



HAMILTON POLICE SERVICES BOARD

NOTICE OF MEETING

PUBLIC AGENDA

October 18, 2010

4:00 o'clock p.m.

3rd Floor Board Room
Hamilton Central Station

Lois Morin
Administrator

AGENDA

1. **Call to Order**
2. **Presentation**
 - a) **PRIDE Award**
 - b) **Theft of Gas Drive-Offs (PSB 10-101 – see item 5 below)**
3. **Declarations of Interest**
4. **Adoption of Minutes – September 27, 2010**
5. **Theft of Gas Drive-Offs (PSB 10-101)**
6. **Pre-Budget Approval 2011 Vehicles (PSB 10-099; See Also PSB 02-052)**
7. **Hamilton Police Service Monthly Report (PSB 10-102)**
8. **Information Items**
 - (a) Budget Variance Report as at August 31, 2010 (PSB 10-095)
 - (b) City Clerk's Division – Council Follow-Up Notice – City Council Meeting – September 15, 2010.
 - (c) Correspondence from Paul Burroughs, President, City Holdings Corp. with respect to the ACTION programme.
 - (d) E-mail from Jennifer Lanzon, Executive Director, Canadian Association of Police Boards with respect to Cyber Security Strategy – Bulletin 115.
 - (e) Correspondence from Kelly Greve, President, Hamilton Police Female Choir expressing thanks for support to the 1st Annual Golf Tournament Fundraiser.

- (f) Thank you card from the organizers of the Travelling Flag Day Event Dedicated to All Soldiers, Remembrance of our Fallen and in Support of Allan's Angels Camp.
- (g) St. Joseph's Healthcare Foundation's: The Future of Hope: Annual Check Up, 2010, report to the community – page 7, Cops, Cats and Caring Students.

9. Other Business

10. Adjournment

THE POLICE SERVICES BOARD WILL ADJOURN THE PUBLIC PORTION OF THE MEETING AND RECONVENE IN CAMERA FOR CONSIDERATION OF PRIVATE AND CONFIDENTIAL MATTERS.

**MINUTES OF THE HAMILTON
POLICE SERVICES BOARD**

4.

Monday, September 27, 2010
4:00pm
Board Room
Hamilton Central Station

The Police Services Board met.

There were present: Bruce Pearson, Chair
 Nancy DiGregorio, Vice Chair
 Fred Eisenberger
 Bernie Morelli
 Irene Stayshyn
 Terry Whitehead

Absent with regrets: None

Also Present: Chief Glenn DeCaire
 Deputy Chief Eric Girt
 Deputy Chief Ken Leendertse
 Superintendent Ken Bond
 Superintendent Debbie Clark
 Superintendent Paul Morrison
 Superintendent John Petz
 Superintendent Bill Stewart
 Inspector Jamie Anderson
 Inspector Vince DeMascio
 Inspector Dan Kinsella
 Inspector Scott Rastin
 Marco Visentini, Legal Counsel
 Rosemarie Auld, Manager, Human Resources
 Staff Sergeant Steve Hahn
 Sergeant Barry Mungar
 Dan Bowman, Manager Fleet and Facilities
 Rita Lee Irvine, Manager, Corporate Planning
 Catherine Martin, Corporate Communicator
 Ted Mason, Chief Accountant
 Lois Morin, Administrator

Chair Pearson called the meeting to order.

Presentation

a) *Member of the Month for July 2010*

Chair Pearson and Chief Glenn DeCaire presented the Member of the Month Award for July 2010 to Detective Constable Peter Weisner. Constable Weisner was recognized for his persistence, actions and work ethic which exemplify our Mission Statement "in the prevention, detection and the suppression of crimes and the relentless pursuit of offenders".

b) Member of the Month for August 2010

Chair Pearson and Chief Glenn DeCaire presented the Member of the Month Award for August 2010 to Constable Josh Vyn. Constable Vyn was recognized for his self motivation, determination and teamwork that resulted in the recovery of stolen property.

c) P.R.I.D.E. Award

One of the values of the Hamilton Police Service is, "Providing Quality Service". This commitment to service excellence is an important part of an organizations journey towards being recognized by our community as one of the Best Police Services in this nation.

There are occasions when members of this Service go above and beyond the normal expectations of our citizens. These are not acts of courage in the face of extreme danger, but they are special acts of compassion, support and quality service that are worthy of recognition.

Chief DeCaire presented the P.R.I.D.E. ("People Really Interested in Delivering Excellence") Award to Hamilton Police Services Facilities Technician Joe Hnatyshyn. Joe Hnatyshyn was recognized for his efforts in the Services custody bed project. As a result, the service realized a cost savings of \$60,000. He served this organization with PRIDE.

d) Presentation-ProAction – The Journey – Reaching New Heights

Deputy Chief Leendertse provided a presentation with respect to the 3rd ProAction Event, "The Journey: - Reaching New Heights".

(Item 2)

Declarations of Interest

None

(Item 3)

Adoption of Minutes – August 9, 2010 & August 30, 2010

Moved by: Member Eisenberger
Seconded by: Member Morelli

The minutes of the meeting held Monday, August 9, 2010 and August 30, 2010, were adopted as printed.

Carried.

(Item 4)

**Hamilton Police
Service Monthly
Report****PSB 10-092****Information Items**

As recommended by Chief DeCaire in Report PSB 10-092 dated September 27, 2010, the Board approved the following:

Moved by: Member Morelli
Seconded by: Vice Chair DiGregorio

That the Board direct the Administrator of the board to refer this report, in its entirety, to the City of Hamilton, for information.

Carried.

(Item 5)

The Board approved the following recommendation:

Moved by: Member Eisenberger
Seconded by: Member Morelli

The Board receive the reports / correspondence as circulated.

- (a) Police Week 2010 (PSB 10-080)

Note: The Board requested that this report be expanded and include more information with respect to Police Week.

- (b) Public Disclosure of Operating Budget Information (PSB 10-054a)
- (c) Correspondence from Neil Everson, Director, Economic Development & Real Estate Division expressing appreciation to Chief Glenn DeCaire and his team for their outstanding contribution to the recent Canada Bread employee tours of Hamilton.
- (d) Correspondence from Richard and Lynn Hamilton with respect to the recent Hamilton Police Service Promotions Ceremony held on Wednesday, July 14, 2010.
- (e) Correspondence from Glenn Murray, Assistant Deputy Minister, Public Safety Division with respect to Staffing Changes – Police Quality Assurance Unit.
- (f) Article from the Word on the Street – South Stipeley Neighbourhood with respect to Chief Glenn DeCaire visits South Stipeley.
- (g) Correspondence from Frederick Dryden, Founder/Executive Director, Liberty for Youth with respect to the 5th Consecutive Liberty and Justice Community Event.

- (h) Copy of correspondence from Chief Glenn DeCaire with respect to the Long-Gun Registry, which was send to all Members of Parliament.
- (i) Correspondence from Jennifer Lanzon, Executive Director, Canadian Association of Police Boards with respect to September 15, 2010, National Day in Support of Long Gun Registry.
- (j) Correspondence from Chief Daniel Parkinson, Cornwall Community Police Service, President, Ontario Association of Chiefs of Police with respect to the summons received by Commissioner Julian Fantino of the Ontario Provincial Police and the private prosecution sections of the *Criminal Code of Canada*.
- (k) Correspondence from Ruth Pretty, Executive Director, Niagara victim Crisis Support Service Inc. with respect to the Hamilton Police Service Raffle Prize Donation.

Carried.

(Item 6)

Other Business

Mounted Unit

The Board commended the Mounted Unit noting that the community is very impressed by their presence around the city.

Deputy Chief Ken Leendertse reminded the Board that the Mounted Unit is a three year pilot project and that an interim report will be submitted to the Board in January 2011.

Thanks

Member Whitehead expressed his thanks to Superintendent Ken Bond for the hard work and dedication he provided to Division 3, wishing him well in his new position in Support Services. He further mentioned that he was looking forward to working with Superintendent Debbie Clark and building the same rapport as he has had with all other Superintendents.

(Item 7)

Adjournment

Moved by: Member Eisenberger
Seconded by: Vice Chair DiGregorio

The public portion of the meeting then adjourned at 4:50pm.

Carried.

(Item 8)

* * * * *

The Board then met in camera to discuss matters of a private and confidential nature.

Taken as read and approved

Lois Morin
Administrator

Bruce Pearson, Chair
Police Services Board

September 27, 2010
lem:

HAMILTON POLICE SERVICES BOARD**- RECOMMENDATION -**

DATE: 2010 October 18
REPORT TO: Chair and Members
Hamilton Police Services Board
FROM: Glenn De Caire
Chief of Police
SUBJECT: *Theft of Gas Drive-Offs*
(PSB 10-101)

RECOMMENDATION:

That the Board request the City of Hamilton develop and enact a Public Safety By-law requiring the pre-payment of gas, 24-hours a day, at all service stations throughout the City of Hamilton.


Glenn De Caire
Chief of Police**FINANCIAL / STAFFING / LEGAL IMPLICATIONS:**

FINANCIAL – n/a

STAFFING – n/a

LEGAL – The matter will be forwarded to City Council for approval to develop and enact a Public Safety By-law.

BACKGROUND:

The theft of gas is a crime that has plagued the City of Hamilton for many years. Over a one (1) year period, from July 2009 – July 2010, there were 271 gas thefts reported to the Hamilton Police Service.

A complex analysis of this issue has revealed that only 5% of the reports taken resulted in charges and it is evident that the amount of police resources being exhausted on these investigations is significant.

This type of crime is completely preventable. Our research has shown that the theft of gas can lead to incidents of violence. It is our position that the City of Hamilton should enact a public safety by-law that will assist in the prevention of this crime.

ISSUE

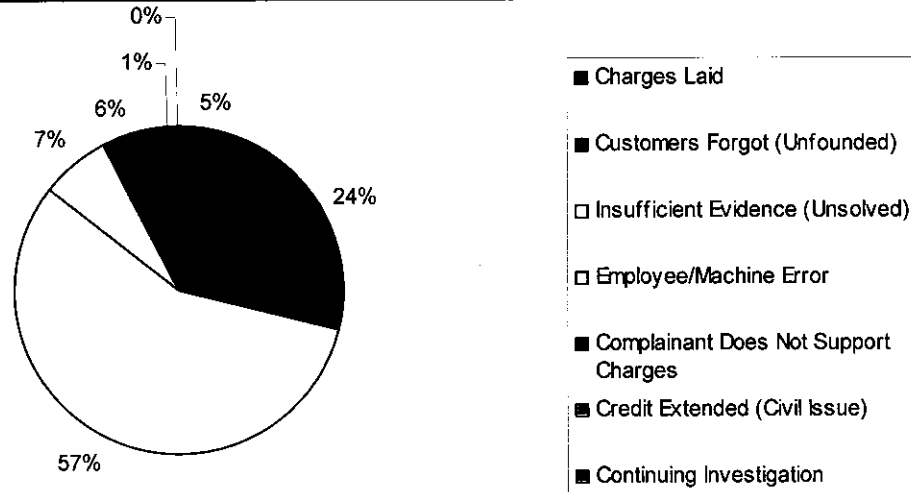
Gas theft is not a crime specific to our region. Police Services from all over the province, and the country, are experiencing the same frustration with regards to this crime trend.

A best practices business case revealed a 2005 criminal case, from British Columbia, of a 24-year old gas station employee named Grant De Patie. This young man was dragged underneath a car for seven (7) kilometers after he tried to stop a \$12.00 gas theft. In response to Grant's death, British Columbia became the first and only province, in Canada, to enact a 'pay-before-you-pump' provincial law in 2008, which is now known as *Grant's Law*. This law falls under the *British Columbia Workplace Safety Act* known, as WorkSafe B.C.

ANALYSIS

A comprehensive analysis was completed on the 271 gas thefts reported to the Hamilton Police Service. The statistics showed that the value of gas stolen varied greatly ranging from \$5.06 to \$189.96. The analysis also revealed surprising results with regard to the outcome of these gas theft investigations (*see pie chart on next page*).

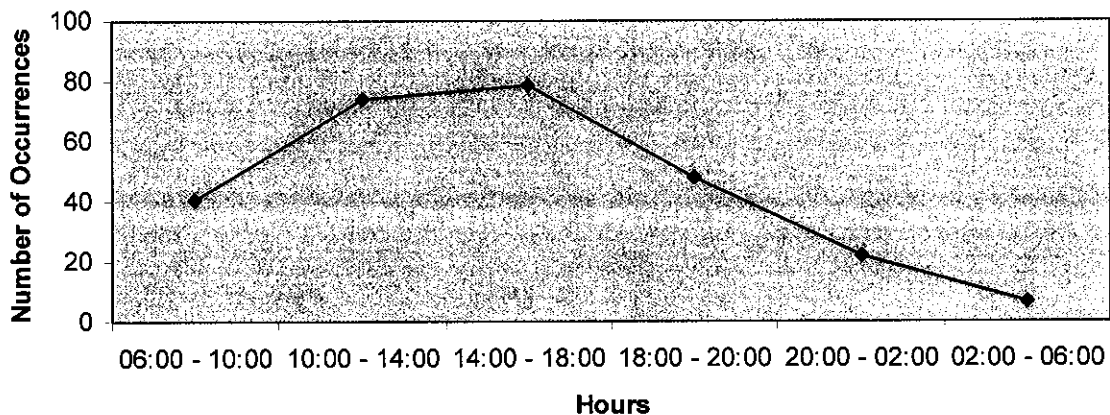
Gas "Drive-Off" Theft Investigation Results (Percentages)



The majority of these investigations go unsolved (57%) or it is a situation where customers forgot to pay (24%). More importantly, these statistics prove that every gas theft could have been prevented had the gas station adhered to a 24-hour pre-payment policy.

While several gas bars in our region (42%) do have a pre-payment policy during late evening hours (typically 10 p.m.-6 a.m.) our review showed that the majority of gas thefts actually occur between the hours of 10:00 a.m. – 6:00 p.m. (see line graph below).

Time of Day Gas Drive-Offs Occurred



In August of 2010, a letter and survey was sent to the 89 gas bar owners in our region. The letter explained that the Hamilton Police Service was conducting research about gas theft and requested they complete an enclosed short survey.

Thirty-eight completed surveys were received back and revealed several interesting facts. The most disturbing statistic was that 29% of the gas bar owners surveyed indicated that their employees had experienced an act of violence while trying to stop a gas theft.

The percentage for 'acts of violence' was alarming because, in most cases, the crime was never reported to the police. One (1) gas bar manager, who has been in the business for 21 years, disclosed that she had been violently assaulted 15 years ago while trying to stop a gas theft and had her two (2) front teeth knocked out. She further advised that more recently, one (1) of her employees suffered serious injuries because he was dragged underneath a car when he tried to stop a gas and dash.

Research revealed that the main reason the gas station owners are not implementing a 24-hour gas pre-payment policy is because the major gas corporations have advised the gas station owners that it is against company policy to make gas pre-payment mandatory, because it is not 'customer friendly'. However, a few stations in the city have chosen to ignore this policy and adopt a 24-hour pre-payment policy because they too recognize the risk of injury and loss of revenue.

The gas station owners have expressed frustration with their company's policy and the majority of gas station owners are in support of mandatory 24-hour pre-payment.

RECOMMENDATION

The analysis of this issue has led us to conclude that this type of crime is completely preventable and the introduction of a City of Hamilton by-law making 24 hour gas pre-payment mandatory would help eliminate gas theft in our city. A Public Safety By-law for the pre-payment of gas would also eliminate the number of violent crimes that occur because of gas thefts.

CONCLUSION

The Hamilton Police Service believes that a By-law would be a proactive approach in order to avoid any such incidents as the one (1) that took the young life of Grant De Patie. Furthermore, it is apparent from the surveys received that this is a great concern for our gas bar owners.

The amount of police resources being spent on these crimes, coupled with the low percentage of charges laid, are strong indicators that prevention strategies must be implemented.

Most importantly, the risk of injury or loss of life is far too great a consequence for what is ultimately a 100% preventable crime. Therefore, it is our position that the Board recommend to the City of Hamilton, that a By-law be enacted to ensure all service stations, within the City of Hamilton, comply with a 24-hour pre-payment policy.

GD/K. Leendertse

HAMILTON POLICE SERVICES BOARD**- RECOMMENDATION -**

DATE: 2010 October 18
REPORT TO: Chair and Members
Hamilton Police Services Board
FROM: Glenn De Caire
Chief of Police
SUBJECT: *Pre-Budget Approval 2011 Vehicles*
(PSB 10-099; see also PSB 02-052)

RECOMMENDATIONS:

- a) That the Board pre-approve the expenditure of \$700,000.00 for the purchase of twenty (20), 2011 police cruisers.
- b) That the Board pre-approve the expenditure of \$90,000.00 for the purchase of Two (2) 2011 4x4 police cruisers.
- c) That the Board pre-approve the expenditure of \$335,000.00 for the purchase of twelve (12) used plain door vehicles.
- d) That the Board pre-approve the expenditure of \$60,000.00 for the purchase of two (2) 2011 full size Cab and Chassis for Prisoner Transport Refit.
- e) That the Board pre-approve the expenditure of \$80,000.00 for the purchase of four (4) used mini vans.
- f) That the Board pre-approve the expenditure of \$100,000.00 for the purchase of four (4) 2011 Police Motorcycles.
- g) That Fleet staff be authorized to participate in the Provincial Co-Operative Purchasing for the above-mentioned cruisers.
- h) That Fleet staff be authorized to purchase used plain door vehicles, as outlined in *PSB 02-052 - Used Vehicle Purchases*.
- i) That the Board pre-approve the expenditure of \$179,500.00 for the upfitting of the above-referenced vehicles.
- j) That the Board pre-approve an expenditure up to \$100,000.00 for the repowering of Marine 1-Hike, including two (2) replacement diesel engines and drives.

- k) That the funds for the acquisition of the new vehicles be taken from the Vehicle Replacement Account #53415, funds for the upfitting of the equipment be taken from Fleet Supplies Account #53039 and that the funds for the replacement of the marine engines be taken from the Fleet Repairs Account #55135.



Glenn De Caire
Chief of Police

FINANCIAL / STAFFING / LEGAL IMPLICATIONS:

FINANCIAL – The total cost of procuring the above-noted vehicles is estimated to be \$1,365,000.00. Revenue of approximately \$75,000.00 will be realized when replaced vehicles are disposed of during 2011. The total cost of supply and replacement of the two (2) marine engines and drives is estimated at \$100,000.00. The request for these replacement vehicles and engines has been included in the 2011 Budget Submissions for the Fleet Branch.

STAFFING – n/a

LEGAL – n/a

BACKGROUND:

Command staff, within Corporate Services, are requesting the pre-approval of these funds to allow ordering of replacement vehicles and equipment in the fall of 2010 to allow for early delivery and deployment in 2011.

Many of the used vehicles will be purchased during December and January when resale prices are at their lowest. This maximizes the purchasing power of the available funding.

New police package units will be purchased through the Provincial Police Co-operative Purchasing Group (PCPG). All major participants in the PCPG have been asked for their projected numbers, as well as a commitment to purchase the police cruisers in the fall, with delivery early in the new year. The calling agency for the Police Co-Operative Purchasing Group for 2011 was the Ministry of Government Services - Ontario Shared Services Vehicle Acquisition Program.

The balance of the vehicles being recommended for Pre-Budget Approval will be procured using the guidelines set forth in *PSB 02-052* for the purchase of used vehicles.

Vehicle manufacturers have consistently been pushing the build out dates earlier and earlier and it is necessary to order most vehicles in the fall to meet build out dates. This is the final year for the Ford Interceptor (Crown Victoria). Ford has advised of the importance of early ordering indicating that once the orders and allocations have been maximized, no more orders can be placed. It is expected that many police agencies in North America will be ordering extra allotments of Crown Victoria's to assist with the transition into the new Taurus police package. This will lead to ordering deadline cut off dates advancing from mid-winter into early winter or late spring for this vehicle.

The replacement of the two (2) Volvo Penta Diesel engines and drives is essential to ensure the vessel can be used in the 2011 boating season. The current replacement value of the Hike is \$125,000.00 based on a marine survey conducted in 2009, by Gill Bibby. The replacement value of a new vessel is approximately \$600,000.00.

The Hike was purchased in 1999 and has been the primary search, rescue and enforcement vessel for the Hamilton Police Service and the combined Hamilton/Halton Joint Marine Agreement that was dissolved in 2009. The engines have surpassed their useful life and are in poor condition, unreliable and must be replaced prior to the 2011 marine season. The infrastructure of the vessel is sound based on fleet staff evaluation which is supported by the marine maintenance contractor that services this vessel.

Repowering of the vessel is recommended as the most economically responsible action vs. the replacement of the whole vessel with a new one. During the 2010 season, it was necessary to borrow the RCMP vessel on numerous occasions when the vessel was out of service due to engine problems. The high cost associated with this engine replacement is due to the fact that they are high durability diesel engines designed for the marine application. Exact replacements are no longer available so there is a cost associated with adapting the vessel to accommodate the new design and refitting of the engine and outdrive assemblies. The long delivery period associated with the replacement engines makes it imperative that this project commence this fall in order to be ready for the spring of 2011.

GD/D. Bowman

cc: Superintendent Michael Shea, Corporate Services

Ted Mason, Chief Accountant

Donna Ciardullo, Purchasing Agent, City of Hamilton

HAMILTON POLICE SERVICES BOARD**- INFORMATION -**

DATE: 2010 October 18
REPORT TO: Chair and Members
Hamilton Police Services Board
FROM: Glenn De Caire
Chief of Police
SUBJECT: *Hamilton Police Service Monthly Report*
(PSB 10-102)

BACKGROUND:

That the Board direct the Administrator of the Board to refer this report, in its entirety, to the City of Hamilton, for information.



Glenn De Caire
Chief of Police

FINANCIAL/STAFFING/LEGAL IMPLICATIONS:

FINANCIAL - n/a

STAFFING - n/a

LEGAL - n/a

BACKGROUND:

Hamilton Officers win ASIS International – Toronto Chapter Law Enforcement Appreciation Award

Detective Jim Elliot, Sergeant Sabrina Feser and Detective Constable Andrea Richard received the 2009 ASIS International-Toronto Chapter Law Enforcement Appreciation Award for outstanding work in the area of 'Crimes of Violence'.

Founded in 1955 as the American Society for Industrial Security (ASIS), the organization officially changed its name in 2002 to **ASIS International**.

The Officers were recognized for their efforts that began on February 14, 2009, when a man was discovered by Uniform Officers, in an apartment where he had been confined and tortured.

The Officers were notified and took over the investigation. They determined that the victim had been held against his will and brutally tortured over an extended period of time.

They conducted numerous interviews, executed search warrants and collected evidence, including weapons and devices used by the suspects to beat and burn the victim.

The Officers also interviewed the three (3) accused and were able to elicit valuable confessions from them, outlining their horrible acts committed against the victim. Further investigations resulted in the arrest and charges against a fourth young offender.

The investigators, and in particular, Detective Jim Elliott, were praised by both the Crown and by one (1) of the Defence lawyers for the outstanding testimony that was presented.

During sentencing of the three (3) adult offenders, Judge Fred Campling, said the vicious beatings, acts of torture and degradation that were inflicted on a 22-year-old mentally-challenged man, during 17 days of captivity, met all the features of "stark-horror cases," for which the courts reserve the maximum punishments set out in the Criminal Code of Canada. He then sentenced the three (3) adults to penitentiary terms ranging from ten (10) to 14 years.

This was a disturbing case that garnered local and national attention. It required considerable care and compassion towards the victim while at the same time required gathering all the facts in order to put together the case against the accused. These Officers worked on their days off and liaised with many of the partners who had an impact on the case including: victim services, social agencies, courts, other police agencies and correctional facilities.

The fact that all accused pleaded guilty and received long prison sentences is a testament to the outstanding investigation that these Officers conducted.

Hamilton Police Stolen Sisters/Sisters in Vigil

Over 40 people attended the Service's *Stolen Sisters/Sisters in Vigil* event in partnership with Amnesty International, OPP, RCMP and the Aboriginal community. The solemn and respectful event was held on October 4, 2010, and took place outside of the Division Three Police Station, at the site of a white pine tree. The tree was planted five (5) years ago to commemorate the vigil. All names of the Hamilton and area Aboriginal women reported missing or murdered, 177 of the 582 in Canada, were read aloud by various participants, including the Vice Chair, of the Hamilton Police Services Board, Nancy Di Gregorio.

Rwandan Genocide

On October 6, 2010, three (3) survivors of the Rwandan Genocide were the featured speakers of a Lunch and Learn for members of Hamilton Police Service. Over 20 members gathered to hear the survivors' experiences, as well as lessons learned. The compelling stories led to member engagement and increased understanding and awareness.

Police Recruitment Night

The Hamilton Police Recruitment Team held a Police Recruiting Session, on Thursday, October 7, 2010, at St. Thomas More High School. There were 126 people who attended to learn more about the process of becoming a police officer. The lively question and answer period included five (5) off-duty Hamilton Police officers who joined the panel to speak with attendees.

Inspector David Calvert Graduates from University of Toronto's Rotman School of Management

October 9, 2010, saw the graduation of Inspector David Calvert, Support Services, from the Police Leadership Program – an MBA-style program delivered at the University of Toronto's Rotman School of Management. Insp. Calvert was one (1) of 19 senior police leaders from across the province to complete the program.

The Police Leadership Program provides leadership and management training for police leaders in municipal, provincial, and military police services nationwide.

Live from Police Headquarters

Central Police Station was the scene of the 6th stop of CHML's Bill Kelly's *Unleashed* broadcast on October 15, 2010. For three (3) hours, the show broadcast from the Bill Sturup Media and Community Room. Joining me on the program was Hamilton Police Services Board Chair Bruce Pearson, our Recruiting Team, Crime Prevention and Road Safety experts.

Upcoming Events:

Operation Yellow Ribbon Fundraiser

October 21, 2010, 11:30 a.m. - 1:30 p.m.

Central Police Station

All proceeds will go to 31st Brigade Military Family Resource Centre and the RHLI 13th Regiment Foundation. Everyone is welcome to attend.

2nd Cop Shop Skate Jam

On Saturday, October 23rd, 2010, between 11:00 a.m. - 3:00 p.m., Division Three will be hosting the 2nd Annual Cop Shop Skate Jam, at Turner Skate Park, beside the Station. The event was held last year and approximately 250 youth attended.

The day will consist of boarding demos, competitions, a barbecue and there will be a live DJ on site. Officers Scott Hamilton and Gerald Blanchard are the prime organizers.

The ACTION (Addressing Crime Trends In Our Neighbourhoods) Weekly Update

This update is sent weekly to neighbourhood BIA's, City Councillors, and HPS Crime Managers. The same is also posted on the HPS Website.

Update for October 10, 2010 is attached.

GD/C. Martin

Attachment: *The Action Weekly: October 10, 2010*

THE ACTION

Addressing **Crime Trends In Our Neighbourhoods**

WEEKLY

For October 10, 2010

Crime Brothers Returned to Montreal

Twin brothers who were responsible for over 100 offences in Hamilton during the last few years were returned to Montreal to face charges on an outstanding warrant. ACTION Officers, the Hamilton Crown Attorney's Office and the Montreal Police worked together to have these two men returned to face the charges. The brothers themselves wished to return to Quebec where they have more family support to help them turn their lives around. The brothers final comment to the Hamilton Officers at the Quebec border was, "You guys have done us a solid, and will never see us again".



Montreal Police will now be looking after the twins

ACTION Officers assist with POP Project to address prostitution in Landsdale Neighbourhood

Police received a complaint about an increase in prostitution in the Landsdale neighbourhood. A problem oriented policing project (POP) was created to address the issue. ACTION Officers worked with the neighbourhood association as well as Patrol, Vice and Undercover officers; developing strategies to help

solve the problem. The project led to the arrest of 16 johns and 6 janes. The project was successful not just because of the number of arrests, but by the feedback from community members who commented on a reduction in fear of crime. The project conclusion discussed ACTION's role in addressing the problem.

During the project, ACTION members were assigned to this area and through tenacity and diligence effectively supported the project goals. Not only did their mere presence discourage offenders from attending the location but also decreased the level of neighbourhood fear of crime. The enforcement of the ACTION team led to a disruption of criminal networks and a deterrence of negative externalities associated to the street level sex trade.

Police Continue to Enforce Prostitution Laws

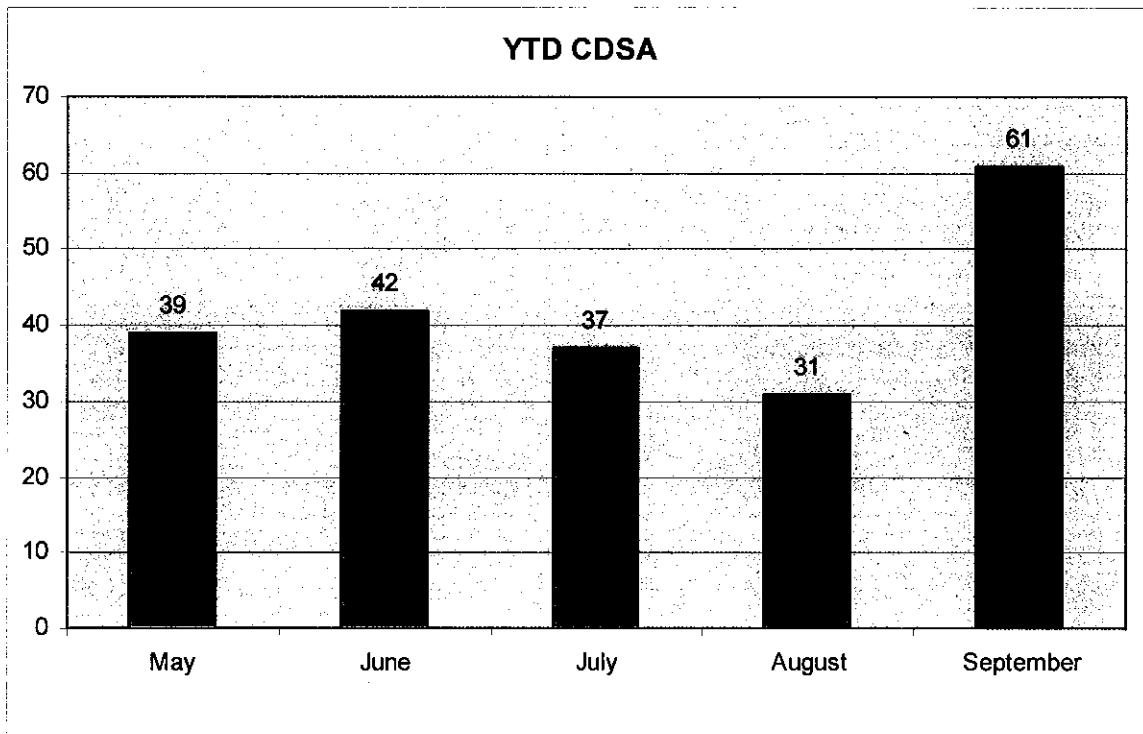
A recent Ontario Supreme Court ruling made many prostitution laws unconstitutional. The ruling is being appealed and

during this time it will be status quo. The following message was issued to all Hamilton Officers by Deputy Chief Ken Leendertse.

It is the position of the Hamilton Police Service that there is no impediment to the police laying charges in relation to prostitution offences while the decision is stayed. If necessary, requests for advice in relation to such charges by police officers should be directed to the Crown Attorney or his or her designate. However, where appropriate, police officers are reminded to consider all applicable charges not implicated by Himel J.'s decision.

Partnership lead to Increase in Drug Arrest

ACTION Officers arrested 61 people for drug offences last month. ACTION Officers have been working with local businesses who have provided both information on drug dealers as well as locations to view the transactions. The result of this partnership was a doubling of drug arrests.



Drug arrests made by ACTION Officers since May. Community contacts have led to partnerships with business which have improved investigation techniques.

To read comments on ACTION or to submit your own, please go to the Hamilton Police Website at www.hamiltonpolice.on.ca or click below.

www.hamiltonpolice.on.ca/HPS/Action/



The ACTION Team (Addressing Crime Trends In Our Neighbourhoods) is a part of the Hamilton Police Neighbourhood Safety Project. ACTION is a Ministry of Community Safety and Correctional Services provincially funded initiative dedicated to reducing violence and disorder in our neighbourhoods, increasing safety in the community and improving the quality of life for all citizens of Hamilton.

**HAMILTON POLICE SERVICES BOARD
RECOMMENDATION**

8.

DATE: October 18, 2010

REPORT TO: Chairman and Members, Hamilton Police Services Board

FROM: Lois Morin, Administrator

SUBJECT: Information Items

RECOMMENDATION:

That the following reports / correspondence, be received:

- (a) Budget Variance Report as at August 31, 2010 (PSB 10-095)
- (b) City Clerk's Division – Council Follow-Up Notice – City Council Meeting – September 15, 2010.
- (c) Correspondence from Paul Burroughs, President, City Holdings Corp. with respect to the ACTION Program.
- (d) E-mail from Jennifer Lanzon, Executive Director, Canadian Association of Police Boards with respect to Cyber Security Strategy – Bulletin 115.
- (e) Correspondence from Kelly Greve, President, Hamilton Police Female Choir expressing thanks for support to the 1st Annual Golf Tournament Fundraiser.
- (f) Thank you card from the organizers of the Traveling Flag Day Event Dedicated to All Soldiers, Remembrance of our Fallen and in Support of Allan's Angels Camp.
- (g) St. Joseph's Healthcare Foundation's: The Future of Hope: Annual Check Up, 2010, report to the community – page 7, Cops, Cats and Caring Students.

HAMILTON POLICE SERVICES BOARD
- INFORMATION -

DATE: 2010 October 18
REPORT TO: Chair and Members
Hamilton Police Services Board
FROM: Glenn De Caire
Chief of Police
SUBJECT: *Budget Variance Report as at August 31, 2010*
(PSB 10-095)

BACKGROUND:

As at May 31, 2010, net expenditures are \$80,538,058 or 64.90% of the 2010 Operating Budget of \$124,090,530. The Budget Variance Summary is provided in the attached Appendix. Overall, revenues and expenditures are on budget.



Glenn De Caire
Chief of Police

GD/T. Mason
Attachment: *Appendix*

**HAMILTON POLICE SERVICE
BUDGET VARIANCE REPORT AS AT AUGUST 31, 2010**

	2010 Budget	2010 Actual	Available Balance	% Spent	Explanations
EXPENDITURES					
Salaries and Wages	\$ 89,231,130	\$ 58,981,450	\$ 30,249,680	66.10%	Salaries and Wages are on budget
Employee Benefits	\$ 22,132,180	\$ 15,334,192	\$ 6,797,988	69.28%	CPP/EI spending is higher through the first three quarters of the year before annual limits are met
Court/Overtime	\$ 3,058,650	\$ 1,586,272	\$ 1,472,378	51.86%	Represents the payout for the first half of the year
Sick Leave	\$ 958,120	\$ 456,225	\$ 501,895	47.62%	Higher expenditures are experienced at year end
Materials/Services	\$ 12,188,590	\$ 7,456,342	\$ 4,732,248	61.17%	
Capital Financing/Chargebacks	\$ 3,555,450	\$ 2,387,094	\$ 1,168,356	67.14%	
TOTAL EXPENDITURES	\$ 131,124,120	\$ 86,201,575	\$ 44,922,545	65.74%	Overall expenditures are on target
REVENUE					
General Revenues	\$ (3,593,590)	\$ (3,370,184)	\$ (223,406)	93.78%	Favourable variance due to revenue from Olympics participation covering salaries and overtime
Capital/Vehicle Reserve Revenue	\$ (500,000)	\$ (333,333)	\$ (166,667)	66.67%	
Provincial Grant Revenue	\$ (2,690,000)	\$ (1,793,333)	\$ (896,667)	66.67%	
Police Tax Stabilization Reserve	\$ (250,000)	\$ (166,667)	\$ (83,333)	66.67%	
TOTAL REVENUE	\$ (7,033,590)	\$ (5,663,517)	\$ (1,370,073)	80.52%	Overall revenues are on target
NET BUDGET	\$ 124,090,530	\$ 80,538,058	\$ 43,552,472	64.90%	Net Budget is on target

City Clerk's Division
COUNCIL FOLLOW-UP NOTICE

TO: Lois Morin, Administrator
Hamilton Police Services Board

DATE: September 23, 2010

FROM: Carolyn Biggs
Legislative Assistant, City Clerks

RE: **City Council Meeting – September 15, 2010**

The following resolutions were approved by City Council at its meeting held on Wednesday, September 15, 2010 at Items 2 and 3 of Committee of the Whole Report 10-024:

2. Funding Agreement: Safer Communities – 1,000 Officers Partnership Program (SCOPP) (PSB05-055(i)) (City Wide) (Item 5.3)

That the Mayor and City Clerk be authorized and directed to execute the Funding Agreement: Safer Communities – 1,000 Officers Partnership Program (SCOPP) respecting additional funding for front-line officers between Her Majesty in Right of Ontario, as represented by the Minister of Community Safety and Correctional Services, the City of Hamilton and the Hamilton Police Services Board, such agreement to be in a form satisfactory to the City Solicitor.

3. Community Policing Partnerships (CPP) Program: Agreement with the Ministry of Community Safety and Correctional Services for Additional Funding for Front-line Officers (PSB98-069(h)) (City Wide) (Item 5.4)

That the Mayor and City Clerk be authorized and directed to execute the Community Policing Partnerships (CPP) Program Agreement respecting additional funding for front-line officers between the Province of Ontario, the City of Hamilton and the Hamilton Police Services Board, such agreement to be in a form satisfactory to Corporate Counsel.

The agreements have been forwarded to the Mayor and City Clerk for execution and as requested, all copies will be returned to you. I understand you will be forwarding a copy of each agreement to the City once they have been fully executed.

Please call me if you have any questions.

Thank you.

cab.



RECEIVED

SEP 20 2010

HAMILTON POLICE SERVICES BOARD

September 20, 2010

Hamilton Police Services Board,
155 King William Street,
P.O. Box 1060, LCD 1,
Hamilton, Ontario,
L8N 4C1

Ladies and Gentlemen:

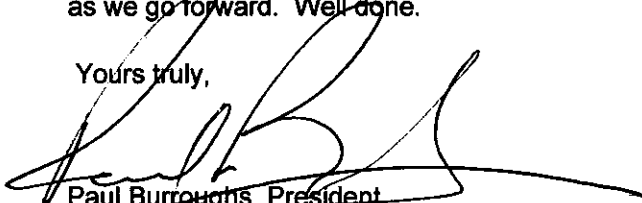
I am writing you today to commend you and the force on the enactment of the ACTION programme. As a business located very close to the Wesley Centre on Ferguson Avenue we have experienced many problems over the years. It has become increasingly frustrating to try and operate a business with drug deals going on beside us and drunks yelling profanities at our customers and staff. The police were in the area constantly but little improved.

I have watched the officers who are part of the ACTION Team and they seem able to accomplish what others were not able to accomplish previously. They are professional and friendly along with being proactive and in larger numbers as the need arises.

I believe that the programme is creating a new level of confidence in our Police Service and a new level of enthusiasm within the neighbourhood that it will help to create a safe city and improve the quality of life for Hamiltonians.

I hope that this is just the beginning and that our officers will become important pieces of our community as we go forward. Well done.

Yours truly,



Paul Burroughs, President
City Holdings Corp.

Morin, Lois

From: Jennifer Lanzon [jlanzon@capb.ca]
Sent: Tuesday, October 05, 2010 10:57 AM
To: CAPB Members
Subject: Cyber Security Strategy - Bulletin115

To: CAPB Members & Partners
Re: Bulletin Cyber Security Strategy

The Honourable Vic Toews, Canada's Minister of Public Safety launched *Canada's Cyber Security Strategy* on October 3, 2010. The Strategy will invest in securing Government of Canada systems, as well as partnering with other governments and with industry to ensure systems vital to Canadian security, economic prosperity and quality of life are protected. It also includes boosting education and awareness to better help Canadians keep their personal information safe and secure when online at home and at work.

Backgrounder: Canada's Cyber Security Strategy

A secure cyberspace is key to Canada's competitive advantage in the global marketplace where industry relies on secure, stable and resilient digital infrastructure to transact business and protect personal and commercially sensitive information such as intellectual property. But just as cyberspace is constantly evolving, so too are the cyber threats to our security, prosperity and quality of life.

Canada's Cyber Security Strategy is Canada's plan to ensure that Canadians can continue to benefit from the advantages of our increasingly digital economy without suffering from the risks inherent in a digital world. This Strategy will enhance the ability of Canadians, their governments and industry to use cyberspace with greater protection and confidence, ensuring it is a place where Canadians can play, work and live safely.

The Strategy will support Canada's national security, economic prosperity, and the quality of life of Canadians and is built upon three pillars:

1. **Securing Government systems** – The Government will put in place the necessary structures, tools and personnel to meet its obligations for cyber security.
2. **Partnering to secure vital cyber systems outside the federal government** – In cooperation with provincial and territorial governments and the private sector, the Government will support initiatives and take steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors.
3. **Helping Canadians to be secure online** – The Government will assist Canadians in getting the information they need to protect themselves and their families online.

Cyber security is a shared responsibility, one in which Canadians, their governments, the private sector, and our international partners all have a role to play. *Canada's Cyber Security Strategy* reflects this shared responsibility.

This investment is part of *Budget 2010: Leading the Way on Jobs and Growth*, which allocated \$90 million over five years, and \$18 million in ongoing funding, towards the Cyber Security Strategy.

Internet crime or cyber crime has been identified by the members of Canadian Association of Police Boards as an important issue; in fact CAPB has approved resolutions on this topic at the 1996, 1997, 2001, 2005 and 2006 Annual General Meetings.

10/12/2010

A copy of the Cyber Security Strategy is attached for your information.

Jennifer Lanzon | Executive Director | Canadian Association of Police Boards
157 Gilmour Street, Suite 302, Ottawa, ON K2P 0N8
613.235.2272 office | 613.235.2275 fax | jlanzon@capb.ca | www.capb.ca

This transmission may contain confidential or privileged communications, and the sender does not waive any related rights and obligations. If you are not the intended recipient and have received this in error, you must immediately destroy it. Unauthorized copying or distribution of any information herein is strictly prohibited and may constitute a criminal offence, a breach of provincial or Federal privacy laws, or may otherwise result in legal sanctions. We ask that you notify the Canadian Association of Police Boards immediately of any transmission received in error, by reply e-mail to the sender.



BULLETIN!
October 5, 2010

GOVERNMENT OF CANADA LAUNCHES CYBER SECURITY STRATEGY

The Honourable Vic Toews, Canada's Minister of Public Safety launched *Canada's Cyber Security Strategy* on October 3, 2010. The Strategy will invest in securing Government of Canada systems, as well as partnering with other governments and with industry to ensure systems vital to Canadian security, economic prosperity and quality of life are protected. It also includes boosting education and awareness to better help Canadians keep their personal information safe and secure when online at home and at work.

Backgrounder: Canada's Cyber Security Strategy

A secure cyberspace is key to Canada's competitive advantage in the global marketplace where industry relies on secure, stable and resilient digital infrastructure to transact business and protect personal and commercially sensitive information such as intellectual property. But just as cyberspace is constantly evolving, so too are the cyber threats to our security, prosperity and quality of life.

Canada's Cyber Security Strategy is Canada's plan to ensure that Canadians can continue to benefit from the advantages of our increasingly digital economy without suffering from the risks inherent in a digital world. This Strategy will enhance the ability of Canadians, their governments and industry to use cyberspace with greater protection and confidence, ensuring it is a place where Canadians can play, work and live safely.

The Strategy will support Canada's national security, economic prosperity, and the quality of life of Canadians and is built upon three pillars:

1. **Securing Government systems** – The Government will put in place the necessary structures, tools and personnel to meet its obligations for cyber security.
2. **Partnering to secure vital cyber systems outside the federal government** – In cooperation with provincial and territorial

governments and the private sector, the Government will support initiatives and take steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors.

3. **Helping Canadians to be secure online** – The Government will assist Canadians in getting the information they need to protect themselves and their families online.

Cyber security is a shared responsibility, one in which Canadians, their governments, the private sector, and our international partners all have a role to play. *Canada's Cyber Security Strategy* reflects this shared responsibility.

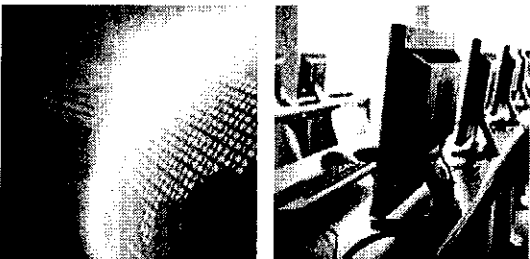
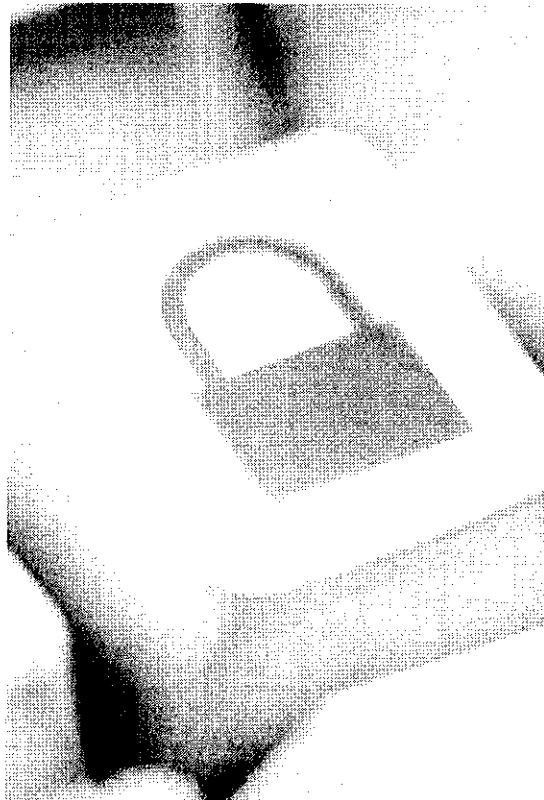
This investment is part of *Budget 2010: Leading the Way on Jobs and Growth*, which allocated \$90 million over five years, and \$18 million in ongoing funding, towards the Cyber Security Strategy.

Internet crime or cyber crime has been identified by the members of Canadian Association of Police Boards as an important issue; in fact CAPB has approved resolutions on this topic at the 1996, 1997, 2001, 2005 and 2006 Annual General Meetings.



Government
of Canada

Gouvernement
du Canada

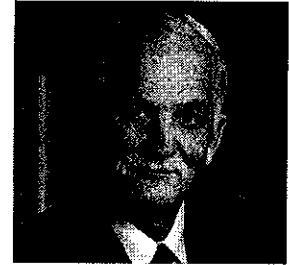


Canada's Cyber Security Strategy

FOR A STRONGER AND MORE PROSPEROUS CANADA

Canada

Message from the Minister



Canadians' personal and professional lives have gone digital: we live, work, and play in cyberspace. Canadians use the Internet, computers, cell phones and mobile devices every day to talk, email, text and twitter with family, friends and colleagues. We do business online everyday, from banking to shopping to accessing government services – and we do it from wherever we happen to be. Digital infrastructure makes all this possible, and also keeps essential services up and running.

Canadians – individuals, industry and governments – are embracing the many advantages that cyberspace offers, and our economy and quality of life are the better for it. But our increasing reliance on cyber technologies makes us more vulnerable to those who attack our digital infrastructure to undermine our national security, economic prosperity, and way of life.

Our systems are an attractive target for foreign military and intelligence services, criminals and terrorist networks. These groups are breaking into our computer systems, searching through our files, and causing our systems to crash. They are stealing our industrial and national security secrets, and our personal identities.

We don't see them, we don't hear them, and we don't always catch them. At times they are mere nuisances. At other times, they present real threats to our families, companies and to our country.

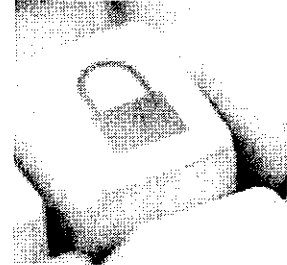
Canada's Cyber Security Strategy is our plan for meeting the cyber threat. It delivers on the Government's 2010 Speech from the Throne commitment to work with provinces, territories and the private sector to implement a cyber security strategy to protect our digital infrastructure. It leverages the partnerships being established under the *National Strategy and Action Plan for Critical Infrastructure*, and supports the ongoing efforts by our law enforcement community to work with partners and international allies in cracking down on those who use the Internet for crime and illegal activities.

Canada's Cyber Security Strategy is a cornerstone of our Government's commitment to keep Canada – including our cyberspace – safe, secure and prosperous.

A handwritten signature in black ink that reads "Vic Toews". The signature is written in a cursive, flowing style.

The Honourable Vic Toews, P.C., Q.C., M.P.
Minister of Public Safety

Introduction



Cyberspace is the electronic world created by interconnected networks of information technology and the information on those networks. It is a global commons where more than 1.7 billion people are linked together to exchange ideas, services and friendship.

The Canadian economy relies heavily on the Internet:

- Canadian online sales in 2007 were estimated at \$62.7 billion,¹ and
- In 2007, 87% of Canadian businesses used the Internet.²

Canadian businesses are moving quickly to adopt the most modern digital applications, including next generation and mobile technologies.

Canada's governments have also become increasingly dependent on the Internet. The federal Government alone now offers more than 130 commonly used services online, including tax returns, employment insurance forms and student loan applications.

Our success in cyberspace is one of our greatest national assets. Protecting this success means protecting our cyber systems against malicious misuse and other destructive attacks. This is a daunting challenge. There is no simple way

Canadians are embracing cyberspace:

- 74% of Canadian households had paid Internet service in 2008;³
- 59% of personal tax filings were electronic in 2008;⁴
- 67% of Canadians banked online in 2009.⁴

¹ Statistics Canada, "The Daily," April 24, 2008

² Canadian Radio-television and Telecommunications Commission, "Communications Monitoring Report," August 2009

³ Canada Revenue Agency, "National Processing Status Report," September 2009

⁴ Statistics Canada, "Canadian Internet Use Survey," 2009

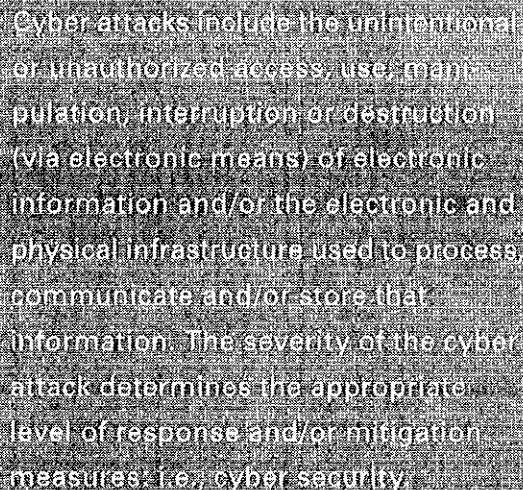
to detect, identify and recover from attackers who cannot be seen or heard, who leave no physical evidence behind them, and who hide their tracks through a complex web of compromised computers.

Cyber security affects us all, in part because even attackers with only basic skills have the potential to cause real harm. Sophisticated attackers can disrupt the electronic controls of our power grids, water treatment plants and telecommunications networks. They interfere with the production and delivery of basic goods and services provided by our governments and the private sector. They undermine our privacy by stealing our personal information. Dealing with cyber threats in isolation is not enough. Through the implementation of this Strategy, the Government will continue to work with the provinces, territories and the private sector in a concerted effort to address the threats facing Canada and Canadians.

Every year, we detect more attackers than the year before. And every year, those seeking to infiltrate, exploit or attack our cyber systems are more sophisticated and better resourced than the year before. They are investing in their capabilities. We must respond by investing more in ours.

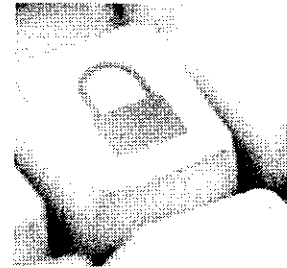
The Government is continuing its efforts to help secure Canada's cyber systems and protect Canadians online. Indeed this Strategy is but one element in a series of initiatives designed to protect Canadians. The Government has established the Canadian Cyber Incident Response Centre to monitor and provide mitigation advice on cyber threats, and coordinate the national response to any cyber security incident. The Government will soon introduce legislation to modernize law enforcement's investigative powers, and ensure that technological innovations are not used to evade lawful interceptions of communications supporting criminal activity.

These are important initiatives, but they are no longer sufficient. The threat is becoming more serious. We cannot allow our cyber security efforts to remain fixed on the threat as we understood it in the past. To ensure that our advanced use of cyberspace remains a strategic asset, Canada must anticipate and confront emerging cyber threats. *Canada's Cyber Security Strategy* is our plan for making cyberspace more secure for all Canadians.



Cyber attacks include the unintentional or unauthorized access, use, manipulation, interruption or destruction (via electronic means) of electronic information and/or the electronic and physical infrastructure used to process, communicate and/or store that information. The severity of the cyber attack determines the appropriate level of response and/or mitigation measures: i.e. cyber security.

Understanding Cyber Threats



There are various ways to gain access to information in cyberspace. Attackers can exploit vulnerabilities in software and hardware. They can exploit security vulnerabilities by tricking people into opening infected emails or visiting corrupted websites that infect their computers with malicious software. They can take advantage of people who fail to follow basic cyber security practices, such as changing their passwords frequently, updating their antivirus protection on a regular basis, and using only protected wireless networks.

Once they have access to a computer, attackers can steal or distort the information stored on it, corrupt its operations and program it to attack other computers and the systems to which they are connected. In many cases, victims suffer a theft of their identity and/or their personal assets. According to a study by McMaster University,⁵ 1.7 million Canadians were victims of identity theft in 2008. The annual cost of identity theft in Canada has been estimated at nearly \$1.9 billion. For this reason the Government has amended the *Criminal Code* to better protect Canadians from identity theft.

Canadian companies can lose the race to bring a product to market, or experience other harm without ever realizing that their losses were caused by a cyber attack. It has been estimated that in a recent one year period, 86% of large

Canadian organizations had suffered a cyber attack. The loss of intellectual property as a result of these attacks doubled between 2006 and 2008.⁶

Though certain attack tools and techniques are more costly and sophisticated than others, most cyber attacks share four characteristics that, in part, account for their growing popularity. Cyber attacks are often:

- **Inexpensive** – Many attack tools can be purchased for a modest price or downloaded for free from the Internet;
- **Easy** – Attackers with only basic skills can cause significant damage;

⁵ McMaster University, *Measuring Identity Theft in Canada: 2008 Consumer Survey*

⁶ CA Technologies, "Canada 2008 Security and Privacy Survey"

- **Effective** – Even minor attacks can cause extensive damage; and
- **Low risk** – Attackers can evade detection and prosecution by hiding their tracks through a complex web of computers and exploiting gaps in domestic and international legal regimes.

While there is some similarity in the targets and methods of cyber attackers, the nature of the threat posed by each is made distinct by their differing motivations and intentions. Three types of threats are discussed below.

STATE SPONSORED CYBER ESPIONAGE AND MILITARY ACTIVITIES

The most sophisticated cyber threats come from the intelligence and military services of foreign states. In most cases, these attackers are well resourced, patient and persistent. Their purpose is to gain political, economic, commercial or military advantage.

All technologically advanced governments and private businesses are vulnerable to state sponsored cyber espionage. Reports from Canada and across the world confirm that these attacks have succeeded in stealing industrial and state secrets, private data and other valuable information.

Some foreign states have declared publicly that cyber attacks are a central element of their military strategy. Some states have been widely accused of using cyber attacks to coincide with – and magnify the effects of – traditional military operations. These cyber attack programs are typically designed to sabotage an adversary's infrastructure and communications. They may also support electronic attacks on an adversary's military equipment and operations. Cyber attacks that disrupt emergency response and public health systems would put lives in danger.

Canada and our allies understand that addressing these risks requires modernizing our military doctrines. It is for this reason that the North Atlantic Treaty Organization (NATO) has adopted several policy documents regarding cyber defence, and like the militaries of our closest allies, the Department of National Defence and the Canadian Forces are examining how Canada can best respond to future cyber attacks.

TERRORIST USE OF THE INTERNET

Terrorist networks also are moving to incorporate cyber operations into their strategic doctrines. Among many activities, they are using the Internet to support their recruitment, fundraising and propaganda activities.

Terrorists are aware of the potential for using the Western world's dependence on cyber systems as a vulnerability to be exploited. For example, there are now online resources providing advice to terrorists on how to defend their own websites while launching cyber attacks on their enemies. In addition, a number of terrorist groups, including Al-Qaeda, have expressed their intention to launch cyber attacks against Western states. Though experts doubt that terrorists currently have the ability to cause serious damage via cyber attacks, they recognize that this capacity will likely develop over time.

CYBERCRIME

In much the same way as states have expanded their operations into cyberspace, so too have organized criminals. The more sophisticated among them are turning to skilled cyber attackers to pursue many of their traditional activities, such as identity theft, money laundering and extortion.

Criminals now sell information stolen online, such as credit and debit card numbers, login passwords for computer servers, and malicious software designed to infiltrate and damage targeted systems. Even those of us who are diligent in protecting our personal information online are at risk of having our personal data stolen from the third parties we share it with.

Some criminal organizations are now developing customized attack software. They are using advanced encryption technologies to protect their own assets and trade secrets. Some in the law enforcement and security communities argue that the capabilities of some cyber criminals now rival those of developed states.

THE THREAT IS EVOLVING

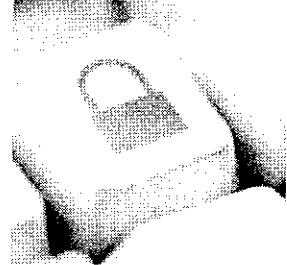
Much like bacteria developing drug resistance to antibiotics, cyber viruses and malicious code are continually evolving to evade our defences and antivirus software. The evolution of cyber attack tools and techniques has accelerated dangerously in the recent past. Statistics compiled by two well known Internet security companies, Akamai and Symantec, together show that malicious computer programs now originate in more than 190 countries.⁷ More than 60% of all the malicious code ever detected was introduced into cyberspace in 2008⁸ alone.

There is no doubt that the frequency and severity of the cyber threat is accelerating. Protecting Canadians in cyberspace will be a constantly evolving challenge. To effectively address this challenge will require a range of actions and responses, accompanied by continuing investment and vigilance over the long term.

⁷ Akamai, "State of the Internet Report," March 2009

⁸ Symantec, "Global Internet Security Threat Report," April 2009

Canada's Cyber Security Strategy



Canadian researchers have been at the forefront of making cyberspace a reality. This same ingenuity must continue to be applied to predicting, detecting and defeating the cyber threats of tomorrow, and exploiting cyberspace to further Canada's national interests.

Canada's Cyber Security Strategy is our plan for meeting the cyber threat. The Strategy is built on three pillars:

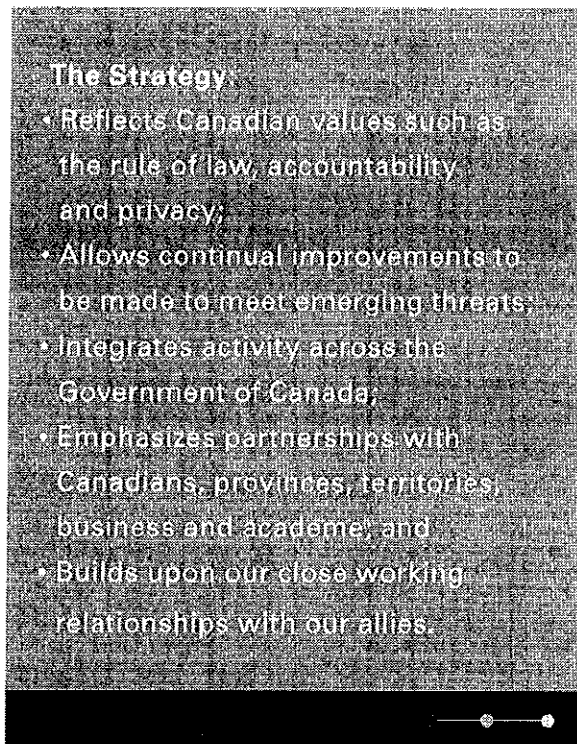
- 1. Securing Government systems** – Canadians trust Government with their personal and corporate information, and also trust Government to deliver services to them. They also trust that the Government will act to defend Canada's cyber sovereignty and protect and advance our national security and economic interests. The Government will put in place the necessary structures, tools and personnel to meet its obligations for cyber security.
- 2. Partnering to secure vital cyber systems outside the federal Government** – Canada's economic prosperity and Canadians' security depend on the smooth functioning of systems outside the Government. In cooperation with provincial and territorial governments and the private sector, the Government will support initiatives and take steps to strengthen Canada's cyber resiliency, including that of its critical infrastructure sectors.

3. Helping Canadians to be secure online –

The Government will assist Canadians in getting the information they need to protect themselves and their families online, and strengthen the ability of law enforcement agencies to combat cybercrime.

Canada's Cyber Security Strategy will strengthen our cyber systems and critical infrastructure sectors, support economic growth and protect Canadians as they connect to each other and to the world. We all have a role to play as we take full advantage of cyberspace to build a safe, resilient and innovative Canada.

The Government has sought input from stakeholders on a wide range of cyber threats and security practices. Collaboration, especially internationally, is essential if cyberspace is to be secured. Canada will benefit from being seen internationally and domestically as a trusted partner in making cyberspace safer.



Three of our closest security and intelligence partners, the United States, the United Kingdom and Australia, recently released their own plans to secure cyberspace. Many of the guiding principles and operational priorities set out in those reports resemble our own. This complementarity reflects our shared experiences in dealing with cyber security, and demonstrates our determination to enhance our collective security by leveraging each ally's domestic cyber regimes. Like Canada, our allies intend to review and update their plans regularly in response to evolution in cyber security technologies and practices, and the cyber threat environment.

Canada will also build on its existing engagement in cyber security discussions at key international fora, such as the United Nations, NATO and the Group of Eight. We are one of the non-European states that have signed the Council of Europe's *Convention on Cybercrime*, and the Government is preparing legislation to permit ratification of this treaty.

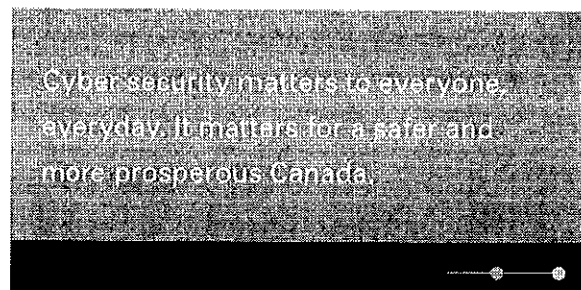
Canada supports international efforts to develop and implement a global cyber governance regime that will enhance our security. To the extent possible, Canada will support efforts to build the cyber security capacity of less developed states and foreign partners. This will help forestall adversaries from exploiting weak links in global cyber defences.

WORKING COOPERATIVELY

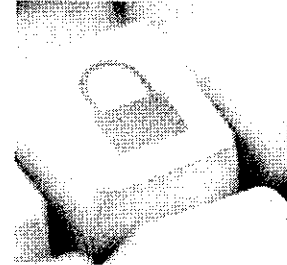
The Strategy will be implemented by the departments and agencies most directly responsible for securing the Government's cyber systems. We will work with our provincial and territorial partners, as they are jointly responsible for protecting much of the critical infrastructure in Canada.

Canada's academic community, non-governmental organizations and private sector must join the Government in securing Canada's cyber systems. Each of these communities has unique technological and analytical capabilities to offer, and a strong incentive to secure their own systems. Their collaboration is essential to our shared success to secure Canada and increase our productivity and prosperity.

Individual Canadians must also play a primary role in securing Canada's cyber future. The Government can introduce and support important cyber security initiatives, but it cannot protect each of us from every threat we encounter when we go online. Canadians must become aware of these threats, and of the tools available to recognize and avoid them. Most importantly, they must use these tools to protect themselves and their families.



Specific Initiatives



Canada's Cyber Security Strategy is built on three pillars:

- Securing Government systems;
- Partnering to secure vital cyber systems outside the federal Government; and
- Helping Canadians to be secure online.

SECURING GOVERNMENT SYSTEMS

The cyber world in which Canadians live, work and play lacks the regimes of law and order that govern our physical world. The Government is entrusted with safeguarding some of our most personal and sensitive information in its electronic databases. It provides services to Canadians and the private sector through its websites and electronic processing systems. And the Government transmits highly classified information essential to our military and national security operations via its classified communications systems.

There have been many cyber attacks directed at Government systems. Cyber attackers regularly probe these systems, looking for vulnerabilities. Securing these links is not simply a matter of operational efficiency. It is a matter of national security and sovereignty, protecting the lives of our foreign service, military and law enforcement personnel, the integrity of our economy, and safeguarding the personal information of Canadians.

We must and will strengthen the Government's capability to detect, deter and defend against cyber attacks while deploying cyber technology to advance Canada's economic and national security interests. Achieving the cyber integrity of Government requires that roles and responsibilities are clear, systems are strengthened and Government employees are aware of proper procedure.

Establishing Clear Federal Roles and Responsibilities

With a subject as critical as cyber security, there is no room for ambiguity in terms of who does what. This Strategy sets out the required clarity.

Public Safety Canada will coordinate implementation of the Strategy. It will design a whole-of-Government approach to reporting on the implementation of the Strategy. It will provide central coordination for assessing emerging complex

threats and developing and promoting comprehensive, coordinated approaches to address risks within the Government and across Canada. Within Public Safety Canada, the Canadian Cyber Incident Response Centre will continue to be the focal point for monitoring and providing advice on mitigating cyber threats, and directing the national response to any cyber security incident. Public Safety Canada will also lead public awareness and outreach activities to inform Canadians of the potential risks they face and the actions they can take to protect themselves and their families in cyberspace.

The Communications Security Establishment Canada has internationally recognized expertise in dealing with cyber threats and attacks. With its unique mandate and knowledge, the Communications Security Establishment Canada will enhance its capacity to detect and discover threats, provide foreign intelligence and cyber security services, and respond to cyber threats and attacks against Government networks and information technology systems.

The Canadian Security Intelligence Service will analyze and investigate domestic and international threats to the security of Canada. The Royal Canadian Mounted Police will investigate, as per the *Royal Canadian Mounted Police Act*, suspected domestic and international criminal acts against Canadian networks and critical information infrastructure.

The Treasury Board Secretariat will support and strengthen cyber incident management capabilities across Government, through the development of policies, standards and assessment tools. The Treasury Board Secretariat is also responsible for information technology security in the Government of Canada.

Foreign Affairs and International Trade Canada will advise on the international dimension of cyber security and work to develop a cyber security foreign policy that will help strengthen coherence in the Government's engagement abroad on cyber security.

The Department of National Defence and the Canadian Forces will strengthen their capacity to defend their own networks, will work with other Government departments to identify threats and possible responses, and will continue to exchange information about cyber best practices with allied militaries. The Department of National Defence and the Canadian Forces will also work with allies to develop the policy and legal framework for military aspects of cyber security, complementing international outreach efforts of Foreign Affairs and International Trade Canada.

Given the speed and complexity of many cyber attacks, barriers to cooperation and information sharing between federal partners must be eliminated. The Strategy includes measures to address this need, and provides the additional financial and personnel resources required to allow the Government to fulfill its cyber security obligations.

Strengthening the Security of Federal Cyber Systems

For each new technology or practice adopted to enhance our cyber security, another is developed to circumvent it. We will continually invest in the expertise, systems and governing frameworks required to keep pace with these evolving threats. We will also review our options for increasing the risks and consequences applied to those who attack our cyber systems.

The Government will enhance the security of its cyber architecture. It will continue to reduce the number of Internet gateways into its computer systems, and take other measures to secure systems.

In 2009 the Government made a number of important amendments to its *Policy on Government Security*. Administered by the Treasury Board Secretariat, the Policy sets out safeguards to assure the delivery of Government services to Canadians. Since the Government relies extensively on information technology to provide these services, the Policy emphasizes the need for departments and agencies to monitor and secure their electronic operations.

The globalization of the technology industry makes it difficult to assess suppliers' trustworthiness. Cyber attackers are well aware of the opportunities created for them by security gaps in the global supply chain. Some organized crime syndicates and foreign intelligence services have already exploited these vulnerabilities in an effort to disseminate exploitable technologies. The Government will strengthen processes to reduce the risk related to compromised technologies.

Enhancing Cyber Security Awareness throughout Government

While clear roles and responsibilities, and strengthened systems are important to achieving cyber security, the Government's success in securing its systems is largely dependent on its employees. As countless incidents in all segments of society have shown, even the most sophisticated security systems can be undermined by simple human error. In Government, as elsewhere, people can fail to follow basic cyber security practices by:

- Not changing their passwords on a regular basis;
- Assuming that an office email system is more secure than it is; and
- Importing malicious viruses into workplace computers by visiting corrupted websites.

PARTNERING TO SECURE VITAL CYBER SYSTEMS OUTSIDE THE FEDERAL GOVERNMENT

The economic success of Canada's private sector depends in large measure on its ability to secure cutting edge research and intellectual property, business transactions and financial data. Failing to secure these assets inevitably leads to lost market share, fewer customers and corporate breakdown.

In much the same way, our personal wellbeing depends on access to secure and reliable services from our transportation systems, communication networks and financial institutions. It is increasingly important to protect two of the primary contributors to our quality of life – private companies that drive

our economic prosperity and the infrastructure systems that support our daily activities – against cyber threats. Failure to do so will have adverse economic impacts and undermine consumer confidence.

A 2008 study by McMaster University⁹ on identity theft in Canada found that 20% of consumers have eliminated or reduced the amount of shopping they do online, and that 9% have eliminated or reduced online banking activities due to the risks they perceive in doing business online. By building a secure and trusted business environment, we will help foster the productivity and innovation that drive our economic prosperity.

The public needs to be more aware of the vulnerabilities inherent in the cyber systems that these industries use to deliver their services. Increased awareness will equip Canadians to avoid identity theft and potential financial loss. The Government will partner with the provinces, territories and private sector to improve the cyber security posture of Canada and Canadians.

The Government will build on existing programs and expertise, such as Defence Research and Development Canada's Public Security Technical Program to better support cyber security research and development activities. We will also collaborate with our private sector and academic partners to enhance information sharing activities.

Partnering with the Provinces and Territories

Strengthened partnerships among all levels of government are an essential component in delivering a comprehensive cyber security strategy for Canada and Canadians. Our provincial and territorial counterparts provide a range of essential services whose delivery is dependent on the safe and secure operation of their cyber systems. For example, they hold sensitive personal information in their electronic databases, including health records, marriage and driver licenses, and provincial tax return information. The provinces

⁹ McMaster University, *Measuring Identity Theft in Canada: 2008 Consumer Survey*

and territories have a key role to play in promoting awareness among Canadians, especially young Canadians in the education system where first exposure to the Internet often occurs. Only when all levels of government are working together can Canadians be assured that their private information is secure and the services that they depend on will be delivered.

Partnering with the Private Sector and Critical Infrastructure Sectors

Many of the risks and impacts of cyber attacks are shared between the Government and private sector. For example, untrustworthy technology is harmful to both government and industry. Identifying these risks must be done in partnership.

Fortunately, Canada's public and private sectors share a long history of working together to achieve shared economic and national security goals. This cooperation needs to be further strengthened. Each partner must share accurate and timely cyber security information regarding existing and emerging threats, defensive techniques and other best practices.

Strengthened public/private partnerships will be fostered through existing structures and organizations, such as critical infrastructure sector networks. Cross sector mechanisms will also be established, providing opportunities for governments and industry to collaborate on a broad range of critical infrastructure issues, including cyber security.

Another key area for collaboration is the security of process control systems. These systems control everything from our machines and factories to our critical infrastructures. They keep our dams from overflowing, our electrical grids from collapsing and our transportation networks from malfunctioning. Their security is critical to the safe delivery of the services and products upon which Canadians depend. Joint public/private sector initiatives will be struck to identify and share best practices for addressing threats to these systems.

Our collective cyber security efforts will be further refined through training and exercise programs. The result of these exercises, some of which are already underway, will be an improved understanding of the dynamic among partners

in cyber security. Participation in these exercises will also support the improvement of procedures to prevent cyber security failures.

The disruption of critical infrastructure and cyber systems can have direct impacts on businesses and communities on both sides of the Canada–United States border. Attacks on interconnected cyber networks can have cascading effects across industrial sectors and national borders. For this reason, Canada will be active in international fora dealing with critical infrastructure protection and cyber security.

HELPING CANADIANS TO BE SECURE ONLINE

Our success in harnessing cyberspace has helped us achieve unprecedented personal productivity and prosperity. But it has also allowed the world's criminals to commit traditional crimes with 21st century technologies. The Government is taking steps to protect cyberspace from becoming a criminal haven. We will deny cyber criminals the anonymity they are seeking while at the same time protecting the privacy of Canadians.

Combatting Cybercrime

Criminals are learning quickly that cybercrime can be inexpensive, low risk and profitable. In one well known incident uncovered in 2007,¹⁰ over 45 million customer records were stolen from a well known North American retailer. The breach occurred over a three year period, during which criminals monitored wireless signals from point of sale credit card terminals. These attacks cost the retailer over \$130 million and inflicted unknown financial harm on individual victims.

Also in 2008, 11 people operating in five different countries were charged¹¹ with breaking into the databases of nine major North American retailers, stealing some 40 million credit and debit card numbers from their databases, and selling the numbers (via the Internet) to other criminals.

¹⁰ *SC Magazine*, "FTC Settles with TJX Over Breach," March 2008

¹¹ *Wired Magazine*, "Feds Charge 11 in Breaches at TJ Maxx, OfficeMax, DSW, Others," August 2008

Canada's law enforcement agencies cannot combat transnational cybercrimes with outdated investigative powers and tools. Equipping our police to protect us in cyberspace requires that we provide them with new legislative authorities and supporting financial resources.

Accordingly, the Royal Canadian Mounted Police will be given the resources required to establish a centralized Integrated Cyber Crime Fusion Centre. This team will increase the ability of the Royal Canadian Mounted Police to respond, using a risk-based analysis approach, to requests from the Canadian Cyber Incident Response Centre regarding cyber attacks against Government or Canada's critical infrastructure.

The Government has already passed legislation to combat identity theft. Other legislative reforms will be re-introduced by the Government to enhance the capacity of law enforcement to investigate and prosecute cybercrime by:

- Making it a crime to use a computer system to sexually exploit a child;
- Requiring Internet service providers to maintain intercept capable systems, so that law enforcement agencies can execute judicially authorized interceptions;
- Requiring Internet service providers to provide police with basic customer identification data, as this information is essential to combatting online crimes that occur in real time, such as child sexual abuse; and
- Increasing the assistance that Canada provides to its treaty partners in fighting serious crimes.

Protecting Canadians Online

Canadian families want their privacy, identities and physical wellbeing protected from cyber predators. And Canadians know that risks exist. According to a Decima Research study:¹²

- Only 35% of Canadians believe their computer is very safe against online threats; and

- 77% are concerned about the security of personal information. Yet 63% use the Internet for sensitive transactions and 57% keep sensitive information on their computers.

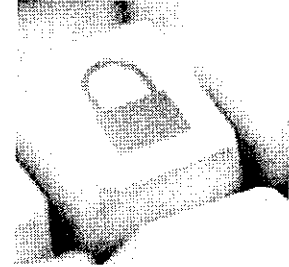
As long as they know how to do so, Canadians will strengthen their own individual cyber security and that of Canada as a whole. We all need to follow basic cyber security practices, such as changing our passwords frequently, updating antivirus protection and using only protected wireless networks.

The Government will increase Canadians' awareness of common online crimes and will promote safe cyber security practices through the use of web sites, creative materials and outreach efforts.

The Government's ultimate goal is to create a culture of cyber safety whereby Canadians are aware of both the threats and the measures they can take to ensure the safe use of cyberspace. Creating such awareness will require a sustained effort over a period of several years. The effort must start now.

¹² Decima Research, *Cyber Security Practices in Canada*, Final Report, February 2008

Moving Forward



With each passing day, Canadians' dependence on cyberspace grows. There is no turning back to a world without an Internet. Just as previous generations took advantage of increasingly complex and helpful methods of communications, we have embraced the Internet.

But as we enjoy the benefits of cyberspace, we also recognize that it threatens us in a variety of ways. Those who choose to abuse the Internet are becoming more sophisticated and dangerous every day. We must invest now in cyber security to protect our economic prosperity, national security and quality of life.

Canada's Cyber Security Strategy is Canada's plan for securing our cyber systems. The Strategy will protect the integrity of Government systems and our nation's critical assets. It will combat cybercrime and protect Canadians as they use cyberspace in their daily lives. By promoting awareness of the need for cyber security, the Strategy will encourage individual Canadians, industry and all levels of government to adapt behaviour and adopt the technology required to confront evolving cyber threats.

The Government will begin implementing new initiatives under the Strategy in 2010. The initiatives outlined in this Strategy are important first steps. They will be adjusted and strengthened as required.

Cyber security is a shared responsibility, one in which Canadians, their governments, the private sector and our international partners all have a role to play. The Strategy reflects this shared responsibility. Implementation will be a collective effort. Its success will depend on our ability to work together.

Everyone must do their part.



155 King William Street, Box 1060, LCD 1, Hamilton, Ontario L8N 4C1 Telephone: 905.546.4925 Fax: 905.546.3892

8.(e)

U N I T Y T H R O U G H H A R M O N Y

RECEIVED

Sept 14, 2010

OCT 08 2010

Dear A/Staff Sgt.S. Hahn:

CHIEF'S OFFICE
HAMILTON POLICE SERVICE

On behalf of the Hamilton Police Female choir, I would like to thank you for your donation of prizes for our 1st Annual Golf Tournament Fundraiser. Your generous support has helped with the choir's operating costs as well as subsidize our annual trip to the National Police Memorial in Ottawa.

The Hamilton Police Female Choir is committed to interacting with and performing for groups that serve women, children and families in our community, through the help of supporters like you.

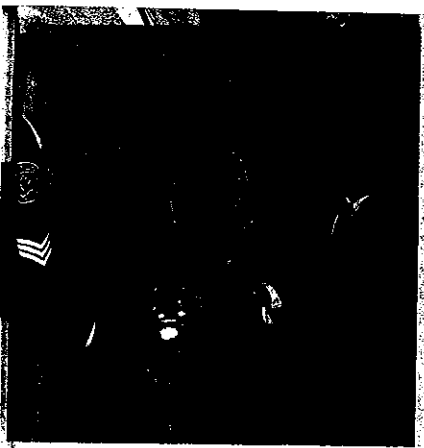
Thank you again for your commitment to the Choir.

Sincerely,

Kelly Greve
President
Hamilton Police Female Choir
"Unity through Harmony"

PSB-Info. (Oct) me





COPS, CATS AND CARING STUDENTS

2010 marked the second year St. Joseph's Healthcare Foundation received funds from the growing Cops, Cats and Caring Students program. **Between March 2 and April 23**, members of the Hamilton Police Service, Hamilton Ti-Cat players and students from across the city played 16 basketball games – raising funds for healthcare in the community. St. Joseph's Healthcare Hamilton received a very generous \$10,000.

The Future of Hope

Thank you for attending
our Traveling Day
events and your kind
words.

It was a huge success.

We raised \$9500.00 for
the Allan's Angels
Camp.

Sincerely
Margaret Davies

Bew McCraw


PS
for
DJ