this further integrated partnership model are seen to be the ability to use secondments to supplement resources, to receive direct support, and to receive advice and influence from varying perspectives in order to solve the complex problem of IBCSE.

19. The Strategy is considered to be fully implemented, with the exception of the implementation of the image database. In addition, the majority of recommendations from the Formative Evaluation have been implemented; two of the recommendations remain to be completed.

iii) Recommendations

[4] This calculation is based on the estimated time that *Cybertip.ca* has saved law enforcement in triaging 23,000 complaints over the past three years. The range is based on estimates of the average amount of time it would have taken for law enforcement to triage the complaints which was estimated to be between one and three hours per complaint by field level interviewees. If *Cybertip.ca* is taking less time on average per complaint, more savings would be realized. *Cybertip.ca* indicates that it could take as few as 15 minutes per complaint.

The paragraphs that follow summarize the recommendations put forward as a result of the conclusions drawn in the previous section.

1. PS should continue its coordination activities and expand its leadership efforts. To this end, PS should further engage the IWG in coordinating activities related to communications (public awareness) and research. The strategic role of PS should be continued and strongly supported in order for the Strategy to get "ahead of the curve" on the issue of IBCSE. Thus, PS should continue to work with national and international partners to improve collaboration, share best practices and exchange ideas on child sexual exploitation on the Internet. PS should continue to advance dialogue with the provinces and territories on issues of common interest. PS should also continue to demonstrate leadership in advancing strategic planning by coordinating research to keep apprised of developments in technology, trends and emerging issues and sharing the results with interdepartmental working groups, including Strategy partners. (PS)

2. Work on legislative issues has taken a good deal of time away from the day-to-day work of the NCECC meaning that other work has suffered. Given the likely continued participation of the NCECC on legislative issues and on high-profile international working groups, the RCMP should consider how they can manage resources in order to both meet these very important "upper-level" priorities and maintain leadership at the NCECC when resources may be drawn away. (RCMP)

3. There is remaining work to be done in developing awareness of other groups, outside the Strategy, involved in public education efforts. To this end, PS should conduct an environmental scan in conjunction with *Cybertip.ca* and the NCECC to determine what other groups exist and what efforts are being undertaken by these groups in the area of education and awareness in order to realize synergies and avoid duplicating activities. (PS)

4. Education efforts and awareness building activities among law enforcement, judicial partners and ISPs have proven effective in increasing knowledge among stakeholders and should continue. Continued law enforcement training needs include: training on trends in sex offender methods, on Internet usage among youth, and on investigative techniques. Training needs among judicial partners include education on the nature of the crime, and, for ISPs, increasing awareness on legal issues. (all partners)

5. The Child Exploitation and Online Protection (CEOP) Centre model should be further studied to assess the benefits of incorporating additional partners, to understand CEOP's strategic approach to "getting ahead of the issue" of IBCSE, and to assess whether parts of this approach can be applicable in the Canadian context. Recognizing that CEOP is part of United Kingdom law enforcement and as such, can apply the full range of policing powers in tackling the sexual abuse of children, but that it also has a unique structure, it is recommended that the Canadian Strategy explore possibilities of benchmarking performance information against CEOP. (PS/NCECC)

6. Efforts should be made to allocate the 20% of funding that is consistently under spent by the RCMP, to forensics support for investigators. It is recognized that retaining forensic support is

currently problematic for all law enforcement with heavy case loads; however, possibilities include providing a centralized forensics unit, seconding officers from other law enforcement agencies or outsourcing this function to another appropriate unit within the RCMP. It is important to note that control of the funding should remain with the NCECC to ensure that the funding is spent on Strategy activities. (RCMP)

7. The NCECC should be more proactive in collecting and reporting performance information as laid out in the RMAF/RBAF (or revised version thereof) including the number of arrests, the type and number of charges laid and sentences pronounced. More work needs to be done with the field level to enable the NCECC to track this information. (RCMP)

1.Introduction

1.1Presentation of the National Strategy

The National Strategy for the Protection of Children from Sexual Exploitation on the Internet (hereafter referred to as the Strategy) is a horizontal initiative providing a comprehensive, coordinated approach to enhancing the protection of children on the Internet and pursuing those who use technology to prey on them. A total of $42 million over five years, beginning in 2004-2005, was allocated to three partners to implement the Strategy[5]. The table below lists the Strategy partners and summarizes the funding that was provided for each partner.

Strategy Partner	**Funding Level over Five Years**
Royal Canadian Mounted Police (RCMP)	$34.34 M
Industry Canada (IC)	$3.00 M
Public Safety (PS) and *Cybertip.ca*[6]	$4.70 M
TOTAL	**$42.04 M**

Under the Strategy, the general expectations and desired achievements of each partner were as follows:

- the was RCMP to expand current capacity of the National Child Exploitation Coordination Centre (NCECC);
- IC was to expand their SchoolNet Program and forge partnerships with industry and Non-government Organizations (NGOs);
- PS was to enter into a contribution agreement with Child Find Manitoba (now the Canadian Centre for Child Protection (C3P)) for the purposes of operating and expanding *Cybertip.ca*, Canada's national tipline for reporting suspected cases of child sexual exploitation and, as the lead department for the Strategy, to coordinate, oversee and evaluate the Strategy.

Under PS lead, and through the collaboration of all partners, a *Results-based Management and*

[5] The National Strategy itself contained five broad objectives; however, the Strategy received funding for only three objectives. The five objectives of the National Strategy are as follows: *1)* enhance law enforcement capacity; *2)* provide for public education and reporting; *3)* forge partnerships with industry and non-governmental organizations; *4)* ensure relevant legislation and public reporting; *and, 5)* engage in research and analysis. (objectives 4 and 5 were unfunded)

[6] *Cybertip.ca* received funding through a contribution agreement managed by PS.

Accountability Framework and *Risk-based Audit Framework* (RMAF/RBAF) was prepared for the Strategy in order to establish accountabilities, guide performance monitoring, audits and evaluations

1.2 Evolution of the Strategy

During the four years since inception, Strategy activities and funding have evolved and expanded in scope leading to a progression of the initiative design that was not anticipated at the outset.

For example, as per the RMAF/RBAF for the Strategy, a formative evaluation, coordinated by PS, was conducted in 2006-07[7]. The results of the formative evaluation indicated that the Strategy was generally being implemented as planned with few exceptions. However, it was found that activities of the partners had expanded, particularly in the area of international cooperation, interaction with Internet Service Providers (ISPs), and identification of legislative issues. Other needs were also identified that had not been previously funded, such as the need for targeted research and a communication strategy. Several recommendations, including the need to update the RMAF/RBAF were put forward as a result of the evaluation[8], and a Management Action Plan was prepared by PS in collaboration with Strategy partners as a result of the formative evaluation. Most of the recommended changes have been made, while activities related to other recommendations are ongoing. Explanations were provided as to why some of the recommendations were deemed impossible to implement (e.g., increased resources at the field level which is a provincial or municipal responsibility).

In terms of funding shifts, in March 2007, IC informed PS that, although the operation of *CyberWise.ca* had two years remaining in its mandate, the SchoolNet Terms and Conditions, under which *CyberWise.ca* was administered, had only been extended for one year. The *CyberWise.ca* component of the Strategy did not include salary dollars and, with the IC Information Highway Applications Branch's reduced funding and downsizing, it was not possible to continue support for the operation of *CyberWise.ca* to meet the requirements of the Strategy. Therefore, IC decided to cease its activities related to *CyberWise.ca*.

As the coordinator of the Strategy, PS had the authority to reallocate funding from one partner to another, if deemed necessary. PS exercised its leadership role and undertook to reallocate the IC money to *Cybertip.ca* to ensure the Strategy objective related to public education and awareness could be maintained. Thus, the $1 million in each of the fiscal years 2007-08 and 2008-09 that had been profiled for IC for *CyberWise.ca* activities under the Strategy was made available to PS, who, in turn, directed the funding to *Cybertip.ca* and provided for one more position at PS in the Serious and Organized Crime division.

In addition to the above-noted shifts, PS coordinated a Treasury Board Submission which detailed the allocation of the additional $6 million per year in funding, announced in Budget 2007, to enhance existing initiatives to combat child sexual exploitation and trafficking. Under PS leadership, new funds were also allocated to activities to combat human trafficking for the first time.

[7] The final report was dated June 2007.
[8] The RMAF/RBAF will be updated by December 2008, should the National Strategy be renewed.

As a result of these developments, including the recommendations of the formative evaluation, the logic model for the Strategy was updated to reflect activities that were deemed to be important yet not anticipated at the outset of the 2004 Strategy. Those activities were undertaken by Strategy partners on their own initiative following the identification of areas where work needed to be done (see Appendix A). PS organized two one-day workshops with the evaluators and Strategy partners to discuss the revised logic model. A separation between the original logic model elements and the new elements is noted. It should also be noted that the original intent of the initiative and outcomes of the Strategy have not changed.

In terms of other assessments of the Strategy, as per the audit plan, PS coordinated an audit of *Cybertip.ca* in fiscal year 2006-07. This audit examined whether funds were used for their intended purposes; assessed compliance with terms and conditions; and, analyzed reliability of results data. The results of the audit concluded that *Cybertip.ca* funding has been managed according to recognized audit practices.

IC's activities under the Strategy were monitored according to SchoolNet Terms and Conditions, as well as according to the objectives of the Strategy.

1.3 Purpose of the Summative Evaluation

As per the combined RMAF/RBAF for the Strategy, PS coordinated this summative evaluation and will submit its findings to the Treasury Board Secretariat (TBS) of Canada, as a basis to determine the ongoing nature and level of funding for the Strategy.

As per the RMAF/RBAF, the Summative Evaluation assessed:

- continuing relevance of the Strategy;
- overall impact and success of the Strategy;
- cost-effectiveness and alternatives; and,
- aspects of the design and delivery of the Strategy related to governance and progress against the recommendations of the formative evaluation.

This summative evaluation covers a four-year period from the receipt of Strategy funding in April 1, 2004 to March 31, 2008.

2. Evaluation Issues and Methodology

2.1 Evaluation Issues and Questions

The list that follows summarizes the research questions for the evaluation. The seven expenditure review questions of the Expenditure Review Committee (ERC) of the TBS have also been included and are referenced as such.

Evaluation Questions

Relevance

1. Is there a continuing need for a national strategy that combats Internet-based Child Sexual Exploitation (IBCSE)? Does the Strategy continue to serve the public interest? (ERC 1)

2. Are allocated resource levels sufficient based upon the scope of the identified need, given the nature, size and evolution of the problem?

3. Is the Strategy appropriate to the federal government mandate and what is the appropriate role for other levels of government or the private/voluntary sector? (ERC 2, 3, 4)

Success

4. To what extent has the Strategy increased knowledge of investigative challenges, best practices and measures to overcome challenges among law enforcement, justice partners and ISP providers?

5. To what extent has law enforcement collaboration been enhanced through information sharing and partnerships?

6. To what extent is information and intelligence being shared nationally and internationally?

7. To what extent have public education efforts contributed to enhanced awareness of the nature of the crime, exploitation signs, prevention behaviours, and reporting mechanisms among the general public and target populations?

8. To what extent has Strategy contributed to coordinated, comprehensive and efficient national and international investigations?

9. To what extent has better awareness contributed to enhanced reporting?

10. To what extent has the Strategy enhanced crime prevention?

11. To what extent has the Strategy contributed to enhanced: protection of children from sexual exploitation; pursuit of those who use technology to facilitate the exploitation of children?

12. How has the evolving nature of the Strategy (additional funding, additional activities undertaken, etc.) impacted the success of the Initiative?

Cost-Effectiveness and Alternatives

12. Are Canadians getting value for their tax dollars? (ERC 5)

13. To what extent have resources been optimised to improve efficiency? If the Strategy continues, how could its efficiency be improved? (ERC 6)

14. Is the Strategy the most appropriate response to the identified need?

Design and Delivery

15. Is the governance structure appropriate to achieve the Strategy's intended outcomes?

16. What progress has been made toward implementation of the recommendations of the formative evaluation?

2.2 Evaluation Methodology

The evaluation used three basic lines of inquiry to complete the analysis. These were: document review, review of quantitative information and interviews. A list of documents and quantitative data reviewed by the evaluation team is contained in Appendix B. In terms of interviews, the table that follows outlines the categories of individuals who were interviewed, as well as the number of interviews conducted. Interview guides are presented in Appendix C. Throughout the report, interview information has been reported according to the guide contained in Appendix D. Thus, the terms used throughout the report associated with “a few”, “some”, “many” and “most” are specifically linked to the proportion of interviewees shown in the guide.

Representation	**Number of Interviews**
Strategy Oversight	2
Cybercrime Working Group Senior Officials (DOJ)	2
Program Management – NCECC	4
International Partners	4
Program Management – Education and Awareness (IC & *Cybertip.ca*)	2
Law Enforcement – Field Level	8
ISPs	3
TOTAL	**25**

2.3 Limitations and Assessment of Data Availability

The evaluation methodology was designed to provide multiple lines of evidence in support of evaluation findings. However, there were some limitations with respect to the methodologies as outlined below.

1. A broad-based survey was not one of the lines of inquiry for the evaluation; the evaluation relied upon surveys previously conducted or immediately available. The evaluation also relied on measures of reach by target audience in order to assess the coverage of educational material, in place of surveying end users.

2. Full analysis associated with cost-effectiveness was not possible due to several factors. First, investigations are linked through a number of levels of law enforcement (federal, provincial, municipal) and these costs could not be attributed. Second, some of the partners and activities leverage resources (financial and in-kind) from other sources and these were not quantified. Finally, benchmarks or comparables were used to the extent possible but this information was limited.

3. Due to budget and time constraints, the total number of interviews was small and the sample size in each group may not have been representative of the full perspective of some target audiences. Where possible, quantitative data was used to supplement and validate the views expressed in interviews in order to mitigate this limitation.

4. In terms of coverage at the field level, the evaluation covered eight law enforcement units in four general geographic regions in Canada as follows: Alberta, Ontario, Quebec, and Atlantic Canada. Saskatchewan and Manitoba did not have integrated child exploitation (ICE) units in operation at the time of the evaluation, and, although requested, the representative from British Columbia was involved in a number of operational files at the time of the evaluation and was therefore unable to participate within the timeframe of the evaluation.

3. Findings and Conclusions

Section 3 of the report presents findings from all lines of inquiry and conclusions based on the findings. It is organized according to the standard evaluation issue areas of relevance, success, cost effectiveness and alternatives, and design and delivery.

3.1 Relevance

Serving the Public Interest[9]

The evaluation sought to examine whether the Strategy continues to address issues and concerns that are relevant to Canadian society and whether the Strategy continues to serve the public

[9] References evaluation questions 1: Is there a continuing need for a national strategy that combats Internet-based Child Sexual Exploitation (IBCSE)? Does the Strategy continue to serve the public interest? (ERC 1)

interest. More specifically, the evaluation examined trends regarding the continuing need for intervention by a national strategy and whether resource allocated to the Strategy are sufficient based on the scope, nature, size and evolution of the problem of Internet-based child sexual exploitation (IBCSE). Finally, the evaluation examined the appropriateness of the federal government role and its partners in the Strategy and whether there are other stakeholders, such as other levels of government or the private and voluntary sectors, which can assume responsibility for achieving some of the objectives.

Trends in Internet Use in Canada

The proliferation of Internet use in Canadian society poses an increasing risk of the exposure of children to sexual predators and potential victimization. The *Internet Sexual Exploitation of Children and Youth Environmental Scan* suggests that Canadians are avid users of the Internet and the trend is increasing. In 2003, data from Statistics Canada showed that approximately 64% of Canadian households reported having accessed the Internet from home, work, school a public library or other locations; this represents a 20% increase from 1999 figures. The study notes: "A cross-section of Canadian children and youth who have (and continue to) grown up in a technological world are not representative of the average Canadian's involvement with computers and the Internet. Millions of children and youth are adept at using computers, with a large part of their time being spent on the Internet."[10] In fact, a study published in 2002, concluded that 84% of Canadian children are "wired".

In 2000-2001, data from *Young Canadians in a Wired World - Phase I (YCWW-I)*[11] revealed that young Canadians were very active users of the Internet, were ahead of their parents and explored the Internet on their own. The study confirms that: "The Internet has been a ubiquitous presence in young Canadians' school lives since 1999, when Industry Canada connected all of Canada's 5,000 public schools to the Internet. However, the Net is also now a pervasive element of young people's home lives. Ninety-four percent of kids report that they have Internet access at home, and a significant majority of them (61 percent) enjoy a high-speed connection. By the time kids hit Grade 11, half of them (51 percent) have their own Internet-connected computer, separate and apart from the family computer."[12] The study also found that Canadian children now have increased access to the Internet through a wide variety of communications media, including cell phones, camera phones and wireless devices; providing them 24/7 online access. Results of the environment scan further support that: "The children and youth of today are many times the experts in computer usage - parents are playing catch-up and often times do not understand the realities of the world that the Internet opens up for their children."[13] These findings have many implications for the safety of youth and child using the Internet.

[10] Ibid.
[11] Young Canadians in A Wired World (YCWW) is a study conducted by Media Awareness Network, a not-for-profit organization based in Ottawa. The study measured online use patterns of young Canadians. The objective of this study was to track, investigate, and measure the behaviours, attitudes and opinions of Canadian children and youth's use of the Internet. The first phase of the research (YCWW-I) took place in 2000-200 1 and a follow up study (YCWW-II) was conducted in 2003-2005.
[12] Media Awareness Network, YCWW-II Trends and Recommendations, p.6
[13] NCECC, *Internet Based Sexual Exploitation of Children and Youth Environment Scan*, January 2005, p.16

The Internet has become a fixture in the lives of today's children and youth. Youth are integrating the Internet into their social lives at an early age. YCWW-II reported that "young people use the Internet as a social space, where they can stay connected to friends and explore social roles".[14] From the youth's point of view, the Internet allows them to do so in a safe environment, with relatively few consequences. However, the safety of these interactions is built upon the assumption that youth will never actually confront the people they are interacting with online.[15] Nevertheless, this assumption is incorrect: a study conducted by the Adolescent Health Survey found that almost 25% of girls in Canada have been in contact with a stranger on the Internet who made her feel unsafe.

Trends in the Nature, Size and Evolution of the Problem

The NCECC conducted the *Internet Sexual Exploitation of Children and Youth Environmental Scan* in 2005. It concluded that Internet-based sexual crimes against children are increasing in Canada and abroad and that the public is increasingly concerned. The distribution of child sexual abuse images is also expanding, in concert with an increase in Internet use. The study states that: "while it is not possible to state empirically that the Internet has changed the demand for child sexual abuse images or if alternative means might have been exploited resulting in the same demand changes, it is possible to state that the Internet has had a large impact on the accessibility, affordability, and assumed anonymity of people seeking child sexual abuse images."[16]

The study reports that while the flow of child sexual abuse images have significantly diminished in the late 1990s, the widespread use and nature of the Internet as a medium has changed the situation.[17] Research suggests that prior to the Internet; there were few distributors of child sexual abuse images. Such material was only available in hard copy and was often purchased in select places. Now, the landscape has changed: individuals have access to child abuse images from their homes or offices, via chat rooms, websites, peer to peer file sharing and others. This material can now be traded, sold and purchased 24 hours a day from various locations throughout the world.[18] It is estimated that 14 million websites offer child sexual abuse images, with some websites containing over 1 million images.[19] Furthermore, findings reported that 23,000 websites and 40,000 chartrooms support sexual activity between an adult and child. Children throughout the world are also used by adults for sexual purposes. The 1998 United Nations Human Rights Commission stated that 10 million children around the work were being abused in such a manner. In Canada, in 2002-2003, Canadian Customs intercepted over 200 shipments of child sexual abuse images per year. That same year, *Cybertip.ca* received 555 reports of sexual abuse images on the Internet.[20]

Effects of Evolving Technology

[14] Media Awareness Network, Y*CWW-II Trends and Recommendations,* p.8
[15] Ibid, p.10
[16] NCECC, *Internet Based Sexual Exploitation of Children and Youth Environment Scan,* January 2005, p.18.
[17] Ibid.
[18] Ibid, p.34.
[19] Ibid.
[20] Ibid.

Due to the evolving nature of technology, the sexual exploitation of children and youth has taken on new forms. Furthermore, interconnections exist with prostitution and trafficking: "The Internet provides new tools to assist in the sale of children and youth, creates space to communicate needs of and availability of such 'services', and provides access to vulnerable people to victimize."[21] Examples include advertisings via chat rooms and bulletin boards; online networks and discussion forums on locations of kiddie strolls[22]; cellular and mobile phones which are used to keep in contact with other predators or to contact youth prostitutes and receive images; and web cams which provide opportunities to broadcast their abuses.[23] Other technologies that enable offenders include digital compression and encryption of material containing abuse, anonymous remailers, email, instant messaging, Internet Protocol telephony, multi-media messaging service, newsgroups, peer to peer (P2P) networks picture messaging, short messaging service, stenography, websites and whispering. Digital compression, which minimizes the size of a file without changing its content, has also increased in popularity. When combined with encryption, files are more difficult to detect. Anonymous remailers are another method which allows for an email to be sent without the recipient knowing the identity of the sender.[24]

The emergence of botnet technology[25] has become a primary concern among law enforcement, and IT professionals, and poses serious risks to computer users and their Internet security. On one hand, they allow controllers to store illegal material and access this material as they wish, without storing evidence on their own systems. Controllers have been known to use bots to store illegal images (including child abuse images) on computers of unsuspecting individuals. During investigations of child sexual exploitation investigations, this may have many implications for police and prosecutors. They must first determine whether the computer user is engaging in illegal activities or being used to conceal the activities of others. Furthermore, offenders may use botnets as defence. They may argue that someone else stored this material on their computers.[26]

Advances in technology have also created easy and inexpensive, low detection means of producing child sexual abuse images: "digital cameras, scanners, and web cameras have changed the way child sexual abuse images are produced, and introduced the option to many."[27] The production of child abuse images occurs all over the world and increasingly, offenders consider this a business opportunity to provide a rare and sought after commodity.[28]

The nature of child sexual abuse images themselves have also evolved. These images can be created using real, morphed, and virtual children. Due to technological advancements, images can be altered to generate large amounts of different depictions of children; a process referred to as

[21] Ibid, p.20.
[22] Kiddie strolls are areas of a city where offenders can find youth and children under the age of 14 for the purpose of engaging in sexual activities
[23] NCECC, *Internet Based Sexual Exploitation of Children and Youth Environment Scan*, January 2005, p.20
[24] Ibid, pp.20-24.
[25] A botnet is a network of bots or robots. Bots are agents of these networks which contain executable files or malicious code; which allow their controllers to take over vulnerable computers. Once these bots are in place and the process is put into motion by the executable file, the controller, a person other than the owner of the computer system, can engage in a variety of activities. Controllers of botnets are often looking to expand their botnet; thus, bots continuously scan the Internet in search of vulnerable systems to infect. It is estimated that unsecure computer systems can be compromised in less than 30 minutes.
[26] NCECC, Botnets Briefing Notes.
[27] NCECC, Internet Based Sexual Exploitation of Children and Youth Environment Scan, January 2005, p.38
[28] Ibid, p.39.

morphing or creating pseudo images.[29] Although these images are computer generated pictures of children who do not exist as depicted in the image, they may appear life-like and portions of the image may originate from images of real people.[30] As technology continues to improve, it becomes more difficult for law enforcement to differentiate between real and virtual images and for the justice system to intervene; particularly in international cases where debates still exist around the legal restriction of pseudo-images (Canada, the United Kingdom, Austria and the Netherlands currently have legislation prohibiting the possession, production, and distribution of child sexual abuse images and pseudo-images; however in the United States, most state laws do not prohibit individuals from possessing, producing or distributing pseudoimages).[31]

A final repercussion resulting from advancements in technology involves the widespread use of wireless technology. Wireless technology is increasingly popular way to access the Internet among individuals and businesses due to its convenience, and its affordability. It is estimated that wireless networks have increased in North America from 30 million in 2005 to 74 million by 2009.[32] However, wireless networks are more susceptible to security vulnerabilities and many wireless users do not take sufficient steps to ensure an adequate level of security when implementing these networks. Consequently, these networks may be accessed by unauthorized users and used to facilitate various illegal activities, including Internet-facilitated child sexual exploitation.[33] The NCECC conducted a survey of various locations in and around Ottawa to determine the presence of wireless networks and their level of security. They found that a significant number of networks had almost no security.[34] Unsecure wireless network connections offer another opportunity for offenders to pursue IBCSE. It has been reported that offenders are known to drive to areas away from their own residence where they can access such material from another person's wireless Internet connection.[35] This makes it more difficult to locate and catch offenders. Law enforcement officers may believe to have located an offender, when in fact, they are pursuing an unsuspecting Internet user, whose wireless connection has been accessed without authorization, to access child abuse images.

Continuing Need

Most interviewees indicated a continuing need for the Strategy citing the Internet and evolving technology as drivers for the proliferation of child exploitation material. Others believed that the proportion of the population who access child exploitation material has not changed but the ability to access it has increased because of these drivers. Some interviewees indicated that the scope and nature of the crime has expanded; it is more severe, there are new forms, it is multi-jurisdictional and international in nature. Many field level interviewees have reported an increase in the number of cases and *Cybertip.ca* has seen an increase in the number of reports over the last four years.

[29] Pseudo images are created by to combine two or more images to form one picture or add and/or delete objects or parts of a photo to create a unique image.

[30] If it can be proven that components used to produce the image originated from real children, the material would be illegal. However, offenders may argue that if a child was not abused in the creation of the image, its possession should be legal.

[31] NCECC, Internet Based Sexual Exploitation of Children and Youth Environment Scan, January 2005, p.35

[32] NCECC, Wireless Networks in Ottawa: Are They Secure?, April 2008, p.5.

[33] NCECC, Wireless Networks in Ottawa: Are They Secure?, April 2008, p.3.

[34] Ibid, pp.12-14.

[35] Ibid, p.13.

Document review also provides evidence of the continuing need for educational material for parents to further protect their children on the Internet. In 2006, an Ipsos-Reid survey was conducted which revealed that: 98% of parents place a high priority on children learning how to protect themselves from sexual exploitation on the Internet; 80% of parents believe that children should learn about personal safety strategies at home and in school; most Canadian parents are using outdated and ineffective information to teach their children personal safety; a third of Canadian parents have not discussed Internet safety with their child; and the majority do not know where to access Internet safety information[36]. As well, a 2007 Pollara Survey revealed that 54% of Canadian parents are worried about their child's safety on the Internet[37].

Interviewees were also asked whether the five areas of the Strategy that were not anticipated at the outset, but are now included in Strategy activities, continue to be necessary. These five areas are as follows: Legislation/ Policy, ISP industry partnerships, Investigative Partnerships, Research, and Communications. Most interviewees indicated that all of these areas remain important. The presence of a continuing need for each of these evolving areas is presented below.

Interviewees mentioned the need to continue to study **legislation** in order to identify gaps and develop legislative tools and standards. They believe that when technology changes (e.g. encryption) and legislation has not kept pace, investigations are inhibited. They cited the need for mandatory compliance in providing passwords for encrypted computers and for companies, such as ISPs and computer repair shops to report child pornography if it is found on their system or on a computer. The issue of mandatory reporting is currently a high priority for the FPT Ministers Responsible for Justice. The Cybercrime Working Group (CWG), of which PS and the RCMP are active members, has been studying this issue on a priority basis over the last year. Since 2007, officials from PS and the RCMP have also been working actively on the lawful access initiative which may, if passed, assist law enforcement to further their investigations by requiring private companies to provide the Customers Name and Address (CNA) of persons suspected to be involved in illegal activities on the Internet.

Interviewees also stated that the continuing need to study legislation is evidenced by the fact that proposed legislative changes are still coming forward. Finally, interviewees stated that, with more cases going through the justice system, case law is developing, and that examination of the results of these cases may necessitate further legislative change.

Interviewees believed that **ISP partnerships** continue to be critical because the relationship helps to "motivate corporate responsibility in a different way". ISP interviewees expressed that issues can be handled more effectively on a voluntary basis within set parameters through partnerships rather than through legislation. Furthermore, interviewees stated that there is a continuing need for expanding partnerships because new partners are brought in to help resolve issues as they arise. For example, they noted that Strategy partners and ISP providers are now looking at how credit card companies might contribute to their efforts. Finally, there is still work to be done, since only about 10 ISPs, out of approximately 400 in Canada, are actively engaged on the

[36] KIK Fold Out

[37] Safer Internet Day Evaluation 2008.

issue and are aware of the reporting tipline (*Cybertip.ca*). It is worth noting that these 10 ISPs have broad coverage through their networks, and cover about 90% of the country.

Interviewees believe **investigative partnerships** continue to be necessary for three principal reasons. First, there is a need to identify challenges and share best practices, and this is accomplished through time spent together on investigations. Second, there are large-scale, international aspects to this crime including the emergence of commercial pornography that require strong investigative partnerships. Third, more provincial and municipal law enforcement agencies are joining to address the issue; therefore further work on partnerships is anticipated.

Interviewees believe that **research** continues to be necessary under the Strategy to assist both educational and law enforcement efforts. There is a need to understand how Canadian children are being targeted, trends for youth and social networking, offender profiles and behaviours, and the impact of evolving technology and the approach to combating child sexual exploitation on the Internet.

Interviewees stated that it is important for the NCECC and *Cybertip.ca* to continue on **communication** efforts to ensure coordination and dissemination of best practices and to find out what is working and what is not working. In addition, a coordinated education and awareness strategy is necessary to avoid duplication of efforts. A communication strategy was produced by PS, in consultation with Strategy partners, in May 2008.

Emerging Issues

Interviewees also identified other possible program areas to be addressed by the Strategy; including judicial partnerships and forensics. Additionally, respondents felt there were other aspects of the crime which were not being addressed by the Strategy. These included the need to understand linkages between commercial pornography and child sex tourism since proceeds of crime falls under the federal mandate but child pornography offences are prosecuted provincially; the involvement of organized crime; and understanding the needs of victims. A few interviewees suggested that having international presence as part of the Strategy could help address problems with child sex tourism. This would involve having an international task force located at the NCECC and active units in other countries to target Canadian citizens travelling for the purposes of child sex tourism. To this end, a new position was recently created at the RCMP to address the issue of child sex tourism.

Resource Demands[38]

The evaluation studied whether resource levels are sufficient based on the scope of the identified need, given the nature, size and evolution of the problem of IBCSE.

Document review indicates that the child pornography industry is expanding, a problem exacerbated by widespread use and availability of the Internet. Criminal Justice statistics support

[38] References evaluation question 2 : Are allocated resource levels sufficient based upon the scope of the identified need, given the nature, size and evolution of the problem?

the finding that the incidence of production and distribution of child pornography and luring children via computers has increased. Furthermore, evidence shows that perpetrators are adults as well as other youth. A study conducted by the NCECC presents a summary of these findings:

Number of Child Pornography and Luring Offences in Canada[39]:	
1998 (per 10,000 adult and youth population)	2005 (per 10,000 adult and youth population)
0.006	0.042

Number of Adults and Youths being Processed through the Court System for Child Pornography Offences[40]:			
Adults (per 10,000 adults)		Youth (per 10,000 youths)	
1998-99	2003-04	1998-99	2002-03
0.042	0.091	0.012	0.044

Efforts and workload trends among law enforcement suggest that the problem is getting worse. Many field level interviewees cited investigative resources as their most pressing need stating that they are unable to meet demand to investigate and process cases that they are receiving. *Cybertip.ca* statistics support these findings. The statistics indicate an increasing number of cases forwarded to local law enforcement. Between 2002 and 2004, 191 cases were forwarded to local law enforcement agencies; in 2005, 203 cases were forwarded; in 2006, 324 and in 2007, 437 cases were forwarded to provincial and municipal law enforcement agencies[41]. It should be noted that the responsibility for field level resources rests with provincial and municipal governments.

Some interviewees identified the lack of an image recognition database and forensics software and personnel as serious impediments to their operations. They cited the need for trained forensics personnel and a desired increase in forensics resources that would see a ratio of one forensics resource for every two investigators. They indicated that lack of forensics resources presents challenges as investigators prepare for court because they do not have enough time to put their cases together both because forensics work is time consuming (size of files being processed is sometimes in terabytes) and due to the backlog in forensics, because of limited resources. Filling positions in forensic analysis would be a provincial/municipal responsibility.

In terms of resourcing the demand for educational material, downloads reported by *Cybertip.ca* suggest an increase in public requests for education and awareness material. Statistics reveal that the number of *Cybertip.ca* educational downloads have significantly increased. Between 2002 and 2004, 20,038 downloads were made, increasing to 120,541 downloads in 2007. *Cybertip.ca* has also tracked the distribution of awareness material. Between 2005 and 2007, the following material has been distributed: 195,463 books and comics, 228,914 safety sheets, 3,161,215 brochures, 29,558 posters and 31,121 kits.

Conclusions – Serving the Public Interest / Providing Resources to Meet the Need

[39] Child Pornography Offences in Canada: Recent Trends. NCECC, 2007. pp.3
[40] Child Pornography Offences in Canada: Recent Trends. NCECC, 2007. pp.3-4.
[41] *Cybertip.ca* triages these reports and forwards them directly to provincial and municipal law enforcement. However, a vast majority of reports are forwarded by *Cybertip.ca* directly to the NCECC for preliminary investigations.

1. Overwhelming evidence suggests a continued need for a national strategy to combat Internet-based Child Sexual Exploitation (IBCSE). The problem of IBCSE has not diminished; rather it continues to be prevalent and expanding in Canadian society. Thus, it remains relevant and in the public interest to address this issue. Interviews and studies conclude that the Internet and technology are pervasive in children's lives, and because of this, offenders have increased access to potential victims. Technological advancements have enabled sophisticated methods for offenders to conceal their identities and to continue to offend, leading to the emergence of new forms of IBCSE.

2. The number of IBCSE cases being processed has increased, and *Cybertip.ca* and the NCECC are forwarding more cases to law enforcement. Evidence from interviews suggests that law enforcement at the field level is lacking skilled investigators and forensics support. However, it should be noted that the responsibility for field level resources rests with provincial and municipal governments.

Roles and Responsibilities/ Governance[42]

The evaluation explored whether the roles of federal partners in the Strategy are appropriate, whether other levels of government, private or voluntary sectors should be involved in the Strategy, and if the current governance structure is appropriate to achieve the Strategy's outcomes.

The Strategy is built on a partnership approach that involves all levels of government, NGOs and the private sector. Formal funding is provided to two federal partners, PS and the RCMP, and an NGO, *Cybertip.ca* through a contribution from PS. However, the Strategy also includes donations to *Cybertip.ca* from the private sector, including ISPs. Although not funded under the Strategy, provincial and municipal police agencies investigate child exploitation files through the ICE units and local police agencies. Interviewees generally believe that federal partners, the RCMP and PS, in conjunction with *Cybertip.ca*, each play the appropriate role with regard to the Strategy.

PS led the [*] coordinated activities of partners during the preparation [*] and the coordination of audits and evaluations. Between 2004 and 2008, PS also coordinated and prepared responses to over 50 Ministerial dockets on behalf of partners, has coordinated two formal evaluations of the Strategy, and an audit of *Cybertip.ca* activities. PS is the "federal face" of the Strategy for FPT working groups such as the Coordinating Committee of Senior Officials - Cybercrime Working Group and the National Coordinating Committee on Organized Crime. PS has also provided input to related TB submissions outside the Strategy such as the lawful access initiative and PIPEDA. In terms of developing and maintaining positive relations with provincial partners, both PS and the RCMP play a key role in FPT fora to exchange information, discuss effective techniques to combat child sexual exploitation, as well as discuss legislation. PS also co-chairs the Interdepartmental Working Group on Trafficking in Persons (IWGTIP) which allow for effective engagement of eighteen federal departments & agencies that share an interest in child sexual exploitation and trafficking.

[42] References evaluation question 3: Is the Strategy appropriate to the federal government mandate and what is the appropriate role for other levels of government or the private/voluntary sector? (ERC 2, 3, 4)

In terms of the RCMP's role, the central coordinating role of the NCECC, on the law enforcement side, is considered a very important aspect of the Strategy that needs to be maintained going forward mainly because the NCECC provides a single point of contact nationally and internationally. Close to half of interviewees believe that little or no overlap exists between the law enforcement area of Strategy and other programs (the other half did not comment). Rather, they noted that other law enforcement bodies such as local law enforcement agencies, ICE units, provincial strategies and the Virtual Global Taskforce (VGT) complement the work achieved through the Strategy.

In terms of *Cybertip. ca* 's role, interviewees were generally positive about the role *Cybertip.ca* has undertaken both in managing complaints and providing educational material. However, interviewees also expressed uncertainty regarding the level of duplication or coordination of educational efforts related to this role. *Cybertip.ca* and many other groups appear to be involved in the educational area. For example, presentations in schools are being provided by law enforcement officials, school liaison officers, guidance counsellors and other organizations such as Kids Internet Safety Alliance (KINSA).

Finally, interviewees suggested further engagement of provincial and municipal governments and other organizations, including grassroots and voluntary sectors, ministries of health, child protection services and school boards. Other federal departments were also suggested for further engagement in the Strategy, these departments include the Department of Justice, Statistics Canada, Canada Borders Services Agency, the Department of Foreign Affairs and International Trade and Citizenship and Immigration Canada[43].

Horizontal Level Governance[44]

The RMAF/RBAF for the Strategy outlined several mechanisms for oversight and horizontal governance. First, PS's role was to a) support the ADM Steering Committee in terms of policy coordination, development and logistics; and b) provide overall coordination for the implementation of the entire Strategy. Second, according to the original design, the Assistant Deputy Minister (ADM) Steering Committee was seen as necessary to provide overall direction, oversight and advice on events and circumstances that may influence the achievement of expected outcomes. Third, partners were to work collectively through an Interdepartmental Working Group (IWG) to measure, monitor and report on performance and risks against expected outcomes and to maintain Strategy corporate memory in support of knowledge management[45]. The RMAF/RBAF also stated "it should be noted that the NCECC is under the direction of the National Steering Committee on IBCSE, representing law enforcement across the country"[46]

[43] These departments currently participate in the IWGTIP which is interested in the issue of child sexual exploitation and trafficking.
[44] References evaluation question 16: Is the governance structure appropriate to achieve the Strategy's intended outcomes?
[45] Formative Evaluation of the National Strategy for the Protection of Children from Sexual Exploitation on the Internet, June 2007
[46] Integrated Horizontal RMAF/RBAF for the National Strategy for the Protection of Children from Sexual Exploitation on the Internet, May 2006

Over half of those interviewed indicated that, generally, the current governance structure for oversight works well or causes no concerns. Overall, interviewees felt that there is no need for an additional level of decision-making such as an ADM Level Steering committee as PS briefs the upper levels when necessary. However, a few interviewees departed from this point of view stating that having upper level involvement would help drive the issue of IBCSE from a government-wide perspective. To this end, following the formative evaluation, PS coordinated the management response and reaffirmed its commitment to revitalizing a National Steering Committee to provide direction and guidance to Strategy partners. In May 2008, a meeting was held with partners (PS and RCMP) to determine the level of representation for the steering committee; it was determined that the Director General/Superintendent level would be the most appropriate.

Coordination and Strategic Direction of the Strategy

In terms of providing strategic direction to the Strategy, PS has assumed this role, and through coordination of the IWG, a revised logic model was developed in 2008 to include some activities that were not part of the original Strategy. PS also recently led the development of a communications plan for 2008-2009 to assist in coordinating education and awareness activities in consultation with RCMP and *Cybertip.ca*. The plan sets out communication objectives for the fiscal year of 2008-2009. Document review indicates that there may still be coordination work to be done since the NCECC also has a communications plan with some shared target audiences and similar activities. A few interviewees noted that the Strategy may be able to increase cohesion through better coordination of strategic direction between the RCMP and *Cybertip.ca*. In addition, a few interviewees mentioned the coordination role of PS as being appropriate; however, they believe that the Strategy requires further and engagement of the IWG to coordinate such activities as: implementation of the communications plan; legislative issues and how work on this file should divided among partners, including DOJ; and to help integrate a research agenda because the NCECC, *Cybertip.ca* and PS are all involved in research.

Some interviewees made suggestions that they believe could make the Strategy more effective in responding to changing needs and emerging issues. The increased coordination of research efforts (noted above) would benefit this forward planning work. On-going progressive research was noted as being important to help the Strategy by providing a broader understanding of the crime and the current technological context, and by regularly challenging the assumptions on which the Strategy is built. This research could provide deeper insight into the issues of how offenders interact on the Internet and why they use the Internet to commit their crime. For example, the Wickerman investigation[47] found that the motives were not about organized or commercial crime but rather; about individuals sharing images for “kudos”. Studying successes such as the Wickerman case and others at the tactical level could translate into action at the strategic level and could assist the Strategy in further realizing success.

Working Level Governance

Some interviewees commented that roles and responsibilities are clearly defined, positive working relationships exist and partners are engaged in discussions. Relationships appear to be

[47] The Wickerman investigation, in which Canada was heavily involved, infiltrated a large group of offenders using new investigative methods

built successfully on an informal basis, but may benefit from meeting more frequently to improve the decision-making process. To this end, partners have worked collectively through the Interdepartmental Working Group (IWG) as the need arises. Performance information received from the NCECC, in particular, for the evaluation has been weak.

At the field level, interviewees support that working level coordination is working well or that there are no particular issues with the governance structure. ICE Officer in Charge (OIC) meetings were viewed as being the greatest contributor to the success of governance at the working level. These meetings were seen as useful for communication, planning and sharing of information on the law enforcement side of the Strategy; issue resolution; communicating what is happening; and making decisions on investigative issues. For example, from the interviewees' perspective, these meetings were an opportunity to discuss case law decisions and to help ICE units with understanding the role of the NCECC in these situations and to discuss the potential role of the NCECC in streamlining business and procedural matters. Interviewees noted that other meetings and committees that have contributed to working level governance include the CETS working group, international working groups, and the Victim Identification working group.

Interviewees suggested the following: holding longer ICE OIC meetings (significant distance to travel for a short time period) and potentially link them to the annual conference, and; invite Crown prosecutors and other relevant players such as heads of education to the ICE OIC meetings to provide an opportunity to share key information and clarify roles.

Conclusions – Roles, Responsibilities and Governance

3. The Strategy is built on a partnership approach that involves all levels of government, NGOs and the private sector. The roles and responsibilities, as they are delineated under the Strategy are appropriate. The federal government continues to play an essential role in the fight against IBCSE. Efforts of partners have been well-coordinated by PS, and the central coordinating role of the NCECC is key to a national strategy to combat IBCSE.

4. Original governance mechanisms as laid out in the RMAF/RBAF have evolved. There has been no requirement for the envisioned Assistant Deputy Minister (ADM) Steering Committee. The National Steering Committee is being revitalized and work of the Interdepartmental Working Group (IWG) has been well-coordinated by PS on an as-required basis. PS has also brought a degree of strategic planning to the Strategy through the redesign of the logic model, participation in national and international working groups and the development of cabinet documents to address changing needs. Further advancement of a strategic agenda and continuing to remain abreast of emerging issues is an important role of PS. There is a need for further engagement of the IWG in areas such as communications (public awareness), and research. In addition, there is still work to be done in developing

awareness of other groups involved in public education efforts (outside the Strategy) so that the Strategy can realize synergies and avoid duplicating the efforts of others. Working level governance through the Integrated Child Exploitation (ICE) Officer in Charge (OIC) meetings is functioning very well although some participants would like to see longer meetings because of the significant travelling distance.

3.2 Success

Section 3.2 presents findings related to the achievement of desired outcomes of the Strategy. The degrees of success in the areas of law enforcement and education/awareness, as well as the impacts on success due to the evolving nature of the Strategy are presented in the sections that follow.

3.2.1 Law Enforcement Capacity Building and Operations

The objectives of the Strategy have a very wide reach and a number of law enforcement beneficiaries. Under the Strategy, through the work of the NCECC, it was intended that municipal and provincial law enforcement agencies across the country would benefit from increased coordination, as well as investigative and intelligence assistance. Under the Strategy, it was also intended that the NCECC would foster particularly close relationships with the ICE units and specialized units in other police services. Finally, the NCECC was intended to be the primary point of contact for international investigations concerning IBCSE cases and would liaise with international police forces to the benefit of both Canadian law enforcement and law enforcement abroad.

Impact of the Strategy on Knowledge and Awareness among Law Enforcement, Justice Partners and Internet Service Providers [48]

The NCECC has been proactive in providing training for the increased knowledge of investigative challenges, best practices and measures to overcome challenges among law enforcement, justice partners and ISP providers. This has been accomplished through the hosting of training sessions and national conferences, the sending of communiqués and website hosting.

Conferences have contributed to knowledge increase for several of the target groups. From 2004-2007, the NCECC hosted the NCECC Annual Conference. These conferences were an ideal venue for investigators from across Canada to share investigative techniques, promote best practices and network. Over the years, the NCECC Annual Conference consistently increased participation of investigators. Approximately 130 participants representing 64 investigative units in the area of IBCSE were expected at the 2007 law enforcement workshop[49]. Participant feedback indicates that the NCECC Annual Conference contributed to increased learning[50]. For every year of

[48] Refers to evaluation question 4: To what extent has the Strategy increased knowledge of investigative challenges, best practices and measures to overcome challenges among law enforcement, justice partners and ISP providers?
[49] No actual data provided.
[50] Participant feedback summary (NCECC Annual Conferences 2004-2007)

the conference, ratings of at least 4.5 out of 5 or above (5 indicating strongly agree) were given on the statement that the conference provided an opportunity to learn.

In 2008, the Atlantic Region Internet Safety Symposium was held by the NCECC to provide a better understanding about the scope of IBCSE and reinforce the need for law enforcement, government and ISP co-operation. The symposium expanded the breadth of participants and subject matter went beyond that of law enforcement topics to include: youth issues, learning about U.S. Electronic Service Providers (ESP), information on mandatory reporting initiatives, and ISP partnership initiatives. Participant feedback indicated that the symposium provided a good opportunity for discussion and a better understanding of the judicial process from complaint to court. Overall, results indicated that the Symposium allowed participants to gain a better understanding of IBCSE and to learn about U.S. ESP initiatives and the need for cooperation among industry, government and law enforcement.

Awareness among Law Enforcement

All law enforcement interviewees indicated that law enforcement knowledge has been increased due to the Strategy, mainly in the area of investigative and legal challenges. Specific knowledge acquired includes: increased knowledge of the Criminal Code; increased knowledge of reporting; age of consent; mandatory reporting; and increased knowledge and awareness about the crime in general. Interviewees noted several benefits of gaining this knowledge: the ability to support less experienced law enforcement; having unique knowledge in areas such as the luring sections of the *Criminal Code;* and the improved communication between stakeholders and the subsequent improvement of cooperation.

Interviewees noted that NCECC training, conferences and speaking venues contributed the most to the increase of law enforcement knowledge. Opportunities to network and educational materials were also mentioned. This was supported by other stakeholders, with training being identified as the most significant contributor to knowledge increase for law enforcement. Areas for further development for law enforcement include more focus on investigative and legal challenges, training on how to identify a hands-on offender and increased information on ISPs.

In the Formative Evaluation[51], interviewees spoke of the need to have properly trained personnel in the area of child sexual exploitation. To respond to these needs, the NCECC developed two Internet Child Exploitation Courses, the Canadian Internet Child Exploitation (CANICE) Course and the Advanced Internet Child Exploitation Course (AICEC). As of the end of 2006-2007, cumulatively, over 200 officers were trained via these courses. As well, in 2006-2007, the NCECC developed a training video for first responders with the Ontario Police Training Video Alliance and the NCECC delivered the Covert Internet Course to 20 candidates. In addition, the NCECC works with its partners to offer the P2P Workshop, with approximately 50 officers having received this training. Investigators also suggested that Lawful Justification and C24 training be provided, and subsequently five officers have been trained as of June 2007.

[51] Formative Evaluation of the National Strategy for the Protection of Children from Sexual Exploitation on the Internet, June 2007

The course feedback summary from the March 2007 CANICE course indicated that this course was successful in expanding law enforcement knowledge of the investigative process when dealing with Internet child exploitation cases. The candidates indicated that they were taught hands-on skills in a controlled environment, and that they benefited from the exposure to different methodologies employed by the different agencies represented on the course (RCMP, OPP, municipal police forces and Crown prosecutors).

Feedback has also been collected on the NCECC communiqué and website. The NCECC communiqué is designed to update partners on the strategic direction of the NCECC and provide updates on operational files[52]. The majority of participants provided positive feedback and agreed that the Communiqué provides valuable and interesting information that they proactively forward to others. Feedback on the NCECC website was also positive with 79% of participants familiar with the NCECC website. The website was noted as being useful for preparing presentations to new members, accessing investigative success stories, and for research and development purposes.

Awareness among Judicial Partners

Judicial partners interviewed indicated that their knowledge has increased the greatest in the area of law enforcement best practices, mainly through the FPT Cyber-crime Working Group meetings, in which PS and the RCMP are active members, and the NCECC sponsored conferences. However, with the quickly changing environment, one interviewee noted that the judiciary should be trained in the area of technology. Other areas for future training were noted as follows: sentencing (some inconsistencies among provinces); education on the crime (40-80% of people who collect pornography will act on their fantasies); and technology (interpretation of the Internet as being a public space). However, it was noted that finding experienced trainers would be a challenge and the interpretation of the CNA tool remains to be set in case law.

Awareness among Judicial Partners

Judicial partners interviewed indicated that their knowledge has increased the greatest in the area of law enforcement best practices, mainly through the FPT Cyber-crime Working Group meetings, in which PS and the RCMP are active members, and the NCECC sponsored conferences. However, with the quickly changing environment, one interviewee noted that the judiciary should be trained in the area of technology. Other areas for future training were noted as follows: sentencing (some inconsistencies among provinces); education on the crime (40-80% of people who collect pornography will act on their fantasies); and technology (interpretation of the Internet as being a public space). However, it was noted that finding experienced trainers would be a challenge and the interpretation of the CNA tool remains to be set in case law.

Awareness among ISPs

ISP interviewees noted that their knowledge has increased mainly with regard to understanding investigative and legal challenges as well as measures to overcome challenges, particularly with

[52] NCECC Contributions to the Achievement of the G8 Objectives, June 2007.

regard to the CNA tool. ISPs noted that they are now more aware of what Crown prosecutors do with this type of information, and how it is used in a case. The Canadian Coalition against Internet Child Exploitation (CCAICE)[53], in which PS and the RCMP are active players, is a multi-sectoral collaboration group that was seen as a benefit to ISPs. PS and the RCMP have had the opportunity to improve collaboration and advance discussion with ISPs through the FPT Cyber-crime Working Group. As well, other opportunities provided by the NCECC for information exchange were seen as helping to increase knowledge. Other interviewees noted that ISP knowledge has increased as a result of the Strategy, mainly through CCAICE and conferences. Law enforcement noted that this increase in knowledge has contributed to a cooperative relationship between themselves and ISPs. However, interviewees noted that a focus on legal issues such as use of the CNA tool and civil liability assurances needs to continue. At the moment, ISPs are often declining to provide a customer name and address to law enforcement due to fears of civil liability, thereby affecting the working relationship between ISPs and law enforcement. As well, one ISP noted that since smaller ISPs are still providing limited cooperation, they need a better understanding of law enforcement challenges which may be achieved through the recent approach to regional ISPs to participate in CCAICE. Finally, ISPs noted that they require clarification on their role when local child welfare and community agencies are involved in the case.

Moving Forward: Potential Areas of Improvement

National training needs are continually assessed by the NCECC. The NCECC has recognized gaps from feedback forms submitted by candidates, and content is currently being revised to improve all courses, as well as identify new training needs. As well, feedback received at the Internet Safety Symposium indicted that there is a need to develop further awareness, training and communications strategies to inform the public on the prevalence of IBCSE and to enhance stakeholder partnerships, particularly with ISPs, and develop partnership with victims and youth. Potential areas of training include[54]: the prevalence of the type of Internet usage in relation to children (e.g., Facebook, MSN); sex offender trends (new tools and software); luring investigations; interview techniques; and more information on the VGT.

Impact of the Strategy on Law Enforcement Collaboration and Information/ Intelligence Sharing[55]

Inception documents of the Strategy clearly outline the intended benefits of working in partnership. The documents indicate that because each complaint may implicate multiple suspects across jurisdictions, coordination among federal, provincial and municipal enforcement, as well as internationally, is very important. Interviewees were asked if activities implemented under the Strategy have had an effect on law enforcement collaboration and

[53] CCAICE is a voluntary group of partners who work to reduce child sexual exploitation on the Internet. Members include: NCECC, Department of Justice, Industry Canada, Canadian Association of Internet Providers, AOL Canada, Bell Canada, Cogeco, Microsoft Canada, TELUS, Rogers, Shaw, MTS, Yahoo!Canada, and SaskTel. CCAICE first met in July 2004 and established a National Action Plan in November 2005.

[54] Participant feedback summary (NCECC Annual Conferences 2004-2007) – Data from 2007

[55] References evaluation questions 5 and 6: To what extent has law enforcement collaboration been enhanced through information sharing and partnerships? and To what extent is information and intelligence being shared nationally and internationally?

information/intelligence sharing. Specifically, interviewees were asked to comment on the impact of conferences and training; investigative tools, such as CETS and image databases; working in partnership; and investigative support from the NCECC. Document review was used to supplement interview findings.

Conferences and Training

Many of those interviewed stated that the working relationship and information sharing among law enforcement has been enhanced through conferences and training. Many field resources mentioned that the NCECC Annual Conference is an important forum for getting to know people personally. They cited the most significant benefit of attending the annual event to be the fact that they were able to "attach a face to a name" and know who to call directly for information. Other noted benefits of the conferences were the ability to share information and best practices, bring everyone up to speed, build capacity, identify gaps and discover common solutions. Interviewees further indicated that attendance at conferences and training helps those working in the field develop standardized terminology which facilitates communication and information sharing. Finally interviewees indicated that the conferences themselves provide a real-time opportunity to share information and actually work on cases together in the same location.

Document review supported these findings. The "ability to network" was the predominant theme from participants who completed feedback forms for the NCECC Annual Conference from 2004, 2006, and 2007. Participants were asked to rate whether "This workshop provided the opportunity to network". This statement consistently received a rating of between 4.7 and 4.9 on a scale of 1-5[56] for 2004-2007[57]. "Information sharing/learning" was the predominant theme for 2005 where participants included comments such as: "I have a vast list of people to call to assist me in an investigation. We can put faces to names and this is easier to communicate later."

CETS and Investigative Tools

Many field interviewees indicated that CETS has provided little enhancement to their working relationships or to information sharing and that there are outstanding issues. They expressed the hope that CETS would be stronger in the near future, but also stated that usability, cumbersome access (e.g., too many passwords), time-consuming data entry, and the fact that CETS is not universally adopted by Canadian law enforcement have been issues. Others stated that CETS will not work with their databases. Some see the CETS tool as a burden in terms of data entry, but thought that retraining may help people understand that taking a few minutes to enter data will provide vital information.

Interviewees expressed concern that the less CETS is used, the larger the gaps in investigations, because information that could be shared is not in the system. Some believed that Canada is lagging behind other countries on the technological side, both in terms of CETS and the image database, which has not yet been implemented. To this end, some expressed that they are

[56] Opinions were rated on a scale of 1 (strongly disagree) to 5 (strongly agree)

[57] Source: Participant feedback summary NCECC Annual Conferences 2004-2007 and Internet Safety Symposium 2008. [58] Source of statistics: CETS Canada – Update 2008. Note: "online identities" is all the identities that a person can assume online. This could be an e-mail address, screen name, nickname, login ID, IP address.

currently using C4P to categorize images in place of having a national database that would more consistently categorize images on a national basis. Others noted the use of GROOVE, in place of CETS, as a secure place to share investigative information.

Document review was somewhat contradictory to these finding. Statistics indicate that, as of February 2008, CETS had 287 trained users and 24 of 32 agencies were regularly contributing to CETS. As a result, the system contained 5,156 investigations and 11,789 pieces of online identity information[58]. The few field level interviewees that are using CETS noted the benefit that they can share information and connect quicker with others who are using CETS.

Investigative Support from the NCECC

About half of interviewees believe that investigative support from the NCECC has enhanced their working relationships and improved information sharing. They stated that the NCECC provides a positive international liaison and national connection point that did not exist four years ago. There was an appreciation that the NCECC provides a focal point for information sharing so that less duplication of effort is occurring; the proper jurisdiction is handling files; and investigators can now share information with all parts of the country through the NCECC if they choose. Interviewees also expressed that confidence and trust with the NCECC has increased. The investigative packages that they receive from the NCECC are more complete and actionable, and that investigations are now moving forward. Others stated that they are now receiving high quality investigative packages in a timely manner, noting that the NCECC used to have a six month backlog, and that now there is no backlog.

A few field level interviewees had suggestions for improvement that included further work on victim and suspect identification through the establishment of the image database; improved consistency in terms of how files are sent from the NCECC to the field (e.g., GROOVE vs. hard copy); improved speed of some outgoing and incoming requests; and the possibility of providing funding to municipal partners to enable participation in working groups. Finally, some stated that, although they are now getting better files packages, which include preliminary investigative steps, the field level does not have the forensic or investigative support to clear the files.

National Partnerships

As shown in the table below, conference participation in the NCECC Annual Conferences also provides an indication of the change in the nature of partnerships.

Conference Year:	**2004**	**2005**	**2006**	**2007**	**2008**

[58] Source: 2008 Internet Safety Symposium: NCECC and RCMP "H" Division – Operation Horizon, Dartmouth, Nova Scotia, Recommendations, January 2008, page 3.

Reach					
Location	Winnipeg	Calgary	Fredericton	Ottawa	Dartmouth
Attendance (excluding presenters and NCECC staff)	54	84	73	107	70
Representation (# of investigative units dealing with child exploitation	41 units	26 unit + 10 RCMP	34 units	64 units	law enforcement (45), government (25), industry (10)

The table illustrates that the conference (or symposium) has not only grown in the number of police services represented, but in 2008 the conference was run in an integrated fashion with law enforcement, government and industry representation. "It became evident during the Symposium that co-operation and collaboration between law enforcement, government and industry is crucial in Internet-facilitated child sexual exploitation investigations. Almost all of the participants indicated that the Symposium provided a better understanding of the need for cooperation".[59]

The work of *Cybertip.ca*, which was subsumed under the umbrella of the Canadian Centre for Child Protection (C3P)[60], in January 2008, has built bridges among law enforcement, the ISP industry and government. For example, one of the main achievements is the establishment of the CCAICE, which is chaired by *Cybertip.ca*. In terms of information sharing among ISPs and law enforcement, one of the major accomplishments of CCAICE is the development of the CNA template. Interviewees frequently mentioned the progress that has been made in the working relationship with ISPs, mostly in central and western Canada. A few interviewees cited the CNA tool as an agreement that has helped working relationships. Having stated this, interviewees also acknowledged that not all ISPs are "on board" in terms of responding to CNA requests, especially in Atlantic Canada. PS (as the policy lead) and the RCMP (as the operational lead) continue to work with ISPs through CCAICE and other FPT fora to advance the file. PS is also providing leadership on the lawful access initiative, which encompasses discussions on CNA, in consultation with Industry Canada, as well as on PIPEDA.

International Partnerships

In terms of partnerships on the international front, the Strategy's main interactions are through the NCECC with the G-8 Strategy against Sexual Exploitation of Children on the Internet; the VGT; and operational work with Interpol, Europol and law enforcement in other countries on ongoing investigations. The G-8 Strategy defines eight objectives in terms of collecting information, identifying victims, locating suspects, legislations, police tools, cooperation with private players, prevention and international cooperation. "The VGT is made up of law enforcement

[59] Source: 2008 Internet Safety Symposium: NCECC and RCMP "H" Division – Operation Horizon, Dartmouth, Nova Scotia, Recommendations, January 2008, page 3.

[60] The Canadian Centre for Child Protection (C3P) is a not-for-profit charitable organization dedicated to the personal safety of all children. Its goal is to reduce child victimization by providing programs and services to Canadians. Through public awareness activities, C3P provides personal safety education program (Kids in the Know) and the national tipline to report online sexual abuse of children (*Cybertip.ca*). See http://www.protectchildren.ca/app/en/whoweare.

agencies from around the world working together to fight child abuse online[61]. The objectives of the VGT are to make the Internet a safer place; to identify, locate and help children at risk; and to hold perpetrators appropriately to account."[62]

Document review indicates that contributions from the NCECC to the G-8 objectives and the VGT that have enhanced collaboration and information sharing include participating in the VGT tipline; increased networking through work exchanges with the FBI's Innocent Images International Task Force; and collaboration with 28 countries during a session organized by Europol in The Hague (May 2007) on an ongoing operation that involved thousands of international targets. Without the existence of the NCECC and Canada's participation in the VGT opportunities for collaboration and information sharing such as these may not have been presented to Canadian law enforcement.

Many interviewees stated that working groups and partnerships have enhanced their working relationships. Many spoke about the positive work of the NCECC in building international relationships with the U.S., the U.K. and Australia and working with the VGT. They indicated that the NCECC has done a lot to build international partnerships and provide exposure to a broad international representation of law enforcement. The feedback summary from the NCECC Annual Conference in 2006 echoed this finding indicating that the majority of participants commented on the NCECC's success in liaising between agencies and countries for the protection of children.

A few interviewees departed from this point of view, indicating that the NCECC does not provide the right level of representation on the VGT and that membership could be more strongly represented. The suggestion was that the RCMP/NCECC should provide the right level of empowerment in the international arena in order to facilitate decision making and the advancement of a strategic agenda. It was also stated that Canada cannot fully maintain its partnership on the VGT because the NCECC does not have the resources to do so.

Impact of the Strategy on Investigations[63]

The evaluation examined the extent to which Strategy, via the NCECC, has contributed to coordinated, comprehensive and efficient national and international investigations.

Coordinated

Since increasingly more IBCSE investigations are international in scope and technologically complex, and because each complaint may implicate multiple suspects across jurisdictions, there is an increased need for coordination among federal, provincial and municipal enforcement agencies. Most of those interviewed indicated that, generally, the Strategy has contributed to more coordinated investigations since 2004. Most commented that the NCECC is the main point of contact between national and international agencies. They added that, prior to the Strategy, since

[61] The VGT is made up of the Australian Federal Police, the Child Exploitation and Online Protection Centre in the UK, the Italian Postal and Communication Police Service, the Royal Canadian Mounted Police, the US Department of Homeland Security and Interpol.

[62] Source: http://www.virtualglobaltaskforce.com/what_we_do.asp

[63] References evaluation question 8: To what extent has Strategy contributed to coordinated, comprehensive and efficient national and international investigations?

there was no single contact point, international partners did not know which law enforcement agency they should refer to for an investigation, and there may have been more than one law enforcement agency each working independently on the same file. Now there is a single point of contact for international partners to go to with a case referral. The biggest risk noted by interviewees is that without the coordination provided by the NCECC, vital information to solving cases would be overlooked or lost.

Document review and quantitative information provided some support to these findings. For example, the NCECC Business Plan for 2008-09 states that "within the priority of combating IBCSE, the NCECC was the coordinating component of 18 multi-national and multi-agency files. As well, the Victim Identification Unit currently collaborates on approximately five international investigations per week via GROOVE[64] and daily with over 18 countries to visually compare images. This helps to eliminate duplicate investigations, thus enhancing the effective and efficient use of police resources globally."[65]

In terms of coordinating and centralizing the processing of case files, from January 2004 to January 2008, the NCECC handled a total of 2083 reports of crimes related to offences against morals[66]. A total of 559 files were handled / processed by the NCECC between November 2007 and April 2008, with a total of 918 targets being identified[67]. As of April 2008, a total of 209 (37.4%) cases have been concluded. Other data regarding the number of investigative packages sent to local jurisdictions was not available to the evaluation.

Comprehensive

The act of ensuring that all relevant information is assembled by the NCECC to be sent out to local jurisdictions makes investigations more comprehensive. This activity includes communication with international law enforcement to fill in information missing from the case file. Large and complex cases are also broken down into complete work packages so that there are fewer gaps in information.

From June 2006 to February 2008, a total of 7,350 targets were investigated in 37 different investigations[68] resulting in the investigation of between one and 5060 potential subjects of interest[69]. In response, the NCECC developed two reactive teams; one multi-suspect file team responsible for files with more than 10 suspects and one core team that concentrates on urgent cases and files with less than 10 suspects. The primary objectives of each of these teams is to validate that an offence has occurred under Canadian law, to establish Canadian jurisdiction of the targets, and to ensure sufficient evidence has been provided. A detailed investigative

[64] Groove is a secure peer-to-peer collaboration software that allows users to work together in a more efficient manner sharing files and messages in real-time without a database.
[65] NPS Sub-Activity – The National Child Exploitation Coordination Centre Business Plan 2008/2009.
[66] Records Management System – Occurrence Statistics. This information does not distinguish if there is one more target. These crimes included 1,698 reports of the transmission of child pornography; 185 reports of luring minors over the Internet for sexual purposes; 64 reports related to the printing or publishing of child pornography; 54 reports of the possession of child pornography, as well as other crimes related to IBCSE.
[67] NCECC Internal Statistical Reporting. NCECC implemented this system to more accurately capture information from investigations. The number of targets identified will increase as file information is updated at case conclusion.
[68] NCECC Summary Report 33
[69] This information reflects the number of targets in investigations that is not tracked in the RCMP Records Management System.

package, inclusive of validated information/intelligence, was forwarded to the appropriate police agency by these teams. The development of these comprehensive investigative packages eliminated the need for the jurisdictions to conduct the preliminary work.

The level of cooperation from ISPs has hindered investigations from becoming more comprehensive because investigations become "un-actionable" when ISPs do not provide information. For the six month period between November 2007 and April 2008[70], the total number of unsuccessful[71] Law Enforcement Requests (CNA requests) to ISPs in Canada was 163 (3 6.5%), with the average turnaround time for a reply being nine days. The total number of unsuccessful U.S. Administrative Subpoenas was 55 (38.6%)[72] and the average time for a U.S. Administrative Subpoena was 19 days. These files were concluded with no further action.

Efficient

Interviewees commented that the Strategy has improved efficiency since 2004 through the NCECC 's front end work on cases and through the triaging of incoming complaints by *Cybertip.ca*. The NCECC eliminates cases that do not require further investigation, reducing the need for local police forces to spend time preparing these cases. Interviewees noted that with the NCECC triaging the reports and preparing packages, field work is accelerated because the front-end work is already done. In addition, *Cybertip.ca* statistics show that, at a minimum, Canadians have reported 11,509 incidents. To the end of 2007, only 9% (1,091) of what Canadians reported was forwarded by *Cybertip.ca* directly to provincial and municipal law enforcement agencies (excluding NCECC)[73].

Interviewees also commented on the improvements they have seen in casework as a result of the work of the NCECC. For example, in a case originating from Texas prior to the Strategy, interviewees noted that information was handed off to Canadian authorities with no knowledge of where the information should go. This resulted in the failed investigation of the case. However, today, cases of this complexity are dealt with on a monthly or weekly basis, and with the NCECC being the main point of contact, cases are handled more efficiently. These cases are now sent to relevant units across Canada for investigation, and investigators are more knowledgeable about their role in the case. Interviewees noted that without the front-end assessment completed by the NCECC, duplication of effort would be a big risk. Now, packages are assembled with international cooperation and technological issues are dealt efficiently. As well, field units are better able to prioritize cases and investigations based on the intelligence provided to them by the NCECC.

Document review and quantitative information supports these findings. During the Formative Evaluation, it was found that backlogs still existed at the NCECC. As competence and expertise increased and systems were streamlined, the information was more efficiently handled and currently, no specific backlogs exist. Metrics provided by the NCECC show that, not only has the backlog been reduced, turnaround times are being achieved. For high risk investigations

[70] Prior to October 2007, the NCECC did not track this information.

[71] Unsuccessful refers to an ISP refusing, ignoring or no longer having the information.

[72] Summary report on number of cases/ investigations impossible to complete due to missing information to identify suspect.

[73] A vast majority of reports, however, are sent directly to the NCECC for preliminary investigation.

(child or suspect child at risk), the investigation must be forwarded by the NCECC within 24 hours to the appropriate law enforcement agency; the NCECC realized a 100% achievement on this goal for 2006-2007[74]. For all other investigations, the NCECC must forward the material within seven days unless the NCECC is waiting for follow-up information from an ISP or where further investigation is required; the NCECC realized an 80% achievement on this goal for 2006-2007.[75]

Efficiencies have also been gained by *Cybertip.ca* and the NCECC through the improved process of handling of websites with suspected illegal content. Originally, *Cybertip.ca* sent reports related to foreign hosted URLs to the NCECC who would then generate an investigation and forward it to the appropriate jurisdiction. Now, *Cybertip.ca* gets the information directly to the jurisdiction or country or transfers information through the International Association of Internet Hotlines (INHOPE).[76]

Conclusions – Law Enforcement Capacity Building and Operations

5. The Strategy has been successful in increasing the knowledge of target audiences in the areas of investigative challenges, best practices and measures to overcome challenges. This outcome is directly attributable to the efforts of the Strategy. For law enforcement, training and the NCECC Annual Conference are the strongest contributors to success in this area. Raised awareness of judicial partners, such as provincial crown prosecutors, is attributed mainly to participation in the Federal Provincial Territorial (FPT) Cyber-crime Working Group (CWG). Raised awareness among Internet Service Providers (ISPs) is attributed mainly to work on Canadian Coalition against Internet Child Exploitation (CCAICE). Remaining work includes: continued training on trends in sex offender methods, Internet usage among youth and training on investigative techniques for law enforcement; education on the nature of the crime among judicial partners, and continuing awareness efforts on legal issues with ISPs.

6. Law enforcement collaboration and information sharing has been enhanced a great deal through the NCECC Annual Conferences, investigative support from the NCECC, and through the building of international relationships. Information sharing has been well coordinated by the NCECC through the provision of high quality investigative packages. Limited buy-in of the Child Exploitation Tracking System (CETS) by some law enforcement agencies and the fact that the image database has not been implemented is hindering information sharing. The NCECC Technology Section continues to address detracting issues.

7. Through the efforts of the NCECC and the work of *Cybertip. ca*, the Strategy has contributed to coordinated, comprehensive and efficient investigations. NCECC provides a single point of contact from which complete investigative packages are sent to the appropriate jurisdiction. *Cybertip.ca* has also realized efficiencies and taken the burden off of police by triaging complaints and forwarding complaints requiring follow-up directly to local

[74] NPS Sub-Activity – The National Child Exploitation Coordination Centre Business Plan 2008/2009.
[75] NPS Sub-Activity – The National Child Exploitation Coordination Centre Business Plan 2008/2009
[76] INHOPE was founded in 1999 under the EC Safer Internet Action Plan. INHOPE represents Internet Hotlines all over the world, supporting them in their aim to respond to reports of illegal content to make the Internet safer. Source: https://www.inhope.org

jurisdictions. The NCECC has reduced backlog and is achieving targeted turnaround times. Despite this success, some investigations are being hindered by lack of cooperation from ISPs in providing responses to Customer Name and Address (CNA) requests which renders an investigation un-actionable.

3.2.2 Public Awareness and Reporting[77]

Beneficiaries of the educational component of the Strategy included children, parents, teachers, and the Canadian public in general. To determine the level of success reached in the area of public education, the evaluation examined two areas. The first of these was the extent to which public education efforts have contributed to enhanced awareness of the nature of the crime, exploitation signs, prevention behaviours, and reporting mechanisms among the general public and target populations. The second was the extent to which enhanced awareness activities has contributed to enhanced reporting.

Changes in Public Awareness

Two Strategy partners were originally funded to conduct public education activities: *Cybertip.ca* through a contribution agreement with PS, and IC through the SchoolNet Program. These two components were designed to assist Canadian parents and teachers by providing useful tools designed for their children and students. However, in 2007, Industry Canada informed PS that they were no longer in a position to manage and operate their *CyberWise.ca* Website. PS lead the transfer of funding and responsibilities related to public education and awareness to the C3P which manages *Cybertip.ca* and Kids in the Know (KIK) program. Therefore, the discussion that follows focuses on C3P education and awareness efforts.

To ensure that the content of the *CyberWise.ca* Website was not lost, PS worked with Industry Canada and *Cybertip.ca* officials to transfer the content of *CyberWise.ca* related to child sexual exploitation to *Cybertip.ca*. The content related to Internet Safety, which was also contained on the *CyberWise.ca* Website, was transferred to Internet 101, an RCMP initiative that promotes the safe use of the Internet.

Cybertip.ca plays an important role regarding public education and referrals. The Canadian public can access a variety of important information from its web portal regarding the victimization of children. Additionally, the web portal offers resources that assist families across Canada in dealing with a variety of child safety issues. This includes programs and services for victims of sexual exploitation, connections to other agencies with related expertise, as well as tiplines located in other countries.

Documents indicate that *Cybertip.ca* has executed six national campaigns since its launch in January 2005. The main reporting audience, those aged 3 1-50, was deemed to be the target audience for these campaigns based upon the highest percentage of reports coming from this age

[77] References evaluation questions 7 and 9: To what extent have public education efforts contributed to enhanced awareness of the nature of the crime, exploitation signs, prevention behaviours, and reporting mechanisms among the general public and target populations? And To what extent has better awareness contributed to enhanced reporting?

range. Key components of these campaigns included outdoor signage, web marketing, public service announcements, magazine ads and stories, print material and partnerships. Success is demonstrated by the fact that public awareness campaigns across the country have been immediately followed by a marked increase in reporting and educational downloads by Canadians. For example following particular campaigns, reports increased by as much as 103%, educational downloads increased by as much as 55%. *Cybertip.ca* officials have also provided numerous keynote addresses at various fora across the country using an inclusive, community-based approach to heighten safety awareness. Education efforts are also geared to raising awareness of the tipline itself, and a recent survey shows that 15% of Canadians are now aware of *Cybertip.ca*, the national reporting tipline[78].

Other measures that demonstrate *Cybertip.ca* success include the fact that *Cybertip.ca* averaged 80,000 hits per month to its web portal, many of which where to obtain important online safety information. To date, from 2002-2007, over 26 million hits to the website have been tracked[79] with over 3.5 million page views. *Cybertip.ca* also reports 300,000 education downloads from 2005-2007.

The awareness mechanism is the Kids in the Know (KIK) program administered by C3P. This is an interactive safety education program used to increase personal safety and to reduce the risk of victimization and sexual exploitation of children from kindergarten to high school[80]. In addition to the curriculum, the program includes: training programs for educators, parents, and communities; downloadable activities for families; children's books and hand puppets; posters and safety sheets; and research into patterns of victimization. In addition, student advisory groups are held with the goals of consulting with young people about their online and offline experiences, to pilot new education material and to empower young people.

According to statistics provided by *Cybertip.ca*, the KIK program is being utilized in most provinces (not yet used in the territories); however, PEI and NS do not yet have the program as an approved educational resource. According to the *Cybertip.ca* interviewees, the use of this program in 10 districts was recently evaluated, with a range of French, English, Catholic and public districts being included in the study. However, at the time of this report, the results of the evaluation were not available. *Cybertip.ca* interviewees also noted that anecdotal evidence has been received about the importance of the KIK program. One comment received from a teacher was that the material facilitated disclosure of Internet safety incidences in their school. Another comment received from parents by *Cybertip.ca* staff was regarding the helpfulness of these materials within the Toronto Safe Schools Network.

Interviewees noted that public education efforts have contributed to enhanced awareness. A few noted that the distribution of information, including the use of *Cybertip.ca*'s school based curriculum in schools, demonstrates that knowledge is increasing. Anecdotal evidence has also been collected on the usefulness of public education. Interviewees noted that children repeated the tips that they learned through the various school programs, and parents have provided feedback

[78] Pollara, May 2007 – as quoted in the Public Awareness Deck
[79] http://www.cybertip.ca/app/en/stats
[80] KIK Fold-Out

after viewing a presentation, that their children have proactively changed their Internet settings to protect themselves.

Also used in the schools is the Billy educational kit[81]: This initiative resulted in 11,000 Billy kits mailed to teachers, with 9500 English and 1500 French kits being sent out. Provincial distribution of the pamphlet was national in scope, with 41% distributed in Ontario, 14% in Alberta, 14% in British Columbia and 12% in Quebec. A postcard was sent out to 500 random schools in order to gauge effectiveness, and teachers felt that Billy was an effective tool for teaching personal safety[82], with 83% of respondents indicating that the kit was very user friendly. A total of 98% of those who responded to the survey indicated that they would use the kit again the next school year.

The C3P also participated in Safer Internet Day, held in February 2008, which is an internationally recognized day to promote the importance of safe and responsible Internet use[83]. Forty countries participate in Safer Internet Day through a variety of activities. For this event, the C3P distributed 2.4 million age-appropriate Safety and the Internet brochures to the parents of 8-15 year olds, issued media releases and conducted media interviews, and promoted the day through online tools. Broad provincial distribution of the brochures was achieved, with at least 7% of the adult population receiving the brochure. In order to gauge adults' understanding of Internet safety issues following Safer Internet Day, a short survey was posted online. The survey was completed by 178 people representing most Canadian provinces (64% of the responses were from Ontario), and these respondents indicted that out of a rating of one to five (five being high), their knowledge increased to an average of 4.4 from 3.7 prior to Safer Internet Day. Safer Internet Day also resulted in other increased awareness. *Cybertip.ca* noted a 240% increase in educational downloads and an increase in page views by 130% following Safer Internet Day. As well, orders for the KIK program tripled.

Interviewees commented on the educational and awareness efforts that they see as providing a significant contribution to increased knowledge and awareness. Interviewees noted that public service announcements (including television campaigns), advertising about *Cybertip.ca* through the media, *Cybertip.ca* prevention activities such as the distribution of materials (posters, pamphlets, KIK program), direct website links from various policing organizations to the *Cybertip.ca* website, billboards, and the distribution of educational DVDs to law enforcement such as *Stolen Innocence,* all contribute to increased awareness.

Many interviewees identified challenges and opportunities faced when working to increase knowledge in the target populations. A few of these interviewees noted that most data on knowledge increase is collected anecdotally, and any measured knowledge increase is difficult to attribute to any one initiative. Some suggestions included becoming better engaged with tools used by youth such as Facebook, Myspace and by having a "report abuse" button on these pages, and that the NCECC could get more directly involved by hosting Safer Internet Day. It was noted that a more active role in education and awareness of IBCSE could be played by *Cybertip.ca* in

[81] Billy Brings His Buddies, 2007-2008 Evaluation
[82] Based on 161 responses between September 9, 2007 and January 31, 2008.
[83] Safer Internet Day Evaluation, 2008.

Quebec and Atlantic Canada, as awareness materials in Atlantic Canada were noted to be out of date and lacked extensive distribution.

While awareness efforts for health professionals are being made, this is a continuing area of improvement for both *Cybertip.ca* and the NCECC. *Cybertip.ca* has only recently made connections with Health Canada and social service and child welfare groups and is working to build relationships with them across the country. The NCECC is also making headway to address the knowledge gaps in the health sector. Since 2007, the NCECC has been working on a joint research project with the Child and Youth Protection Program at the Children's Hospital of Eastern Ontario, the Suspected Child Abuse and Neglect Program at the Hospital for Sick Children and the Ontario Network of Sexual Assault/Domestic Violence Centers. The project is the first of many that will gather information from health care clinicians as well as sexually assaulted children and youth with respect to IBCSE.

RCMP and Awareness Building

The NCECC is uniquely positioned as the operational coordination centre nationally and plays a key role in raising public awareness about the Internet, child exploitation, and policing in this field. In this respect, the following is a list of some of the activities that have been held to support this function. However, unlike C3P, the NCECC is not directly funded to conduct these activities.

- In 2006, the RCMP contributed to the development of an anti-trafficking video, pamphlets, and posters, which were provided to law enforcement agencies nationally/internationally.
- The NCECC participated in the development of the *Stolen Innocence* video. This video was disseminated across Canada to increase awareness of investigational guidelines for IBCSE.
- The National Youth Cybercrime Awareness Conference was held in Ottawa in June 2004. The conference was attended by 39 youth aged 17 through 21 from across Canada.
- To address the topic of the needs of victims, NCECC representatives provided several presentations to Victim Advocacy Groups.
- Deal.org[84] developed three public service announcements in partnership with the NCECC.
- The NCECC worked with Deal.org to present a workshop to undercover police officers about youth trends and popular culture. This information was disseminated to national and international law enforcement agencies to support undercover police officers.
- CCAICE, of which the NCECC is a partner, ran a national public awareness campaign concurrently with the *Cybertip.ca* awareness campaign.
- In 2006, NCECC took part in a joint national initiative with Safe Canada, Service Canada, Internet 101, Deal.org, Industry Canada and Childfind Manitoba to advertise Internet Safety.

These activities are ongoing and NCECC has been proactive in developing a plan that identifies the key audiences, key messages, and most appropriate means of delivering these messages to both internal and external audiences. This plan is being implemented to effectively communicate the NCECC's mandate, role, and the issues around IBCSE.

[84] The RCMP Deal.org program is a by youth, for youth web-based initiative that acts as an information resource and crime prevention tool for youth aged 12-17.

Interviewees noted the importance of ensuring coordinated efforts among awareness and education activities between C3P and the RCMP. With the RCMP's focus on prevention, and with the police often being the first point of contact when the public wants information, interviewees noted that consideration should be given to fund these activities. However, good cooperation between the law enforcement and *Cybertip.ca* was noted, with the RCMP promoting *Cybertip.ca* in their presentations, and certain police services having a direct link to *Cybertip.ca* on their website. While interviewees did not feel that efforts were currently being duplicated, they expressed that coordination among awareness efforts would result in cost savings and consistent messaging. To this end, a communication plan has been developed recently by PS to ensure that efforts, related to public education and awareness, are not duplicated.

Reporting

In addition to being a source of education and awareness, *Cybertip.ca* is Canada's national tipline for reporting the online sexual exploitation of children. *Cybertip.ca* accepts and addresses online and telephone reports from the public regarding child pornography, online luring, child exploitation through prostitution, and travelling to sexually exploit children. *Cybertip.ca*'s technical infrastructure rivals the best tiplines in the world and is capable of handling a large volume of reports as the initiative expands on a national basis, while in turn providing the security required to protect the sensitive information that is handled by the tipline. Having a specialized mandate is generally considered a best practice as it allows the tipline to focus expertise and build capacity in specific areas, making it more effective and addressing the type of Internet crime for which they were established.

Since 2005, *Cybertip.ca*'s tipline has received over 25,000 reports with the tipline receiving an increasing number of tips year after year for each province, as well as the marked increase in reports after education and awareness campaigns. Between 2002 and 2004, *Cybertip.ca* received a total of 1,912 reports, including cases of child exploitation and educational responses. In 2005, this number tripled to 6,788 reports and 8,093 cases were reported in 2007. *Cybertip.ca* reporting breaks down per capita with a ranking from highest to lowest as follows: Ontario, Quebec, British Columbia and Alberta. Many reports have also been received from the United States, England, Denmark and other countries. Within its first year of operation, *Cybertip.ca* received over 550 reports regarding either criminal acts against children or requests for educational resources and support[85] which was a 430% increase in tips over the previous year[86]. To date, *Cybertip.ca* has received over 7,000 reports dealing specifically with websites, 216 of which involved a Canadian web host[87]. The public response to *Cybertip.ca* has exceeded expectations and confirmed the belief that Canadians needed and wanted a place to report these crimes against children. Moreover, *Cybertip.ca* bridged the gap between those who wanted to report these types of crimes against children and the law enforcement agencies that needed the information to identify and investigate those who exploit children.

Conclusions – Public Awareness and Reporting

[85] Cybertip ! ca. Taking Stock a Year Later. Annex A
[86] Public Awareness and Education Session, February 2008, Vancouver BC.
[87] http://www.cybertip.ca/app/en/stats

8. The work of the Canadian Centre for Child Protection (C3P) has greatly contributed to enhanced awareness among the general public. This is evidenced by the marked increases in reporting and educational downloads immediately following campaigns. There is evidence that children and parents are being reached because the Kids in the Know (KIK) program is being utilized in most provinces, and 15% of Canadians are now aware of *Cybertip.ca* as the national reporting tipline. In terms of reach, the Billy educational kit has been distributed in Ontario, Alberta, B.C. and Quebec. Evidence indicates that the kit is effective and will be used again by teachers. Limited anecdotal evidence suggests that behaviours have changed as a result of these educational efforts. Educational efforts, geared toward health care professionals and ISPs, are underway but this remains an area that requires continuing improvement. Positive results of a broad-based survey of Canadians would further solidify

   these findings and provide understanding as to whether awareness activities have resulted in preventative behaviours among target groups.

9. Although PS has recently developed a communication plan with participation from all Strategy partners, it appears that some coordination may still be necessary between the RCMP and *Cybertip.ca* in terms of conducting public awareness activities. Document review indicates that there are two communications plans in existence with similar target audiences, one from the NCECC and the other the joint communication plan for the Strategy.

3.2.3 Crime Prevention and Protection of Children[88]

This section outlines the successes that the Strategy has had in the areas of crime prevention, pursuit of suspects and protection of children through the combined efforts of law enforcement and public awareness and education.

Crime Prevention and Pursuit of Suspects

As a measure of crime prevention, or harm prevented, the evaluation sought to quantify the number of arrests, the type and number of charges laid and sentences pronounced as a result of the Strategy.

Cybertip.ca data indicates that as a result of tips being forwarded to law enforcement, as of June 2008, 37 arrests have been achieved due to reports to the tipline[89]. During *Cybertip.ca*'s first year of operation, the tipline forwarded 44% of reports of potentially illegal content to law enforcement agencies, assisting them in shutting down as many as 100 websites housing child pornography, and providing them with information that led to the arrests of 5 individuals who were subsequently charged with possession and distribution of child pornography[90].

---

[88] References evaluation questions 10 and 11: To what extent has the Strategy enhanced crime prevention? and To what extent has the Strategy contributed to enhanced: protection of children from sexual exploitation and pursuit of those who use technology to facilitate the exploitation of children?

[89] http://www.cybertip.ca/app/en/stats

[90] Cybertip ! ca. Taking Stock a Year Later. Annex A

Data available from the NCECC resides solely in case summaries as results of investigative packages sent to local jurisdictions have not been tracked[91]. Summaries of Canadian cases indicate four individuals were arrested between June and September 2007 as a result of case files that were prepared and forwarded to local jurisdictions by the NCECC. Charges laid include possession and distribution of child pornography. There were no dispositions on these cases at the time of this report since there is no mandate or requirement for NCECC partners to provide dispositions to the NCECC on the intelligence disseminated to them.

For international cases, case summaries cited three international investigations initiated by the NCECC that led to the arrest of three individuals and the sentencing of two individuals. The third trial is ongoing in the U.S. In the other overseas cases, the sentences ranged from seven to fourteen years, and in both cases, although they maybe have completed their sentences, the offenders will remain in custody until they are deemed to be safe to return to society.

Success in the area of crime prevention is also measured through the number of websites containing child abuse images that have been shut down or blocked. *Cybertip.ca* data indicates as of June 2008, a total of as many as 2,850 websites have been shut down due to reports to the tipline. The Cleanfeed initiative, implemented by *Cybertip.ca* in November 2006, has reportedly blocked over 11,000 URLs with child abuse images on the Internet[92]. *Cybertip.ca* plays a major role in this area, since most complaints received at the NCECC deal with other areas of child exploitation such as luring attempts and distribution of child pornography over the Internet via emails.

Interviewees stated that the arrest of criminals in this area is critical for preventing the abuse of other children. Two interviewees noted that there has been an increase in the number of arrests made in this area since 2004, and quicker investigations were also quoted by three interviewees as being an enhancement from the Strategy. Another interviewee stated that law enforcement is now able to complete investigations that may not have been completed before the Strategy through the enhancement of the delivery and coordination of files through the NCECC (e.g., less duplication of effort). Finally, it is noted that on June 26, 2008 during the time of this evaluation, charges of child pornography were laid against 27 suspects from various parts of Quebec due to an investigative package sent by the NCECC to the Sureté du Québec.

Protection of Children and Identification of Victims

The Victim Identification Unit (VIU) within the NCECC was established to develop effective methods of identifying and locating victims of IBCSE in order to help counter the effects of abuse suffered by victims. The VIU provides support and assistance through analysis, information and recommendations to partner agencies (national and international) that may or may not locate the victims/offenders in their jurisdictions.

[91] The NCECC faces the challenge of reporting accurate statistics in the area of arrests for several reasons. Although some police agencies do provide feedback/dispositions to the NCECC, the NCECC does not hear back on the majority of packages sent out. To further complicate the reporting statistics, it is extremely difficult to garner information on the investigations with multiple suspects. As well, agencies do report to Statistics Canada at case conclusion but there is no current mechanism, in this reporting, to link the NCECC to being involved. Mandatory reporting on the disposition of all cases needs to be considered.

[92] Public Awareness and Education Session, February 2008, Vancouver BC.

From 2004-2007, 233 victims of on-line child exploitation were identified by Canadian law enforcement partner agencies including the VIU[93]. This number reflects files VIU and other Canadian agencies have forwarded to the international Interpol Data Base. Canadian investigators have also been instrumental in a number of investigations that have resulted in the identification and rescue of numerous foreign children; however, data to support this is not available.

Some interviewees indicated that children are being identified and rescued from abuse as a result of the Strategy, with more victims being identified now versus prior to the Strategy. Interviewees also noted that cases are now being expedited because of the Strategy, mainly from the faster coordination of files (including international files) by the NCECC. Interviewees noted that the protection of children has also been accomplished through involvement in international cases, Project Cleenfeed, increased reporting, as well as through undercover operations.

Interviewees also noted that a significant improvement since the start of the Strategy is that links between cases are being discovered and investigated now versus prior to the Strategy due to the coordination of files by the NCECC.

The need to automate and standardize tools utilized in the identification process is a priority. While there are similarities between child sexual abuse image categorization systems across Canadian police agencies, there is currently no national standardized database. This fact contributes to inconsistent categorization of images across different jurisdictions within Canada and overseas. Consequently, the NCECC continues to develop a computer image database referred to as VOICE system, which will provide access to Canadian law enforcement to the database once established. This image analysis tool will provide a centralized data repository to identify victims and offenders depicted in images, videos and text documents. The tool will be made available nationally and there are plans to share information with international partners who have image databases (e.g., Interpol, United Kingdom). To strengthen the capacity of police partners, multiple agency access to the database is under development.

Conclusions – Crime Prevention, Pursuit of Suspects and Protection of Children

10. From the information provided, it cannot be fully determined whether the Strategy has enhanced the pursuit of suspects; however, it would appear that some progress has been made. Anecdotal evidence indicates that, because of the Strategy, investigators are now able to complete investigations that they would not have been able to complete prior to the Strategy. The NCECC has contributed to 34 arrests while *Cybertip.ca* reports contributing to 37 arrests. The NCECC statistics are based mainly on case summaries as the NCECC is not able to report on the actual number of individuals arrested due to information sent to law enforcement agencies. It is probable that the figure significantly under represents the number of arrests, charges and prosecutions because many field investigation dispositions have not been completed. In addition, law enforcement agencies are not reporting back on the results of the information that was sent from NCECC.

[93] Summary report on trend in number of children identified and located as result of the NSPCSEI.

11. In terms of prevention efforts, offenders have been prevented from accessing child exploitation material through the shutting down of 2,850 websites by *Cybertip.ca* and through the blocking of access to 11,000 URLs through the efforts of project Cleanfeed. It cannot be determined whether or not these efforts contributed to preventing abuse of children but it can be said that it is possible that offenders and the Canadian public have been prevented from viewing offensive material.

12. Protection of children has been enhanced through the identification of 233 victims. These results are not attributable solely to the Strategy since other Canadian law enforcement agencies have contributed to this result. It is also noted that Strategy partners have provided programs to help children build their self-esteem which helps to reduce their vulnerability of victimization. Protection of children could potentially be enhanced through the implementation of the image database originally envisioned as part of the Strategy, but yet to be implemented.

3.2.4 Impacts on Success due to the Evolution of the Strategy[94]

As previously mentioned, the Strategy has evolved over the last four years to include activities not anticipated at the outset. Interviewees were asked what the impact of the shifts has been. A few interviewees believe that the shifting nature of the initiative has been positive as it has forced partners to examine issues as they arise resulting in the further advancement of some outcomes.

A positive result in the legislation/policy area was seen by interviewees to be the fact that mandatory reporting is on the FPT Ministers of Justice meeting agenda and at the top of the FPT Working Group on Cyber-Crime agenda in which PS plays a key role. The fact that mandatory reporting is at the top of the agenda is believed to be due, in part, to the fact that the Strategy partners (PS and RCMP) have had to examine legislative issues in order to advance their efforts. However, a few mentioned negative unintended impacts such as the fact that the NCECC did not anticipate that they would need to spend so much time on legislative issues such as PIPEDA and Age of Consent legislation. While this has advanced the understanding of the legislative agenda, other work at the NCECC has suffered such as development of best practices and P2P investigative tools.

Challenges presented by the evolving nature of the Strategy include the feeling that managing workload and maintaining the appropriate capacity has been difficult. At the field level, being able to manage the volume of incoming files has been a challenge.

Conclusions – Evolution of the Strategy

13. There have been no major negative impacts due to the evolution of the Strategy. As the Strategy has evolved, partners have worked well together to address changing needs as they arise. The exception to this is that work on legislative issues has taken a good deal of time away from the day-to-day work of the NCECC meaning that other work has suffered as a result.

[94] References evaluation question 12: How has the evolving nature of the Strategy (additional funding, additional activities undertaken, etc.) impacted the success of the Initiative?

3.3 Cost-effectiveness and Alternatives

In the issue area of cost-effectiveness and alternatives, the evaluation explored whether Canadians are receiving value for the tax dollars, whether resources have been optimized to improved efficiency, and whether the Strategy is the appropriate response to the identified need.

Value for Money[95]

Many interviewees expressed the belief that the Strategy has provided value-for-money to Canadians. Some interviewees provided examples of how the Strategy has allowed Canada to move forward during the last four years. They cited the following examples: less duplication of efforts in dealing with international partners because of the focal point provided by the NCECC; the ability to keep up on the issue of child exploitation within the international community and achieve a profile in the G-8; the safeguarding of children and the apprehension of offenders; and the ability to address international files.

The evaluation also explored whether results achieved through expenditures on *CyberWise.ca* have been maintained during the transition to *Cybertip.ca*. Document review indicates the *Cybertip.ca*, in partnership with PS, prepared a plan for incorporating elements of the *CyberWise.ca* material. PS also discussed with *Cybertip.ca* officials and later organized an introductory meeting with representatives of *Internet 101* to discuss the transfer of the content of the *CyberWise.ca* Website. The educational material on the *CyberWise.ca* Website had received praise in the formative evaluation report and PS deployed efforts to ensure that the content was not lost. A review of the website indicates that most of these elements have been incorporated with the exception of the "Respect Yourself" section of the website geared towards adolescents which does not appear to have been implemented at the date of this report. The content of the *CyberWise.ca* Website can now be found on the *Cybertip.ca* and *Internet 101* Websites. As a final note, a few interviewees mentioned negative impacts of shifting resources out of IC in that the outreach function has suffered in terms of the provision of presentations in schools.

Leveraging of Resources

Many interviewees mentioned the donations of time and money by the technology industry to supplement the Strategy and leverage resources. Examples included donations of legal, marketing and IT personnel by ISPs to the work of CCAICE and funding assistance from ISPs to *Cybertip.ca*. In addition, Bell hosted the Delta Sessions which is valued at about $25,000 and Bluebear assisted in sponsoring events at the VGT conference in Vancouver in February 2008. Microsoft was also mentioned as creating and donating CETS and related technical assistance to law enforcement.

Some interviewees focused on the leveraging of public funds that have been provided to the educational efforts of *CyberWise.ca* and *Cybertip.ca*. Quantitative analysis shows that for 2007-08, *Cybertip.ca* received 41 cents in private sector funding for every dollar of government

[95] References evaluation question 13: Are Canadians getting value for their tax dollars? (ERC 5)

funding for a total of $725,000 in private sector funding. The ratio of funds leveraged for other years could not be determined based on the information provided.

A few interviewees mentioned delivery partners that provided investments in-kind to deliver educational and training material. These included: Internet 101, Vous NET pas seul, Infoburg, Computer for Schools, and the Community Access Program on behalf of Industry Canada; and Service Canada outlets; Safecanada.ca, and the educational system in various provinces on behalf of *Cybertip.ca*.

Efficiencies[96]

Efficient Use of Resources

An analysis of expenditures against budgets from 2004-05 to 2007-08 indicates that PS and *Cybertip.ca* are within acceptable limits. The exception to this is PS having a 10% surplus in 2007-08 due to the fact that PS only got the approval for the additional $6 million TB submission in December 2007. PS was unable to spend all the contribution and the salary money. Efforts were made to allocate money to a few projects, but this could not be accomplished due to delays in the approval process.

The RCMP has consistently under spent its budget since 2004-05 by approximately 40%. Approximately 20% of this amount can be accounted for by the fact that the image database is delayed and funding is re-profiled each year to account for the delay.

Investigative Efficiencies

Many field level interviewees indicated that the NCECC has saved time and money by putting investigative packages together. Information provided by the NCECC shows turnaround times for the NCECC to assemble various types of investigative packages and forward them to the appropriate jurisdiction; the NCECC is now meeting the turnaround times whereas at the outset a six-month backlog existed.

Many field level interviewees stated that the *Cybertip.ca* triage function has taken the burden off police and saved time by filtering out irrelevant complaints. They noted that *Cybertip.ca* has also decreased duplication of efforts among law enforcement in provinces and municipalities. Documents also stated that "by serving as the front door to the public, *Cybertip.ca* eliminates the burden that would otherwise be placed on law enforcement agencies in triaging complaints and information requests"[97]. Quantitative analysis supports this finding indicating that cost savings are realized for every complaint that is triaged by *Cybertip.ca*, freeing up local police to concentrate on investigations. This translates to an amount of between $600,000 and

[96] References evaluation question 14: To what extent have resources been optimised to improve efficiency? If the Strategy continues, how could its efficiency be improved? (ERC 6)
[97] Source: Cybertip ! ca. Taking Stock a Year Later. Annex A., p. 26

$1,800,000[98] in cost savings over the last four years since the inception of the Strategy. These savings have been realized by local provincial and municipal law enforcement.

Efficiencies through Targeted Research

There was no clear trend in comments from interviewees related to optimization of educational planning through the use of targeted research. *Cybertip.ca* uses techniques such as teachers' fora in combination with trends from the tip line to design educational products. In addition, *Cybertip.ca* tracks direct correlations between educational activities and impacts of the activities in order to understand effectiveness. It was also noted that some educational initiatives have been quickly abandoned by *Cybertip.ca* after success was not observed (e.g. newspaper advertisements were found to be ineffective).

Some field level interviewees indicated that having centralized, credible answers from NCECC research saves investigators time because the officers do not have to spend time looking for answers themselves. They indicated that the research allows investigators to reorient their investigations by having information on court decisions and case files.

Cost efficiencies due to research activities could not be quantified based on the information provided.

Conclusions – Cost Effectiveness

14. From the information provided, it has been demonstrated that the Strategy has provided value for money to some extent. For example, monetary donations and donations in-kind have been added to Strategy resources. In 2007-08, for every dollar spent on *Cybertip.ca*, 41 cents in private sector donations was realized resulting in $725,000 in private sector funding. Interviewees generally believe that value has been provided, and PS and *Cybertip.ca* have maintained the value that was provided by IC through the proactive and efficient transfer of this file and the associated materials. Without further financial and performance information and comparable benchmarks, it cannot be conclusively stated that the Strategy overall has provided value for money.

15. The Strategy has realized efficiencies. Centralized triaging by *Cybertip.ca* and preparation of investigative packages by the NCECC has made work more efficient for field resources. In quantifiable terms, the work of *Cybertip.ca* is estimated to have saved provinces and municipalities at least somewhere between $600,000 and $1,800,000[99] over the last four years. The NCECC is now meeting its turnaround times. Efficiencies due to targeted research

[98] The range is based on estimates of the average amount of time it takes to triage complaints which from interview information appears to be between one and three hours per complaint. The volume of complaints for the past three years has been 23,000 according to *Cybertip.ca* information.

[99] This calculation is based on the estimated time that *Cybertip.ca* has saved law enforcement in triaging 23,000 complaints over the past three years. The range is based on estimates of the average amount of time it would have taken for law enforcement to triage the complaints which was estimated to be between one and three hours per complaint by field level interviewees. If *Cybertip.ca* is taking less time on average per complaint, more savings would be realized. *Cybertip.ca* indicates that it could take as few as 15 minutes per complaint.

could not be quantified but interview evidence suggests that this has been the case.

16. Spending of resources against budgets by Strategy partners is generally within acceptable limits with the exception of the RCMP, which has under spent its budget since 2004-05 by approximately 40%. Approximately 20% of this amount can be accounted for by the fact that the image database is delayed and funding is re-profiled each year to account for the delay. Another factor that may have contributed to under spending is the challenge of recruitment and retention across the RCMP and law enforcement, in general, and in the child exploitation area, in particular, because it is a psychologically demanding field of law enforcement specialization.

Alternatives[100]

The evaluation sought to compare the Strategy to that of other similar programs in order to determine if it is the most appropriate response to the identified need. The evaluation reviewed four other initiatives:

1. United Kingdom: Child Exploitation Online Protection Centre (CEOP)
2. United States: Project Safe Childhood and other participants
3. Ontario Provincial Strategy
4. Australian Federal Police Online Child Sex Exploitation Team (OCSET)

It should be noted that these centres work in different legal systems and under different roles and mandates. In addition, although the Provincial Strategy may demonstrate a best practice, not all components translate to the national level. Having stated this, these initiatives have very similar objectives in that they exist to combat IBCSE.

Inquiries by the NCECC with VGT partners indicated that delivery costs related to investigation and awareness activities could be undertaken; however, partners would require additional time and would require specific guidance and information in terms of what information was required. Thus, the comparisons that follow are based on interviews and document review. To the extent possible, for each organization, four areas were examined: program design; funding model; results achieved; and advantages/disadvantages.

1. United Kingdom: Child Exploitation Online and Protection Centre

General Description/ Program Design

CEOP was established in April 2006 in response to growing concern about online child abuse. The aim of the organization is "to play a decisive part, with the Department for Children, Schools and Families, police forces, offender managers, children's services and other stakeholders in protecting children, young people, families and society from sex offenders; in particular those who use the Internet and other new technologies in the sexual exploitation of children."[101] Organisationally, CEOP is divided into three major faculties as follows: Intelligence, Operations, and Harm Reduction.

[100] References evaluation question 15: Is the Strategy the most appropriate response to the identified need?
[101] Child Exploitation and Online Protection Centre Business Plan 2007-08, p. 5

CEOP's activities include intelligence gathering and dissemination, offender management, operational support to law enforcement, education and training, and harm reduction strategies. "CEOP is an affiliate of the Serious Organised Crime Agency. This means that it is ultimately accountable to the Serious Organised Crime Agency Board, but enjoys full operational independence. From inception, the CEOP model was based on partnership."[102] Disciplines included in the CEOP team are as follows: law enforcement, forensics, banking authorities, Internet service providers, charities that have credible understanding of victims, victim support, child welfare specialists; industry representatives like VISA, and Microsoft who understand the next generation of technology so that law enforcement can leapfrog criminals; and Ford that supplies educational vehicles.

CEOP also has a dedicated training unit and national education strategy. Their trained trainers include: teachers, guidance counselors, social workers, law enforcement school liaison officers. CEOP has built a 60-member youth panel between ages of 11 and 17 who advise on the content and construct of their materials.

Funding Model

Funding for CEOP was built on a platform of funds from various sources. This is critically important as CEOP's funding is red circled meaning that, although partners contribute to CEOP, their budgets remain available only for the intended purpose. In 2007-08, funding for CEOP was $17.4M CDN. There was a total of 69 staff, 13 of whom were on secondment. It is noteworthy that CEOP also generates income mostly through CEOP's training program and direct partnership support. CEOP accesses significant levels of financial support/ benefit in kind, and in 2007-08 this represented 27% of CEOP's overall budget. CEOP's affiliation with Serious and Organized Crime Agency means that it also received subsidy to fund corporate services activities. CEOP estimates that it will need to incrementally develop its budget to 21M pounds per year if they are to optimise their success.

Results Achieved

The following items are among the results that CEOP highlights in its Annual Review 2007-08.

Law Enforcement

- 131 children have been safeguarded from sexual abuse either directly or indirectly as the result of CEOP activity.
- 297 arrests have been made as a result of CEOP activity.
- 25 of the UK's highest risk child sex offenders have been located as a direct result of CEOP activity.
- 6 organised paedophile rings have been dismantled or disrupted as a result of CEOP activity.

Education

- Over 2,600 law enforcement and child protection professionals have attended specialist CEOP training courses.

[102] Child Exploitation and Online Protection Centre Business Plan 2007-08, p. 5

- 5,812 intelligence reports have been received by the CEOP – a culmination of public reports through the 'Report Abuse' mechanism, via the online industry and law enforcement partners in the UK and overseas.
- Over 11,000 teachers and trainers are now delivering the Thinkuknow education programme in schools across England, Scotland, Wales and Northern Ireland.
- Since its launch, the Thinkuknow education programme has reached 1.7 million children and young people between the ages of 8 and 16 years across all parts of the UK.

Advantages and Disadvantages

CEOP was cited most frequently by interviewees as a model to be followed that may have similarities to the Canadian strategy in that it offers the same types of programs. Interviewees stated that CEOP has a true, co-located multi-disciplinary environment. "Partnership has been fundamental to CEOP's design. This model recognises that the problem of child abuse is a complex one, best addressed not only by the various arms of government, but also by industry, charities and others interested in child protection. CEOP benefits hugely through its network of partners in terms of secondments, other direct support, advice and influence".[103] In order to properly manage its partnerships, CEOP has developed a Partnership Policy and a Partnership Committee who advise on the adoption of new partnerships, taking into account ethical and other factors.

Interviewees stated the benefits of the CEOP model are as follows: because CEOP has created a victim support group made up of adults, many of whom were child victims, they have a better understanding of the issues; CEOP is more streamlined and intelligence-led; CEOP concentrates it efforts on intelligence and are very good at prevention efforts; there is a sense that they have the right people in the right jobs who are very knowledgeable.

2. Ontario Provincial Strategy

General Description/ Program Design

The Ontario Provincial Strategy has brought together a team of municipal, regional and Ontario Provincial Police officers, Crown prosecutors and victim service providers. The partnership includes 18 municipal agencies throughout Ontario.

The strategy includes:

- A dedicated child-victim tip line and referral service available 24-7, managed in partnership with the Ontario Association of Crime Stoppers: 1-800-222-TIPS
- Specialized teams of police officers to conduct online child-luring investigations and attempt to identify victims
- Dedicated support for child victims and families to offer emotional support, referral to appropriate community services and practical assistance
- Training and support for dedicated Crown prosecutors
- Increased liaison work with law enforcement agencies and others.

[103] Child Exploitation and Online Protection Centre Annual Report 2007-08. p 8

Funding Model

The Ontario Provincial Strategy's receives $2.5M in funding from the Ontario Provincial Government every year for two years beginning in 2006-07. The resource level is 60 FTEs.[104]

Results Achieved

Interviewees indicate that the Ontario Provincial Strategy handles 400-500 cases per year. Others state that for 2006-2007, 1069 cases were handled and from April 1 to December 31, 2007, 1515 cases were handled by the provincial strategy. Information regarding numbers of arrests or children safeguarded could not be obtained within the timeframe of the evaluation.

Advantages! Disadvantages

Interviewees indicated that the partnership approach implemented by the Ontario Provincial Strategy has shut down silos and implemented multi-disciplinary teams that include law enforcement, Crown prosecutors, and victim services. One of the main advantages was seen to be that the Ontario Strategy has alleviated challenges with information sharing and variations in investigations and prosecutions.

3. United States: Project Safe Childhood

General Description! Program Design

The United States has no National Strategy *per se*, but is currently looking at a national approach through Project Safe Childhood (U.S. Department of Justice). "Project Safe Childhood (PSC) is a Department of Justice initiative launched in 2006 that aims to combat the proliferation of technology-facilitated sexual exploitation crimes against children. Through a network of federal, state, and local law enforcement agencies and advocacy organizations, PSC coordinates efforts to protect our children by investigating and prosecuting online sexual predators. PSC is implemented through a partnership of U.S. Attorneys; Internet Crimes Against Children (ICAC) Task Forces; federal partners, including the FBI, U.S. Postal Inspection Service, Immigration and Customs Enforcement and the U.S. Marshals Service; advocacy organizations such as the National Center for Missing and Exploited Children (NCMEC); and state and local law enforcement officials in each U.S. Attorney's district."[105]

Internet Crimes against Children (ICAC) Task Force, United States

ICAC regional task forces developed from state and local law-enforcement network through grants from US DOJ. There are 45 task forces. DHS/ICE strongly supports the efforts of the ICAC task forces as demonstrated by ICE special agents being active members of ICAC's throughout the United States. Investigators receive specialized training and technological

[104] The Provincial Strategy has been extended for another year. However, the funding received wasn't sufficient to cover the strategy in the same format. There are three fewer members.
[105] Source : Project Safe Childhood website http://www.projectsafechildhood.gov/attyefforts.htm

resources to serve as sources of prevention, education, investigative experience, and technical assistance for parents, teachers, law enforcement agencies, and other professionals.

Funding Model

PSC is implemented through a partnership approach. Federal grants are provided to ICAC Task Forces. In 2007, the Department of Justice awarded $4 million USD in PSC grants. No other funding information was available.

Results Achieved

The following items are among the results that PSC has achieved as reported on its website[106].

Law Enforcement:

- 2,118 indictments were filed in fiscal year 2007 against 2,218 defendants. This represents a 27.8 percent increase over fiscal year 2006.
- In fiscal year 2007, 332 child exploitation cases resulted in the forfeiture of 458 assets. The value of the forfeited assets is $5,237,490. This represents a 492.7 percent increase over fiscal year 2006.
- In fiscal year 2007, ICAC Task Forces made 2,354 arrests for online child exploitation crimes across the nation, an increase of nearly 15 percent over the number of arrests in fiscal year 2006.
- At the end of calendar year 2005, 590 child pornography victims had been identified through the efforts of NCMEC's CVIP. As of April 27, 2008 that number had grown to 1,342 -- an increase of more than 127 percent of the total in approximately two and a half years.

Education and Awareness:

- The Department sponsors a number of resources to help educate parents about how to keep their kids safe on the Internet, including NetSmartz.org, isafe.org and WebWiseKids.org.
- Since launching in 2004, the Online Sexual Exploitation campaign has garnered over $188 million in donated media support, and the toll-free number, 1-800-THE-LOST, has received more than 225,000 calls.

Advantages and Disadvantages

A few interviewees mentioned that the U.S. model is less coordinated than other alternatives. As a result, these organizations may be involved in the issue separately, and possible competition among organizations for the same funds was cited as a disadvantage.

4. Australia: Australian Federal Police Online Child Sex Exploitation Team

General Description/ Program Design

[106] Source : Project Safe Childhood website http://www.projectsafechildhood.gov/attyefforts.htm

"The Australian Federal Police Online Child Sex Exploitation Team (OCSET) performs an investigative and coordination role within Australia for multijurisdictional and international online child sex exploitation matters. These cases include those from Australian State and Territory Police, government and non-government organizations (including Internet Service Providers and Internet Content Hosts), the Australian High Tech Crime NCECC, the Virtual Global Taskforce, international law enforcement agencies, Interpol and members of the public.

The Australian Federal Police investigate online child exploitation which occurs using the telecommunications service, such as Internet or mobile phones. The types of offences include accessing, sending or uploading child pornography or child abuse material. Grooming and procuring of children over the Internet is also investigated by the Australian Federal Police.

Investigations may also focus on Internet sites carrying this material and operated from an ISP in Australia. Any sites not within Australia are referred to overseas law enforcement agencies.[107]

The Australian Communications and Media Authority delivers educational material through its Cybersmart kids' website at http://www.cybersmartkids.com.au/about-us.htm. It also manages Australia's reporting site and investigates all valid complaints.

Funding Model

In May 2007, the Federal Government renewed its commitment to combating child sex tourism and human trafficking offences with funding extended to the Australian Federal Police over a further four years. Actual funding levels were not available.

Advantages/ Disadvantages

The Australian model was mentioned less frequently by interviewees who believed that the focus of the Australian initiative was travelling sex offenders.

Conclusions – Alternatives

17. From a review of other similar initiatives, it appears that the Strategy is a very appropriate response to the identified need. In terms of a general approach to combating IBCSE, work in other countries involves a law enforcement component and an education and awareness component, similar to the Strategy. Also, a partnership approach appears to be good practice.

18. Of the initiatives studied, CEOP provides a model that may warrant further study because of the apparent benefits of an approach that is further integrated than the Strategy. Following this approach may mean integrating additional partners such as: charities that have credible understanding of victims, victim support, guidance counselors, social workers, and a youth panel. Benefits to this further integrated partnership model are seen to be the ability to use secondments to supplement resources, to receive direct support, and to receive advice and influence from varying perspectives in order to solve the complex problem of IBCSE.

[107] Source: http://www.afp.gov.au/national/e-crime/online_child_sex_exploitation.html

3.4 Design and Delivery

Implementation of the Recommendations of the Formative Evaluation[108]

A key component of the Formative Evaluation was recommendations provided under evaluation issue areas that were linked to partner responsibilities. Seven recommendations were listed in the formative evaluation, three in the area of Design and Delivery and four in the area of success[109].

The majority of recommendations from the Formative Evaluation have been completed. All actionable recommendations from the Formative Evaluation have been addressed to some extent. It is noted that two recommendations were not accepted due to the limited influence of the RCMP on provincial staffing levels.

Overall, based on the management response to the recommendations, as well as the research of the Summative Evaluation, the following areas outline the partners' remaining items from the Formative Evaluation recommendations that will help ensure continuous improvement of the Strategy:

Recommendation 2: The governance of the Initiative should be strengthened. A stronger central forum is required to address shared strategic and operational issues that cannot be solved by individual partners. Clear terms of reference should be developed for each committee or sub-committee, including the National Steering Committee and the IWG; and the membership of these groups should be carefully considered in terms of what participation, at what level of each organization, will make them function well. (PS in consultation with all partners)

This recommendation is considered to be in progress. Although preliminary meetings have been held among senior managers (Director General/Superintendent level) and this will be the group who will provide direction to the Strategy, the National Steering Committee needs to remain active in providing guidance and direction to partners involved in the delivery components of the Strategy. Terms of reference have not been developed for the National Steering Committee or the IWG.

Recommendation 3: Industry Canada and the RCMP should seek a mechanism to ensure better financial management so that funds do not lapse in future years. (Industry Canada, RCMP)

This recommendation has not been implemented successfully. The RCMP continues to lapse funds at a level that is outside acceptable limits.

Implementation of Strategy Activities and Outputs

As a final note, in terms of the implementation of activities associated with the Strategy, all planned activities and outputs of the original Strategy design have been implemented with the exception of the image database by the RCMP.

[108] References evaluation question 17: What progress has been made toward implementation of the recommendations of the formative evaluation?

[109] Management Action Plan (MAP) – Law Enforcement and Border Strategies (PLIEB) document entitled Management Response to the Recommendations Proposed on the Formal Evaluation.

Conclusions – Design and Delivery

19. The Strategy is considered to be fully implemented, with the exception of the implementation of the image database. In addition, the majority of recommendations from the Formative Evaluation have been implemented; two of the recommendations remain to be completed.

4. Recommendations

The paragraphs that follow summarize the recommendations put forward as a result of the conclusions drawn in the previous sections.

1. PS should continue its coordination activities and expand its leadership efforts. To this end, PS should further engage the IWG in coordinating activities related to communications (public awareness) and research. The strategic role of PS should be continued and strongly supported in order for the Strategy to get "ahead of the curve" on the issue of IBCSE. Thus, PS should continue to work with national and international partners to improve collaboration, share best practices and exchange ideas on child sexual exploitation on the Internet. PS should continue to advance dialogue with the provinces and territories on issues of common interest. PS should also continue to demonstrate leadership in advancing strategic planning by coordinating research to keep apprised of developments in technology, trends and emerging issues and sharing the results with interdepartmental working groups, including Strategy partners. (PS)

2. Work on legislative issues has taken a good deal of time away from the day-to-day work of the NCECC meaning that other work has suffered. Given the likely continued participation of the NCECC on legislative issues and on high-profile international working groups, the RCMP should consider how they can manage resources in order to both meet these very important "upper-level" priorities and maintain leadership at the NCECC when resources may be drawn away. (RCMP)

3. There is remaining work to be done in developing awareness of other groups, outside the Strategy, involved in public education efforts. To this end, PS should conduct an environmental scan in conjunction with *Cybertip.ca* and the NCECC to determine what other groups exist and what efforts are being undertaken by these groups in the area of education and awareness in order to realize synergies and avoid duplicating activities. (PS)

4. Education efforts and awareness building activities among law enforcement, judicial partners and ISPs have proven effective in increasing knowledge among stakeholders and should continue. Continued law enforcement training needs include: training on trends in sex offender methods, on Internet usage among youth, and on investigative techniques. Training needs among judicial partners include education on the nature of the crime, and, for ISPs, increasing awareness on legal issues. (all partners)

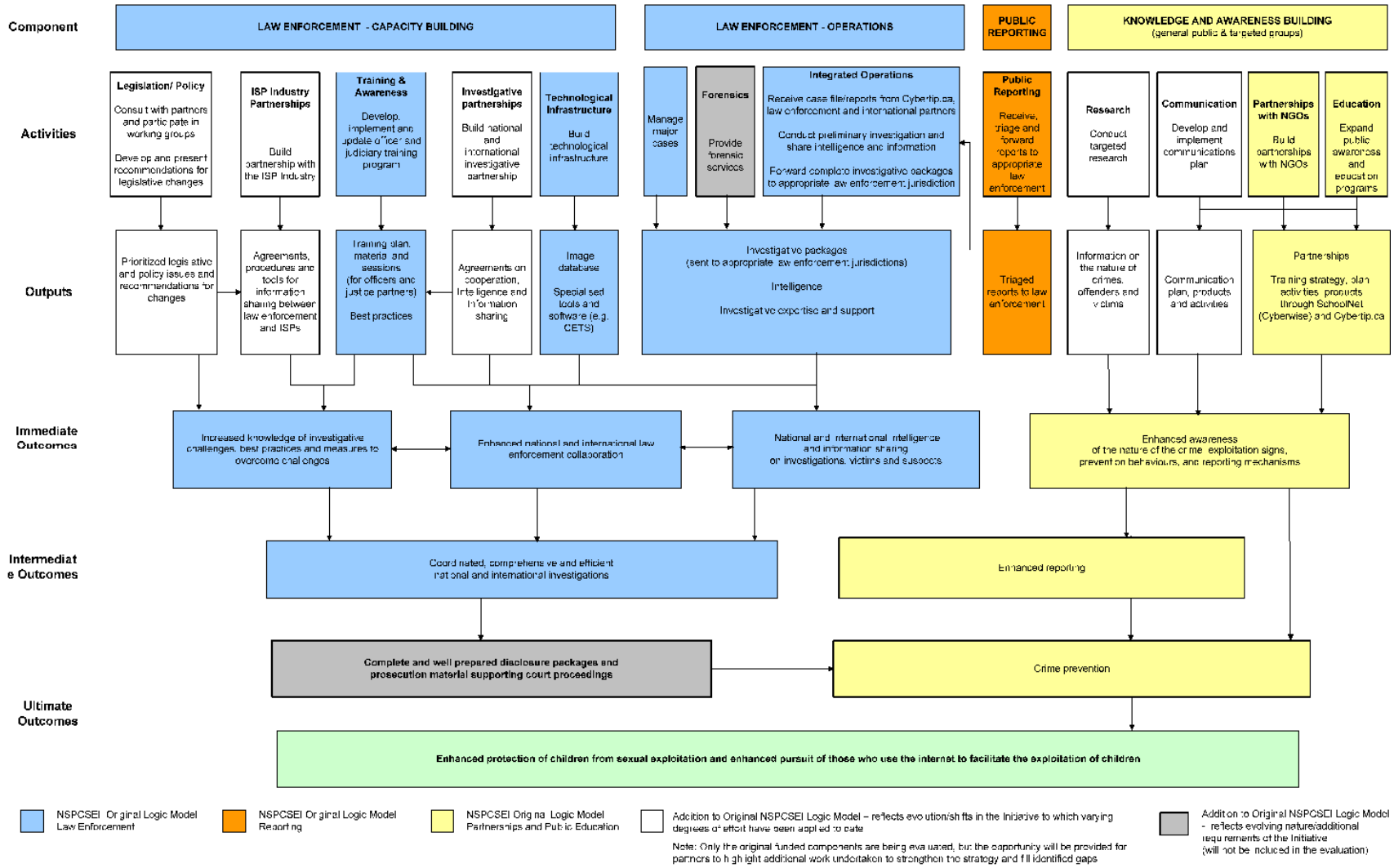
5. The Child Exploitation and Online Protection (CEOP) Centre model should be further studied to assess the benefits of incorporating additional partners, to understand CEOP's strategic approach to "getting ahead of the issue" of IBCSE, and to assess whether parts of this approach can be applicable in the Canadian context. Recognizing that CEOP is part of

United Kingdom law enforcement and as such, can apply the full range of policing powers in tackling the sexual abuse of children, but that it also has a unique structure, it is recommended that the Canadian Strategy explore possibilities of benchmarking performance information against CEOP. (PS/NCECC)

6. Efforts should be made to allocate the 20% of funding that is consistently under spent by the RCMP, to forensics support for investigators. It is recognized that retaining forensic support is currently problematic for all law enforcement with heavy case loads; however, possibilities include providing a centralized forensics unit, seconding officers from other law enforcement agencies or outsourcing this function to another appropriate unit within the RCMP. It is important to note that control of the funding should remain with the NCECC to ensure that the funding is spent on Strategy activities. (RCMP)

7. The NCECC should be more proactive in collecting and reporting performance information as laid out in the RMAF/RBAF (or revised version thereof) including the number of arrests, the type and number of charges laid and sentences pronounced. More work needs to be done with the field level to enable the NCECC to track this information. (RCMP)

Appendix A - Strategy Logic Model



Appendix B - List of Documents and Quantitative Data Reviewed

Documents	
1.	[*]
2.	[*]
3.	RMAF-RBAF
4.	RCMP DPR 2006-2007
5.	PS DPR
6.	Speech from the Throne
7.	Trend analysis, Needs Assessment, Environmental scan, Research studies
8.	EKOS Survey
9.	Public Safety Act
10.	RCMP Legislation
11.	Formative Evaluation
12.	Management Action Plan
13.	Agenda items and minutes from working groups and committees – Minutes from the National Steering Committee Meeting on Internet Based Sexual Exploitation of Children. April 15, 2005. RCMP Headquarters, Ottawa Ontario
14.	Terms of reference for working groups and committees
15.	Records of decision and minutes of meetings
16.	*Cybertip.ca* and *Cyberwise.ca* contribution agreement terms and conditions and audit reports
17.	Memorandum for the Minister – Revised Contribution Agreement with the Canadian Centre for Child Protection Inc. in the amount of $1 Million for Fiscal Years 2007/08 and 2008/09
18.	Combating Sexual Exploitation of Children at the G8 Roma-Lyon (issue analysis paper)
19.	BBC News – EU extends net safety programme
20.	Briefing Notes (Begins National Child Exploitation Coordination Centre)
21.	Letter to Lianna McDonald, - Agreement between PSEPC and Child Find Manitoba Inc.
22.	Letter to Lianna McDonald – Amendment #1 to the Agreement between PSEPC and Child Find Manitoba
23.	Letter to Liana McDonald, Jan 22, 2008, re. Amendment #3 to the contribution agreement

Documents	
24.	Participant Feedback Summary (NCECC Annual Conferences 2004-2007) • 2004 National Child Exploitation Workshop, Winnipeg • 2005 National Child Exploitation Workshop, Calgary • 2006 Law Enforcement Workshop, Fredericton • 2007 Law Enforcement Workshop, NCECC and OPP, Ottawa • 2008 Internet Safety Symposium – NCECC and H Division – Operation Horizon, Dartmouth
25.	CANICE End of Course Critique (March 2006, March 2007, November 2007)
2	Public Opinion Survey on Public Perceptions of Organized Crime in Canada
2	Organized Crime in Canada 2007. Public Opinion Survey – Preliminary Findings
2	Public Safety and Emergency Preparedness Canada. Report on the Audit of the Canadian Centre for Child Protection Inc. April 25, 2007
2	*Cybertip.ca* Taking Stock a Year Later - Annex A
3	Child Exploitation and Online Protection Centre Business Plan 2007-08; Annual Report 2007-08
3	*Cybertip.ca* promotional material to law enforcement - "*Cybertip.ca* is a resource to policing"
3	Project Cleanfeed Canada Frequently Asked Questions
3	Canadian Coalition Against Internet Child Exploitation (CCAICE) Mid-year Review, November 2006
3	Canadian Coalition Against Internet Child Exploitation (CCAICE) Action Plan 2008
3	Internet Based Sexual Exploitation of Children and Youth Environmental Scan
3	Botnets Research Brief
3	Wireless Networks in Ottawa: Are They Secure?
3	Virtual Worlds, Virtual Behaviours: The Legal Impacts of Second Life
3	Child Pornography Offences in Canada: Recent Trends
4	Public Safety Canada Letters/Correspondence
4	Young Canadians in a Wired World, Phase II (Media Awareness Network)
4	Britain seeks pedophiles Facebook ban (CTV.ca, published April 4, 2008)
4	Boyish, cunning and cruel: Online predator shut down (The Ottawa Citizen, January 25, 2008)
4	Court ruling clears a path for wiretap law (The Ottawa Citizen, April 7, 2008)
4	Initiative 'gets ahead' of cybercriminals (National Post, March 21, 2008)

Documents	
4	NPS Sub-Activity – The National Child Exploitation Coordination Centre Business Plan 2008/2009
4	NCECC Contributions to the Achievement of the G8 Objectives, June 2007
4	Public Safety Communications Plan: National Strategy of the Protection of Children from Sexual Exploitation on the Internet, 2008-2009.
4	Public Awareness and Education Session, February 2008, Vancouver BC.
5	Pollara, May 2007 – Public Awareness Deck
5	KIK Fold-Out
5	Kids in the Know – Student Advisory Groups Presentation
5	Billy Brings His Buddies, 2007-2008 Evaluation
5	Safer Internet Day Evaluation 2008.
5	Working Together to Educate Canadians, 2007
5	NCECC Communication Plan, Draft 4.0, 2008-09
Quantitative Data	
5	Summary report on ISPs turn around time
5	Summary report on number of cases/ investigations impossible to complete due to missing information to identify suspect
5	Summary report on trend in number of children identified and located as result of the NSPCSEI
6	Records Management System – Occurrence Statistics.
6	NCECC Internal Statistical Reporting
6	*Cybertip.ca* Reports Statistics
Websites	
6	Australian Federal Police Website (www.afp.gov.au/home.html)
6	VGT Website (www.virtualglobaltaskforce.com/vgt_members.html)
6	US Immigration and Customs Enforcement - Cyber Crimes Centre Website (www.ice.gov/partners/investigations/services/cyberbranch.htm)
6	State Police Italy - Polizia di Stato Website (www.poliziadistato.it/pds/lingua/english/operativi.html)
6	Interpol Website (www.interpol.int/public/children)
68.	http://www.cybertip.ca/app/en/stats, *Cybertip.ca* Summary Statistics

Appendix C – Interview Guides

Interview Guide 1
National Child Exploitation Coordination NCECC Staff
Integrated Child Exploitation Units
Other Police Services

Introduction

Public Safety Canada (PS), in conjunction with the funded partners of the National Strategy for the Protection of Children from Sexual Exploitation on the Internet (Strategy), has asked Government Consulting Services (GCS) to conduct a summative evaluation for the Strategy initiative.

The Strategy initiative, beginning in 2004-2005, was funded a total of $42 million over five years to implement the National Strategy in three core areas: Law Enforcement Capacity; Public Education and Reporting; and Partnerships with Industry and Non-government Organizations (NGOs). The table below lists the Strategy partners and summarizes the funding that was provided for each partner.

Strategy Partner	Funding Level over Five Years
Royal Canadian Mounted Police (RCMP)	$34.34 M
Industry Canada (IC)	$3.00 M
Public Safety (PS) and *Cybertip.ca*	$4.70 M
TOTAL	**$42.04 M**

Under the Strategy, the general expectations and desired achievements of each partner were as follows. Funding for the RCMP was directed towards the expansion of the current capacity of the National Child Exploitation Coordination NCECC (NCECC). IC received funding to expand SchoolNet and forge partnerships with industry and NGOs. PS was to enter into a contribution agreement with Child Find Manitoba for the purposes of operating and expanding the *Cybertip.ca* program on a national basis. In addition to the contribution agreement funding, as the lead department for the Strategy, PS received funding to fulfill its coordination and oversight role and responsibilities.

The above-noted activities have been underway for approximately four years. As such, the summative evaluation will review the past four years in order to assess the continuing relevance of the initiative; impacts and successes, value to taxpayers, cost efficiencies and alternatives to the initiative design. Information from the summative evaluation will be used to support the renewal of the Strategy in 2010-11. Additional activities that have been undertaken by partners and/or new activities that have been identified as necessary during the last four years will also be taken into consideration during the evaluation.

As part of the summative evaluation, GCS is conducting interviews with key stakeholders involved in the Strategy. The questions that follow will help structure our conversation with you and we hope that you will find it useful in preparing for the interview. We anticipate that interviews will take about an hour and a half. Please note that not all questions will be applicable to all participants. In addition, responses you provide will not be attributed to you, but will only be released in aggregate form.

Background

1. Please briefly describe your role and involvement with the Strategy.

Relevance

2. How has the nature, size or evolution of the problem of Internet-based child sexual exploitation changed since the inception of the Strategy in 2004? Is there a continuing need for a national strategy that combats Internet-based child sexual exploitation? Why or why not?

3. Are there currently any aspects of the crime related to Internet-based child sexual exploitation that are not being addressed under the current strategy? In your estimation, what is the level of effort that would be necessary to fill the gaps?

4. Since 2004, have sufficient **investigative** resources been available for the fight against Internet-based child sexual exploitation? If not, please prioritize the following and provide an explanation for your ranking (with 1 being the highest priority):

__ Support from NCECC
__ Staffing (appropriate people with appropriate expertise)
__ Training (relevant/available training)
__ Tools and technology (CETS, images databases, equipment, hardware, software) __
Other (please specify): _____

5. Since 2004, the Strategy has involved three funded federal partners (PS, IC and RCMP) and a nongovernmental organization (*Cybertip.ca*). Does each of these partners currently play the appropriate role? If not, what needs to change? What activities or programs might be transferred to other federal departments, other levels of government or the private/voluntary sector? Are there any activities or programs that would benefit from being incorporated into Strategy? Please explain.

Design and Delivery

Is the Strategy governance structure effective?

- at the horizontal level (e.g. decision making, issue resolution, strategic planning, performance measurement, financial control)
- at the working level (e.g. planning, working groups, coordination of activities)

Why or why not? Do you have any suggestions for improvement?

Success

6. By obtaining your answers to the questions in the following table, we hope to determine what changes have occurred since 2004 in each of the listed Strategy activity areas. Please give some thought to the level of impact the following activities have had, and we will fill out this table during the interview.

Activities	**Since 2004, when Strategy was funded, how have the activities impacted:**			
	the working relationship among law enforcement		**the level of information sharing among law enforcement (investigations, victims and suspects)**	
	Level of impact: not applicable/ don't know detrimental not enhanced enhanced strongly enhanced	Please explain.	Level of impact: • not applicable/ don't know • detrimental • not enhanced • enhanced • strongly enhanced	Please explain.
Training and/or conferences				
Tools and technology (CETS and image databases)				

Partnerships and agreements for cooperation with national and international law enforcement and ISPs				
Investigative support from the NCECC				
Other factors				

Have there been any challenges in these areas that have limited success? E.g. missing tools, gaps in the partnerships that need to be filled, inability to provide support for programs in other countries or provinces, etc

7. Can you provide any examples where Strategy education and awareness activities delivered by *Cybertip.ca* or IC have contributed to increased knowledge in the general population or among target groups (parents, children, educators, health professionals)? Please explain.

8. a) Have Strategy activities (e.g. training, examination of legislative issues, ISP partnerships), increased **your knowledge** in the following areas?

Please rate your answers as follows: *not applicable, no change, improved, significantly improved*

- understanding of investigative and legal challenges
- law enforcement best practices
- measures to overcome challenges
- other areas of knowledge increase

b) Have the activities contributed to increased knowledge **in general** among law enforcement, justice partners, and ISP providers? Please explain.

Please rate your answers as follows: *not applicable, no change, improved, significantly improved*

Knowledge Area	**Law Enforcement**	**Justice Partners**	**ISP Providers**
Understanding of investigative and legal challenges			
Law enforcement best practices			
Measures to overcome investigative and legal challenges			
Other areas of knowledge increase			

c) Are there other areas of training or awareness that need to be addressed going forward?

9. One of the objectives of the Strategy is that investigations become more coordinated, comprehensive and efficient. Since 2004, when Strategy was funded, how have investigations changed? Has Strategy contributed to this change? Please explain.

10. Since 2004, when Strategy was funded, in what ways has the Strategy contributed to:
    - enhanced protection of children from sexual exploitation?
    - enhanced pursuit of those who use technology to facilitate the exploitation of children?

11. The Strategy has evolved over the last four years to include activities not anticipated at the outset. These are in the areas of:
    - Legislation/policy
    - ISP industry partnerships
    - Investigative partnerships
    - Research
    - Communications

Can you briefly explain a) why these changes have occurred; b) what the contribution has been and; c) if they continue to be necessary and why.

What is the impact of shifting resources into these areas? Are these areas sufficiently resourced?

12. How has the evolving nature of the initiative impacted its success? What are the specific challenges and opportunities presented by the evolution? Have the changes resulted in any unintended impacts (either positive or negative)?

Cost Effectiveness and Alternatives

13. Do you feel the Strategy program has provided value-for-money for Canadian citizens? If yes, how so?

14. In the area of law enforcement, what efficiencies have been gained as a result of targeted research, support from NCECC and the *Cybertip.ca* triage function? (e.g. save money/ time, resources put where they are most needed). What else has helped realize efficiencies? Has targeted research had other impacts?

15. Are you aware if private or non-governmental organizations have provided financial or in-kind investments to the Strategy? If yes, please describe.

16. Are you aware of any other programs that overlap or complement the NSPSCEI? Please explain.

17. Are you aware of initiatives similar to the Strategy that exist in other parts of Canada or other countries? How does the success of these initiatives compare to the success of Strategy? What lessons learned could help improve the Strategy going forward?

Other

18. Is there anything else you would like to add?

INTERVIEW GUIDE 2
PUBLIC SAFETY AND ROYAL CANADIAN MOUNTED POLICE MANAGEMENT AND OVERSIGHT CYBERCRIME WORKING GROUP OFFICIALS
Background

1. Please briefly describe your role and involvement with the Strategy.

Relevance

2. How has the nature, size or evolution of the problem of Internet-based child sexual exploitation changed since the inception of the Strategy in 2004? Is there a continuing need for a national strategy that addresses this issue? Why or why not?

3. Are there currently any aspects of the crime related to Internet-based child sexual exploitation that are not being addressed under the current strategy? In your estimation, what is the level of effort that would be necessary to fill the gaps?

4. Since 2004, the Strategy has involved three funded federal partners (PS, IC and RCMP) and a non-governmental organization (*Cybertip.ca*). Does each of these partners currently play the appropriate role? If not, what needs to change? What activities or programs might be transferred to other federal departments, other levels of government or the private/voluntary sector? Are there any activities or programs that would benefit from being incorporated into Strategy? Please explain.

5. Since 2004, have sufficient resources been available for the fight against Internet-based child sexual exploitation? If not, please prioritize the following and provide an explanation for your ranking (with 1 being the highest priority):

__ Staff (appropriate people with appropriate expertise) __ Training (relevant/available training)
__ Tools and technology (equipment, hardware, software) __ Other (please specify): _____

Design and Delivery

6. Is the Strategy governance structure effective?

- at the horizontal level (e.g. decision making, issue resolution, strategic planning, performance measurement, financial control)
- at the working level (e.g. planning, working groups, coordination of activities)

Why or why not? Do you have any suggestions for improvement? **Success**

7. By obtaining your answers to the questions in the following table, we hope to determine what changes have occurred since 2004 in each of the listed Strategy activity areas. Please give some thought to the level of impact the following activities have had, and we will fill out this table during the interview.

Activities	Since 2004, when Strategy was funded, how have the activities impacted:			
	the working relationship among law enforcement		the level of information sharing among law enforcement (investigations, victims and suspects)	
	Level of impact: • not applicable/ don't know • detrimental • not enhanced • enhanced • strongly enhanced	Please explain.	Level of impact: • not applicable/ don't know • detrimental • not enhanced • enhanced • strongly enhanced	Please explain.
Training and/or conferences				
Tools and technology (CETS and image database)				
Partnerships and agreements for cooperation with national and international law enforcement and ISPs				
Investigative support from the NCECC				
Other factors				

Have there been any challenges in these areas that have limited success? E.g. missing tools, gaps in the partnerships that need to be filled, inability to provide support for programs in other countries or provinces, etc

8. Have Strategy activities (e.g. training, examination of legislative issues, ISP partnerships) contributed to increased knowledge **in general** among law enforcement, justice partners, and ISP providers? Please explain.

Please rate your answers as follows: *not applicable, no change, improved, significantly improved*

Knowledge Area	Law Enforcement	Justice Partners	ISP Providers
Understanding of investigative and legal challenges			
Law enforcement best practices			
Measures to overcome investigative and legal challenges			
Other areas of knowledge increase			

c) Are there other areas of training or awareness that need to be addressed going forward?

9. One of the objectives of the Strategy is that investigations become more coordinated, comprehensive and efficient. Since 2004, when Strategy was funded, how have investigations changed? Has Strategy contributed to this change? Please explain.

10. Over the last four years, in what ways has the Strategy contributed to:
    - enhanced protection of children from sexual exploitation?
    - enhanced pursuit of those who use technology to facilitate the exploitation of children?

. The Strategy has evolved over the last four years to include activities not anticipated at the outset. These are in the areas of:

- Legislation/policy
- ISP industry partnerships
- Investigative partnerships
- Research
- Communications

Can you briefly explain a) why these changes have occurred; b) what the contribution has been and; c) if they continue to be necessary and why.

What is the impact of shifting resources into these areas? Are these areas sufficiently resourced?

12. How has the evolving nature of the initiative impacted its success? What are the specific challenges and opportunities presented by the evolution? Have the changes resulted in any unintended impacts (either positive or negative)?

Cost Effectiveness and Alternatives

13. Do you feel the Strategy program has provided value-for-money for Canadian citizens? If yes, how so?

14. In the area of law enforcement, what efficiencies have been gained as a result of targeted research and the *Cybertip.ca* triage function? (e.g. save money/ time, resources put where they are most needed). What else has helped realize efficiencies? Has targeted research had other impacts?

15. Are you aware of any other programs that overlap or complement the NSPSCEI? Please explain.

16. Are you aware of initiatives similar to the Strategy that exist in other parts of Canada or other countries? How does the success of these initiatives compare to the success of Strategy? What lessons learned could help improve the Strategy going forward?

Other

17. Is there anything else you would like to add?

INTERVIEW GUIDE 3

CYBERTIP.CA AND INDUSTRY CANADA

Background

1. Please briefly describe your role and involvement with the Strategy.

Relevance

2. How has the nature, size or evolution of the problem of Internet-based child sexual exploitation changed since the inception of the Strategy in 2004? Is there a continuing need for a national strategy that addresses this issue? Why or why not?

3. Are there currently any aspects of the crime related to Internet-based child sexual exploitation that are not being addressed under the current strategy? In your estimation, what is the level of effort that would be necessary to fill these gaps?

4. Since 2004, the Strategy has involved three funded federal partners (PS, IC and RCMP) and a non-governmental organization (*Cybertip.ca*). Does each of these partners currently play the appropriate role? If not, what needs to change? What activities or programs might be transferred to other federal departments, other levels of government or the private/voluntary sector? Are there any activities or programs that would benefit from being incorporated into Strategy? Please explain.

Design and Delivery

5. Is the Strategy governance structure effective?

- at the horizontal level (e.g. decision making, issue resolution, strategic planning, performance measurement, financial control)
- at the working level (e.g. planning, working groups, coordination of activities)

Why or why not? Do you have any suggestions for improvement?

Success

6. Please comment on the following items regarding the educational and/awareness material that you produce:
   - Description of the types of materials and types of activities
   - Target audience(s) for these materials
   - Geographic area of distribution
   - Known demand
   - Ability to meet the demand (if not able to meet demand, identification of the gaps or target audiences not being reached)
   - Programs that duplicate, supplement or complement your materials

7. Are you aware of any evidence or examples of usage of SchoolNet and/or *Cybertip.ca* materials by teachers within schools? Have any of these materials been integrated into the school curriculum?

8. Are there other groups that help in your delivery of educational material? How have these delivery partners helped you to achieve your goals regarding education and awareness?

9. Since 2004, when the NSPSCEI was implemented, please describe how Strategy education and awareness activities have increased knowledge (e.g. nature of the crime, exploitation signs, prevention behaviours, and reporting mechanisms) among the following groups:

   Please rate your answers as follows: *not applicable, no change, improved, significantly improved*

   - general population

- parents
- children
- educators
- health professionals

Please explain.

10. Since 2004, when Strategy was implemented, in what ways has the Strategy contributed to:
    - enhanced protection of children from sexual exploitation?
    - enhanced pursuit of those who use technology to facilitate the exploitation of children?

11. The Strategy has evolved over the last four years to include activities not anticipated at the outset. These are in the areas of:

    - Legislation/policy
    - ISP industry partnerships
    - Investigative partnerships
    - Research
    - Communications

    Can you briefly explain a) why these changes have occurred; b) what the contribution has been and; c) if they continue to be necessary and why.

    What is the impact of shifting resources into these areas? Are these areas sufficiently resourced?

12. How has the evolving nature of the initiative impacted its success? What are the specific challenges and opportunities presented by the evolution? Have the changes resulted in any unintended impacts (either positive or negative)?

Cost Effectiveness and Alternatives

13. Do you feel the Strategy has provided value-for-money for Canadian citizens? If yes, how so?

14. How has targeted research contributed to planning of education and awareness activities so that educational resources are used efficiently? What other impacts has targeted research had since the inception of the Strategy in 2004?

15. In the area of law enforcement, what efficiencies have been gained as a result of the *Cybertip.ca* triage function? (e.g. save money/ time, resources put where they are most needed). What else has helped realize efficiencies?

16. Are you aware if private or non-governmental organizations have provided financial or in-kind investments to the Strategy? If yes, please describe.

17. Are you aware of initiatives similar to the Strategy that exist in other countries? How does the success of these initiatives compare to the success of Strategy? What lessons learned could help improve the Strategy going forward?

Other

18. Is there anything else you would like to add?

Interview Guide 4
International Partners
Background

1. Please briefly describe your involvement or interaction with partners of the Canadian National Strategy for the Protection of Children from Sexual Exploitation on the Internet (Strategy).

Relevance

2. How has the nature, size or evolution of the problem of Internet-based child sexual exploitation changed over the last four years.

3. From your experience working with Canadian law enforcement, do you believe there are currently any aspects of the crime related to Internet-based child sexual exploitation that are not being addressed by the Canadian strategy? In your estimation, what is the level of effort that would be necessary to fill these gaps?

Success

4. By obtaining your answers to the questions in the following table, we hope to determine what changes have occurred since 2004 in each of the listed Strategy activity areas. Please give some thought to the level of impact the following activities have had, and we will fill out this table during the interview.

Activities	Since 2004, when Strategy was funded, how have the activities impacted:			
	the working relationship among law enforcement		the level of information sharing among law enforcement (investigations, victims and suspects)	
	Level of impact: • not applicable/ don't know • detrimental • not enhanced • enhanced • strongly enhanced	Please explain.	Level of impact: • not applicable/ don't know • detrimental • not enhanced • enhanced • strongly enhanced	Please explain.
Training and/or conferences				
Partnerships and agreements for cooperation with national and international law enforcement and ISPs				
Investigative support from the NCECC				
Other factors				

Have there been any challenges in these areas that have limited success?

5. One of the objectives of the Strategy is that investigations become more coordinated, comprehensive and efficient. From your perspective, since 2004, when the Strategy was funded, how have investigations changed? Has Strategy contributed to this change? Please explain.

6. Over the last four years, how have international partnerships with the Strategy contributed to:

   - enhanced protection of children from sexual exploitation?
   - enhanced pursuit of those who use technology to facilitate the exploitation of children?

Cost Effectiveness and Alternatives

7. Does your country have a national strategy that addresses crimes related to Internet-based child sexual exploitation? Please describe the key elements and/or activities of this strategy (i.e. legislative, law enforcement, education and awareness, etc.).

8. Please describe the types of partners involved in your (national) strategy e.g. other governmental organizations and/or private sector. Does your country include foreign representation (taskforce) within its strategy? How is funding allocated to each of these partners (what is the funding model)?

9. Please describe the successes that have been realized as a result of your (national) strategy. Can you compare this to Canada's strategy? (advantages/disadvantages, similarities/differences). Has Canada's strategy contributed to your national strategy and its success? How so?

10. Is your country involved in or leading any International Strategy? If so, what should Canada do to contribute to your country's International strategy? What barriers exist? How can they be overcome?

11. What lessons learned from your national or international strategy could help inform Canada's strategy going forward?

Interview Guide 5
Internet Service Providers

Background

1. Please briefly describe your role and involvement with the Strategy.

Relevance

2. How has the nature, size or evolution of the problem of Internet-based child sexual exploitation changed since the inception of the Strategy in 2004? Is there a continuing need for a national strategy that combats Internet-based child sexual exploitation? Why or why not?

3. Are there currently any aspects of the crime related to Internet-based child sexual exploitation that are not being addressed under the current strategy? In your estimation, what is the level of efforts that would be necessary to fill these gaps?

Success

4. Since 2004, the Strategy has involved three funded federal partners (PS, IC and RCMP) and a non-governmental organization (*Cybertip.ca*). Does each of these partners currently play the appropriate role? If not, what needs to change? What activities or programs might be transferred to other federal departments, other levels of government or the private/voluntary sector? Are there any activities or programs that would benefit from being incorporated into Strategy? Please explain.

5. Since 2004, when the Strategy was implemented, please describe how your partnerships/ and or agreements with law enforcement have impacted the level of information sharing. Have there been any challenges in these areas that have limited success?

6. a) Have Strategy activities (e.g. training, examination of legislative issues, ISP partnerships), increased **your knowledge** in the following areas?

   Please rate your answers as follows: *not applicable, no change, improved, significantly improved*

   - understanding of investigative and legal challenges
   - law enforcement best practices
   - measures to overcome challenges
   - other areas of knowledge increase

b) Have the activities contributed to increased knowledge **in general** among law enforcement, justice partners, and ISP providers? Please explain.

Please rate your answers as follows: *not applicable, no change, improved, significantly improved*

Knowledge Area	Law Enforcement	Justice Partners	ISP Providers
Understanding of investigative and legal challenges			
Law enforcement best practices			
Measures to overcome investigative and legal challenges			
Other areas of knowledge increase			

c) Are there other areas of training or awareness that need to be addressed going forward? E.g. education on the issue of Internet child sexual exploitation in general, challenges to law enforcement investigations, activities of *Cybertip.ca* etc.

7. Over the last four years, in what ways has the Strategy contributed to:
    - enhanced protection of children from sexual exploitation?
    - enhanced pursuit of those who use technology to facilitate the exploitation of children?

8. The Strategy has evolved over the last four years to include activities not anticipated at the outset. These are in the areas of:

    - Legislation/policy
    - ISP industry partnerships
    - Investigative partnerships
    - Research
    - Communications

    Can you briefly explain a) why these changes have occurred; b) what the contribution has been and; c) if they continue to be necessary and why.

    What is the impact of shifting resources into these areas? Are these areas sufficiently resourced?

9. How has the evolving nature of the initiative impacted its success? What are the specific challenges and opportunities presented by the evolution? Have the changes resulted in any unintended impacts (either positive or negative)?

Cost Effectiveness and Alternatives

10. Do you feel the Strategy program has provided value-for-money for Canadian citizens? If yes, how so?

11. What lessons learned could help improve the Strategy going forward?

Other

12. Is there anything else you would like to add?

Appendix D – Guide for Analysis of Interview Information

Number in Group	None (0%)	A few (1-24%)	Some (25-49%)	Many (50-74%)	Most (75-99%)	All (100%)
3	always answer using X out of four interviewees unless its ALL or NONE					
4	always answer using X out of four interviewees unless its ALL or NONE					
5	always answer using X out of four interviewees unless its ALL or NONE					
6	0	1	2	3-4	5	6
7	0	1-2	3-4	5	6	7
8	0	1-2	3-4	5-6	7	8
9	0	1-2	3-4	5-6	7-8	9
10	0	1-2	3-5	6-7	8-9	10
11	0	1-3	4-5	6-8	9-10	11
12	0	1-3	4-6	7-9	10-11	12
13	0	1-3	4-6	7-10	11-12	13
14	0	1-3	4-7	8-10	11-13	14
15	0	1-4	5-7	8-11	12-14	15
16	0	1-4	5-8	9-12	13-15	16
17	0	1-4	5-8	9-13	14-16	17
18	0	1-4	5-9	10-13	14-17	18
19	0	1-5	6-9	10-14	15-18	19
20	0	1-5	6-10	11-15	16-19	20
21	0	1-5	6-10	11-16	17-20	21
22	0	1-5	6-11	12-16	17-21	22
23	0	1-6	7-11	12-17	18-22	23
24	0	1-6	7-12	13-18	19-23	24
25	0	1-6	7-12	13-19	20-24	25