Fall 2012

Report of the Auditor General of Canada to the House of Commons

CHAPTER 3

Protecting Canadian Critical Infrastructure Against Cyber Threats

OAG

Office of the Auditor General of Canada

The Report is available on our website at www.oag-bvg.gc.ca.

For copies of the Report or other Office of the Auditor General publications, contact

Office of the Auditor General of Canada
Distribution Centre
240 Sparks Street
Ottawa, Ontario
K1A 0G6

Telephone: 613-952-0213, ext. 5000, or 1-888-761-5953
Fax: 613-943-5485
Hearing impaired only TTY: 613-954-8042
Email: distribution@oag-bvg.gc.ca

Ce document est également publié en français.

Cat. No. FA1-2012/2-3E-PDF
ISBN 978-1-100-21243-2
ISSN 1701-5413

CHAPTER 3

Protecting Canadian Critical Infrastructure Against Cyber Threats

Performance audit reports

This report presents the results of a performance audit conducted by the Office of the Auditor General of Canada under the authority of the *Auditor General Act*.

A performance audit is an independent, objective, and systematic assessment of how well government is managing its activities, responsibilities, and resources. Audit topics are selected based on their significance. While the Office may comment on policy implementation in a performance audit, it does not comment on the merits of a policy.

Performance audits are planned, performed, and reported in accordance with professional auditing standards and Office policies. They are conducted by qualified auditors who

- establish audit objectives and criteria for the assessment of performance;
- gather the evidence necessary to assess performance against the criteria;
- report both positive and negative findings;
- conclude against the established audit objectives; and
- make recommendations for improvement when there are significant differences between criteria and assessed performance.

Performance audits contribute to a public service that is ethical and effective and a government that is accountable to Parliament and Canadians.

Table of Contents

Protecting Canadian Critical Infrastructure Against Cyber Threats

Main Points

What we examined

Critical infrastructure consists of physical and information technology assets, such as the electricity distribution networks, telecommunications networks, banking systems, manufacturing and transportation systems, as well as government information systems and services that support the continued and effective functioning of government. Elements of critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories, and international borders. Most of Canada's critical infrastructure is owned by the private sector or by municipal, provincial, or territorial governments, and much of it is connected to other systems.

Cyber threats to Canada's critical infrastructure refer to the risk of an electronic attack through the Internet. Such attacks can result in the unauthorized use, interruption, or destruction of electronic information or of the electronic and physical infrastructure used to process, communicate, or store that information.

Our audit examined whether selected federal departments and agencies are working with the provinces and territories and the private sector to protect Canada's critical infrastructure against cyber threats. This included examining leadership roles and responsibilities for securing key government information systems.

Audit work for this chapter was completed on 17 July 2012. More details on the conduct of the audit are in **About the Audit** at the end of this chapter.

Why it's important

Canada's public and private sectors depend on a secure, robust, and stable information infrastructure to conduct day-to-day operations. Computer-based systems, together with their Internet and network connections, form the backbone for much of Canada's critical infrastructure, including the energy, finance, telecommunications, and manufacturing sectors as well as government information systems. The smooth operation of critical infrastructure supports our way of life and Canada's economic, political, and social well-being.

Attacks on aspects of critical infrastructure of many nations, including Canada, have been reported. The government has stated that the frequency and severity of cyber threats are accelerating and it considers that protecting Canadians in cyberspace will be a constantly evolving challenge. The government has concerns that the cyber threat environment is evolving more rapidly than the government's ability to keep pace.

What we found

- Between 2001 and 2009, the government made limited progress in its efforts to lead and coordinate the protection of Canada's critical infrastructure from cyber threats as these threats were rapidly evolving. During this time, the government released several strategies and policies with recurring commitments and funding.
- Since 2010, with the announcement of the Cyber Security Strategy and of the National strategy and action plan for critical infrastructure, the government has made progress in securing its systems against cyber threats, in improving communications, and in building partnerships with owners and operators of critical infrastructure.
- Eleven years after the government said it would establish partnerships with other levels of government and with critical infrastructure owners and operators to help protect Canada's critical infrastructure, not all of the sector networks that facilitate these partnerships are fully established, and coverage is incomplete. This lack of progress limits Public Safety Canada's ability to communicate with critical infrastructure owners and operators.
- Seven years after the Canadian Cyber Incident Response Centre (CCIRC) was created to collect, analyze, and share cyber threat information among federal departments, provincial and territorial governments, and the private sector, many stakeholders are still unclear about the Centre's role and mandate. As a result, the CCIRC cannot fully monitor Canada's cyber threat environment, which hinders the Centre's ability to provide timely advice on defending against new cyber threats. Furthermore, the Centre is still not operating on a 24-hour-a-day, 7-day-a-week basis, as originally intended. This restriction on operating hours can delay the detection of emerging threats and the sharing of related information among stakeholders.

- The January 2011 intrusion on government systems identified weaknesses in protecting these systems. Incidents were not reported in a timely manner and cyber threat information was not properly shared with appropriate agencies. Also, good information technology (IT) security practices, such as how to store sensitive information, were not consistently followed. Lead security agencies are taking action by updating the government's IT Incident Management Plan to clarify the roles and responsibilities of lead security agencies and to address the need for timely reporting of incidents. The government has allocated more funds to bolster its capacity to detect cyber threats, and is working to increase awareness of best practices for IT security across the government.

The entities have responded. The entities agree with all of the recommendations. Their detailed responses follow the recommendations throughout the chapter.

Introduction

3.1 Canada's critical infrastructure consists of physical and information technology assets, such as the electricity distribution networks, telecommunications networks, banking systems, manufacturing and transportation systems, and government information systems. All of these assets and systems support the safety, security, and economic well-being of Canadians.

3.2 Elements of critical infrastructure are often interconnected and interdependent within and across provincial, territorial, and international borders. Protecting critical infrastructure from cyber threats is a responsibility that is shared among the Government of Canada, the provinces and territories, and the private sector.

3.3 Through the Internet, computer systems that control critical infrastructure can be subjected to a **cyber attack** from anywhere in the world using inexpensive hardware and software. Over time, hackers, criminal organizations, terrorists, and foreign states can quietly and methodically target a critical infrastructure's computer systems, attempt to defeat these systems' defences, and acquire their control. Once they achieve control, intruders can disrupt or destroy the systems or use them for their own purposes, such as stealing information. Attackers may also try to stay undetected within these computer systems for future exploitation.

Cyber attack—[T]he 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.

Source: Government of Canada Cyber Security Strategy

3.4 Critical infrastructures in Canada and in other nations have been the target of cyber-related attacks for criminal, political, or other motives (Exhibit 3.1). Cyber attack tools and techniques have quickly evolved. The federal government has stated that the frequency and severity of cyber threats are growing and that protecting Canadians in cyberspace will be a constantly evolving challenge. Officials told us that the government has concerns that the cyber threat environment is evolving more rapidly than the government's ability to keep pace.

3.5 A cyber assault on key Estonian websites in 2007 illustrates the effects of cyber attacks on critical infrastructure. During a three-week period, websites of government ministries, service providers, banks, and news organizations were the target of a concerted attack that blocked access to users. The denial-of-service attack not only affected large entities, such as banks, media corporations, and government institutions, but also small and medium-sized businesses, all of which experienced disruptions to daily activities.

Exhibit 3.1 US Government Accountability Office audits show that challenges remain in dealing with cyber threats

In 2011 and 2012, the US Government Accountability Office (GAO) reported that protecting the systems supporting the United States' critical infrastructure is a high risk for government. The GAO found that cyber-based threats to critical infrastructure and federal systems were evolving and growing. Over the past six years, the number of incidents reported by federal agencies increased by nearly 680 percent. Recently reported incidents include a sophisticated computer attack targeting a system used to operate industrial processes in critical sectors, including the energy and nuclear sectors, and another attack by hackers to access the personal information of hundreds of thousands of customers of a major bank.

The GAO found that despite recent actions taken, a number of significant challenges remain to enhancing the security of cyber-reliant critical infrastructures, such as strengthening public-private partnerships, particularly for information sharing, and improving the national capability for cyber warning and analysis.

Source: US Government Accountability Office reports

3.6 The Government of Canada plays an important role in protecting the nation's critical infrastructure from all hazards, including cyber threats. As the Prime Minister of the day stated in 2001, "The protection of Canada's critical infrastructure from the risks of failure or disruption is essential to assuring the health, safety, security and economic well-being of Canadians." The Prime Minister announced the creation of the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) to develop and implement a comprehensive approach to protecting Canada's critical infrastructure.

3.7 Since then, Public Safety Canada, which was created in 2003, has assumed the responsibilities of OCIPEP.

Focus of the audit

3.8 In this audit, our objective was to determine whether selected federal departments and agencies are helping to secure Canada's critical infrastructure from cyber threats by leading and coordinating activities in partnership with provinces, territories, and the private sector. We also examined whether leadership roles and responsibilities for securing information systems that are important to the operation of the Government of Canada are clear and are being fulfilled as intended.

3.9 This audit focused on the prevention and preparedness efforts required to protect Canada's critical infrastructure against cyber threats. It did not examine response and recovery activities.

3.10 Legislation and policy require a number of federal departments and agencies to lead and coordinate federal efforts to help secure critical infrastructure and to work with provinces, territories, and

private sector owners of critical infrastructure where necessary. We included the activities of these departments and agencies in the audit:

- Canadian Security Intelligence Service,
- Communications Security Establishment Canada,
- Department of Finance Canada,
- Industry Canada,
- Department of Justice Canada,
- Natural Resources Canada,
- Privy Council Office,
- Public Safety Canada,
- Royal Canadian Mounted Police,
- Shared Services Canada, and
- Treasury Board of Canada Secretariat, including the Chief Information Officer Branch.

3.11 We did not examine matters of provincial or territorial jurisdiction, nor did we examine provincial and territorial or private sector protection efforts for critical infrastructure. We also did not examine any classified systems or new legislative authorities provided to law enforcement agencies to combat cyber crime.

3.12 The audit covered the period between the January 1999 release of The Report of the Special Senate Committee on Security and Intelligence and 31 May 2012. More details on the audit objectives, scope, approach, and criteria are in **About the Audit** at the end of this chapter.

Observations and Recommendations

Protecting critical infrastructure from cyber threats

3.13 In 1996, the federal government acknowledged that systems vital to operating Canada's critical infrastructure could be subject to cyber attacks and that the government had a role to play in protecting these systems from such attacks. In 1999, The Report of the Special Senate Committee on Security and Intelligence recommended that the government take action by reviewing its ability to assess and reduce infrastructure vulnerabilities and to prevent or respond to physical and cyber attacks.

3.14 In 2000, the Government of Canada established the Critical Infrastructure Protection Task Force to advise ministers on the role of

the federal government in protecting Canada's critical infrastructure. The task force found that the limited protection afforded to Canada's critical infrastructure, as well as its electronically interconnected and interdependent nature within and across provincial, territorial, and international borders, required a national strategy to strengthen security.

3.15 The government is well positioned to provide critical infrastructure owners and operators with national and international **situational awareness** of the cyber threat environment because it has access to information sources, such as foreign intelligence sources, that are not available to other stakeholders. It can collect and share cyber threat information in a way that protects the source of the information and it can use established partnerships to inform all stakeholders quickly.

Situational awareness—Insight into one's environment and circumstances to understand how events and actions will affect business objectives, both now and in the near future. It requires understanding the relationships between critical services and information, the safeguards supporting information technology infrastructure and processes, and evolving threats.

3.16 In response to the Critical Infrastructure Protection Task Force's concerns, the Government of Canada created the Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP) in 2001. The mandate of OCIPEP was to develop and implement a comprehensive approach to protecting Canada's critical infrastructure by establishing partnerships and by monitoring and analyzing cyber attacks and threats against federal government systems.

3.17 In December 2003, the government announced that OCIPEP would be integrated into the newly created Public Safety Canada to consolidate emergency response activities and to work with provinces, territories, and the private sector owners and operators of critical infrastructure. Exhibit 3.2 details the timeline of the federal government's commitments to protect Canada's critical infrastructure, including protection from cyber threats.

3.18 In the *Department of Public Safety and Emergency Preparedness Act* (2003), Public Safety Canada is responsible for exercising national leadership on public safety and emergency preparedness. But Public Safety Canada does not direct provinces, territories, critical infrastructure owners, or other federal departments on how to carry out their activities. Based on OCIPEP's mandate, the National Security Policy, the National strategy and action plan for critical infrastructure, and Canada's Cyber Security Strategy, Public Safety Canada is to exercise its leadership and coordination role by providing unique support and services to critical infrastructure owners and operators that otherwise may not be available to them. These include

- building partnerships and providing a forum for advancing the timely sharing of cyber threat information among stakeholders;
- monitoring the international and national cyber threat environment to obtain timely and relevant warnings of cyber

security vulnerabilities and to analyze cyber threats to critical infrastructure stakeholders; and

- building critical infrastructure protection capacity through an enhanced policy framework, education and awareness, and research and development.

Exhibit 3.2 Commitments to protect Canada's critical infrastructure go back more than 11 years

Year	Source	Federal government commitment
2001	OCIPEP mandate	Provide national leadership to help ensure the protection of Canada's critical infrastructure, both its physical and cyber elements, by • building partnerships and promoting dialogue among Canada's critical infrastructure owners and operators; • monitoring critical infrastructure around the clock; • building national capacity; and • securing government systems.
2004	National Security Policy	To ensure that Canada is prepared for and can respond to current and future threats, including reducing Canada's vulnerability to cyber attacks and cyber accidents, the Government of Canada committed to • building partnerships; • working with provinces, territories, and the private sector on national capabilities in critical infrastructure protection; • securing government systems by increasing capacity to predict and prevent cyber attacks against government systems; • modernizing the *Emergency Management Act* to include critical infrastructure protection and cyber security; • developing a critical infrastructure protection strategy; and • developing a national cyber security strategy.
2005	Review of the National Security Policy	The Canadian Cyber Incident Response Centre (CCIRC) was announced with the mandate of • serving as a national focal point for cyber security readiness and response; • dealing with threats and attacks to Canada's cyber critical infrastructure 24 hours a day, 7 days a week; and • building national capacity (by providing standards, best practices, awareness, and education).
2010	National strategy and action plan for critical infrastructure	The strategy's goal is to enhance the resiliency of critical infrastructure in Canada by • building partnerships; and • advancing the timely sharing and protection of information among partners.
2010	Canada's Cyber Security Strategy	Canada plans to meet the cyber threat by • securing government systems; • partnering to secure vital cyber systems outside the federal government; and • helping Canadians to be secure online.

Funding of $780 million was allocated for emergency management and other national security activities, including critical infrastructure protection

3.19 To determine how much funding had been allocated to cyber protection of critical infrastructure activities, we examined government approval documents and identified 13 federal departments and agencies that received funding approval between 2001 and 2011 in support of their activities. We noted that approvals identified four key areas:

- critical infrastructure protection of Government of Canada and private sector systems, and emergency management capacity building;
- addressing security priorities on intelligence and cyber security;
- enhancing cyber protection of Government of Canada information systems; and
- implementing Canada's Cyber Security Strategy.

3.20 We identified about $780 million in funding approvals to these 13 departments and agencies where cyber security for critical infrastructure and government systems was one of the objectives. However, we found that these approvals included several objectives under the broad categories of emergency management and national security. The approved funding requests did not specify amounts for cyber protection activities. We then found that departmental documents supporting the requests for funding also did not specify how much funding was expected to go toward cyber protection activities. Therefore, we were unable to determine how much of the $780 million was specifically allocated to activities for the protection of critical infrastructure from cyber threats. We also identified a further $200 million in ongoing funding where cyber security for critical infrastructure was part of the approval, but we were not able to match funding to cyber protection activities.

3.21 Of the $780 million, we did identify that about $570 million was approved for Communications Security Establishment Canada (CSEC). We were informed by CSEC officials that, in line with the approvals, this funding was provided for more than just cyber protection activities; it also was intended to improve CSEC's overall program capacity, some of which could directly or indirectly support cyber protection of critical infrastructure. We asked officials at Public Safety Canada about funding to the other departments, but found that little information was available to show how much funding was directed by departments for their activities. Nevertheless,

Public Safety Canada officials informed us that about $20.9 million of the remaining $210 million was directed toward cyber protection for critical infrastructure between 2001 and 2011.

Since 2001, missing action plans have hindered progress

3.22 Action plans are important tools to guide the implementation of any initiative. We examined whether the government had action plans to guide its implementation of the commitments to protect Canada's critical infrastructure as outlined in Exhibit 3.2.

3.23 We asked Public Safety Canada for action plans that would provide more information on how funds for cyber security were to have been spent, what they were to achieve, and by when. The Department was not able to provide us with action plans, as none had been developed, with the exception of the National strategy and action plan for critical infrastructure.

3.24 The government has restated in several strategies and policies since 2001 its commitment to protecting Canada's critical infrastructure from cyber threats. However, while we noted that there has been progress in enhancing the policy frameworks, such as developing the Cyber Security Strategy and the National strategy and action plan for critical infrastructure, progress toward building partnerships and monitoring threats has been limited. In our opinion, the lack of action plans since the 2001 commitments for cyber security were announced has contributed to the overall lack of measurable progress. We noted that the 2010 Cyber Security Strategy does not yet have an action plan to guide its implementation. The lack of a plan makes it difficult to determine whether progress is on schedule and whether its objectives have been met.

3.25 **Recommendation.** Public Safety Canada should develop an interdepartmental action plan with deliverables and timelines for Canada's Cyber Security Strategy (2010) to guide the implementation of the strategy and measure progress.

The Department's response. Agreed. Public Safety will release an interdepartmental action plan. This action plan will be based on the implementation plan that was developed prior to the launch of the Cyber Security Strategy in October 2010. Since some of the activities in that plan were of a sensitive nature and dealt with issues related to national security, the plan was not publicly released. Public Safety Canada is currently leading the development of a horizontal performance measurement strategy to measure and report on the progress made against commitments in the implementation plan.

Partnering to protect critical infrastructure

3.26 Most of Canada's critical infrastructure is owned by the private sector or is managed through other levels of government. This mix of ownership and jurisdictions creates challenges in leading and coordinating stakeholders' efforts to protect Canada's critical infrastructure from cyber threats, for a number of reasons:

- Significant numbers of stakeholders are involved. Federal government departments, provinces, territories, the private sector, and international partners all need to agree on how to protect Canada's critical infrastructure.
- Critical infrastructure, such as the electricity distribution network, is geographically dispersed throughout North America, spanning both Canada and the United States, thereby requiring international cooperation.
- In some cases, stakeholders are reluctant to share information that is sensitive or of a competitive nature.

3.27 Through consultations in 2001, the Office of Critical Infrastructure Protection and Emergency Preparedness found that critical infrastructure owners and operators had suggested a collaborative approach for assuring the protection of critical infrastructure. The government therefore determined that building partnerships with all critical infrastructure owners and operators would be the best way to achieve the cooperation needed to coordinate efforts. The government has committed to building partnerships with critical infrastructure owners and operators consistently since then.

3.28 In 2003, as outlined in the National Critical Infrastructure Assurance Program Discussion Paper, the federal government acknowledged that dialogue with critical infrastructure owners and operators was needed to launch effective partnerships. This view was further supported in the 2004 Government of Canada Position Paper on a National Strategy for Critical Infrastructure Protection. Public Safety Canada was tasked with creating the partnerships needed to provide national direction and coordination of critical infrastructure protection.

3.29 Between 2004 and 2008, Public Safety Canada continued its work on developing these partnerships and monitoring the nature and extent of threats to critical infrastructure. In 2008, the Department produced Working Towards a National Strategy and Action Plan for Critical Infrastructure, in which it proposed strengthening the resiliency of Canada's critical infrastructure by creating partnerships with provinces, territories, and private sector owners of critical infrastructure.

3.30 In May 2010, the government released its National strategy and action plan for critical infrastructure. The strategy proposed that partnerships with provinces, territories, and private sector owners and operators be implemented through 10 sector networks. The federal government planned to have these sector networks in place by May 2011.

Building partnerships to protect critical infrastructure has been slow

3.31 We examined the progress the government has made since its initial commitment to build partnerships with the private sector, provinces, and territories.

3.32 At the time of our audit, 11 years after the Government of Canada first committed to using partnerships to strengthen Canada's critical infrastructure protection, we found uneven progress in establishing working sector networks. Based on Public Safety Canada's monitoring, we found that limited progress had been achieved and that the sector networks are at various stages of maturity. All 10 networks have **sector risk profiles** and lead departments identified, but 6 did not include representatives from all the industry groups that Public Safety Canada identified as key stakeholders. We also noted that while most have met, only 5 have included cyber security in their discussions.

Sector risk profile— An overview developed by Public Safety Canada for each sector that contains a list of the sub-sectors that should be included in the sector network.

3.33 Critical infrastructure sector networks are meant to be forums for discussions and information exchanges among sector-specific industry stakeholders and governments. Membership is voluntary. The National strategy and action plan for critical infrastructure explains that these sector networks are expected to identify and address interdependencies within and across sectors and to develop plans and programs that will protect critical infrastructure.

3.34 We found that the energy and utilities sector network, managed through Natural Resources Canada, meets regularly and has active participation from all stakeholders. We reviewed the network's stakeholder survey and found a high degree of satisfaction and commitment among members. In our opinion, this result shows that networks can work and can be a valuable forum for exchanging needed information to protect critical infrastructure.

3.35 We also found that the information and communication technology sector network has been established. This network was to represent several sub-sectors as defined in Public Safety Canada's Sector Risk Profile, which lists which industries should participate.

However, we found that the network includes only the telecommunications providers, which meet regularly. We asked Industry Canada, the lead federal department for the sector, and Public Safety Canada why other groups, such as radio and television broadcasters, global navigation, remote sensing, and identity management, were not included. The departments told us that the decision was taken to focus only on telecommunications and to expand coverage at a later date.

3.36 The government's approach to implementing its Cyber Security Strategy was to use sector networks with critical infrastructure owners and operators to build the partnerships needed to secure systems. However, since sector networks are only now starting to develop and are incomplete in coverage, one of the principal mechanisms for implementing the Cyber Security Strategy has been missing.

3.37 **Recommendation.** Public Safety Canada should ensure that all sector networks are fully established and operating as outlined in the National strategy and action plan for critical infrastructure so that they can be an effective tool in helping to secure critical infrastructure in order to deliver the objectives of Canada's Cyber Security Strategy.

The Department's response. Agreed. The sector networks provide a useful mechanism to deliver the private sector engagement objectives of Canada's Cyber Security Strategy, including sharing information on cyber threats and partnering with critical infrastructure sectors to conduct risk management activities. The Department will continue to work with lead federal departments and agencies to strengthen the sector networks, share information with sector stakeholders, including cyber threat information, and provide tools to support each sector's risk management efforts. Recognizing that each sector is unique and that representation is not expected to be uniform across each of the critical infrastructure sectors, Public Safety Canada will also provide guidance to lead federal departments and agencies on appropriate coverage for sector networks by December 2013.

Recent progress has been made to improve communications

3.38 Since the release of the Cyber Security Strategy and the National strategy and action plan for critical infrastructure, we found that there has been activity toward improving communication among stakeholders. For example:

- The National Cross Sector Forum was created to represent the 10 sector networks and has met twice since December 2010.

- A multi-industry cross sector forum has also met once, in April 2012, as an alternative to the sector networks that are not yet fully functioning.
- The Critical Infrastructure Gateway (a web-based critical infrastructure information-sharing portal) was launched in March 2012 and the Information Sharing Framework (mechanisms and processes to support information sharing among the critical infrastructure community and protect this information from inappropriate disclosure) was approved in December 2011.
- Federal, provincial, and territorial officials have met to discuss cyber issues.
- A memorandum of understanding for sharing cyber security information was signed with the Canadian Electricity Association in March 2012.

Monitoring cyber threats to critical infrastructure

3.39 Constant monitoring of cyber threats is necessary to help stakeholders reduce vulnerabilities and defend their systems. In 2003, the National Critical Infrastructure Assurance Program Discussion Paper proposed that the Government of Canada provide warnings, alerts, advisories, and relevant threat assessments to critical infrastructure owners and operators. Alerts, warnings, and threat assessments from government sources are important because they can provide owners and operators with knowledge and information that may not otherwise be available to them; that information helps them protect their assets from cyber threats.

3.40 In 2005, Public Safety Canada established the Canadian Cyber Incident Response Centre (CCIRC) as Canada's focal point for monitoring and providing advice on mitigating cyber threats. CCIRC is mandated to help owners and operators reduce risks to Canada's critical infrastructure from cyber threats by

- monitoring and analyzing cyber threats 24 hours a day, 7 days a week;
- providing security-related technical advice on information technology;
- providing standards, best practices, awareness, and education; and
- coordinating and supporting the Government of Canada's national response to cyber security incidents.

3.41 CCIRC's role was envisioned as an information hub for collecting relevant information from other federal departments, provincial and territorial governments, the private sector, and

foreign allies. CCIRC analyzes that information and distributes the analyses to stakeholders so they can use the information to better protect and defend their critical infrastructure.

Monitoring the cyber threat environment has not been complete or timely

3.42 We examined whether CCIRC was fulfilling its mandate to maintain situational awareness of the cyber threat environment in Canada. Our recommendation is found in paragraph 52.

3.43 **Hours of operation.** Since its creation, CCIRC has not operated 24 hours a day, 7 days a week to monitor and analyze cyber threats. At the time of the audit, the centre was staffed to operate from 8:00 a.m. to 4:00 p.m. (Ottawa time), five days a week. Cyber threats or attacks being reported to CCIRC after operating hours are received by the Government Operations Centre, which then pages a CCIRC employee who is on call at that time. That employee contacts the Government Operations Centre to determine the nature of the event and decide on the course of action.

3.44 As CCIRC is not operating around the clock, there is a risk that there will be a delay in the sharing of critical information linked to newly discovered vulnerabilities or active cyber events reported to CCIRC after operating hours. A restriction on operating hours means that CCIRC is not able to monitor the cyber threat environment 24 hours a day, as was envisioned in its mandate. Public Safety Canada officials told us that the Department is now working to extend CCIRC's coverage to 7 days a week, from 6:00 a.m. until 9:00 p.m. (Ottawa time), although there are no plans to go to a 24-hour-a-day operation. Based on our discussions with officials, it is our opinion that operating 24 hours a day, 7 days a week is important for the timely detection and notification of cyber threats, and for communicating with the computer emergency response teams of Canada's foreign allies, which operate in different time zones.

3.45 **Timely information sharing.** If infrastructure owners and operators communicate directly with other federal departments and agencies, CCIRC is left out of the discussion. When this happens, information is not always shared with CCIRC in a timely manner, which limits its situational awareness and reduces its ability to share that information as intended. Some private sector critical infrastructure owners and operators that we interviewed told us they were not sure whether cyber events should be reported to the Government of Canada and, if so, to which agency. In some cases, these owners and

operators speak directly with other federal agencies as part of their sector network. Others have said they were not aware of the existence of CCIRC or of the opportunity to share cyber threat information.

3.46 As a result, CCIRC is missing out on timely or complete cyber threat information from critical infrastructure owners and operators—information the centre needs to fully monitor Canada's cyber threat environment. In our opinion, expanded hours of operation to improve access, as well as fully established sector networks, could improve stakeholders' awareness about CCIRC.

3.47 As part of its mandate and under the Cyber Security Strategy, CCIRC was responsible for monitoring the cyber threat environment in Canada, including federal government systems, which allowed CCIRC to add the knowledge gained from its monitoring to its own alerts, warnings, and threat assessments. CCIRC relied on departments and agencies to keep it informed of cyber threats and attacks. This information could then be shared with all critical infrastructure owners and operators.

3.48 We noted that, during an incident where federal government systems were the target of hackers, CCIRC was not notified by the affected departments until more than one week after the intrusion was discovered, contrary to procedure.

3.49 In 2011, CCIRC transferred the responsibility for protecting government information systems to Communications Security Establishment Canada (CSEC). This transfer occurred because CSEC has the technical capacity and supporting mandate to protect government information systems from cyber threats. At the time of the transfer, it was agreed that CSEC would provide CCIRC with timely and complete information about identified threats to government systems. We found that CSEC has not been consistently providing CCIRC with timely and complete information gained from its monitoring of government systems. We asked officials from the two agencies what kept CSEC from sharing this information. CSEC told us it was concerned about sharing information because of the sensitive nature of the information it collects, such as classification levels or the sensitivities of client departments. This issue was to be resolved by the end of August 2011, but had not yet been resolved at the time of the audit. CSEC and CCIRC have agreed to resolve this issue by 30 November 2012 and have placed a CCIRC employee on a trial basis within CSEC to facilitate more frequent and secure information sharing.

3.50 Technical advice. As part of its mandate, CCIRC provides technical advice on defending against new cyber threats by maintaining an up-to-date awareness of the national and international cyber threat environment. This advice aims to help critical infrastructure owners and operators protect their systems from emerging sophisticated cyber threats. However, CCIRC's difficulties in collecting timely and complete cyber threat information reduce its ability to provide such advice promptly.

3.51 Education, awareness, and standards. We found that since its creation in 2005, CCIRC's efforts have been dedicated to analyzing the cyber threat environment and providing alerts and warnings to its stakeholders. It has been progressing slowly in two additional areas of its mandate: providing education and awareness of cyber threats and standards. Now, with the launch of the Cyber Security Strategy in 2010, Public Safety Canada has transferred these responsibilities from CCIRC to another section within its department.

3.52 Recommendation. Public Safety Canada should increase the Canadian Cyber Incident Response Centre's ability to maintain situational awareness of cyber threats to Canada's critical infrastructure and to increase the Centre's ability to communicate this information to critical infrastructure owners and operators.

The Department's response. Agreed. To enhance support for critical infrastructure and other partners, Public Safety Canada is augmenting CCIRC's operational capacity and capabilities, strengthening its policies and processes, and improving its information-sharing partnerships.

In 2012, the government allocated an additional $13 million over five years to extend CCIRC's operational hours to 15 hours a day, 7 days a week. CCIRC's capabilities have been bolstered through the acquisition of a world-class malware analysis laboratory from the Communications Research Centre and the deployment of an industrial control systems test bed.

CCIRC's mandate has been updated to provide greater clarity to internal and external partners. Standard procedures and policies are being updated where necessary to support the expansion of CCIRC's operations, ensuring that CCIRC provides value-added services that are efficient, effective, and consistent.

Finally, CCIRC is improving information sharing with the introduction of the CCIRC Community Portal, a secure environment for collaboration, and the creation of formal information-sharing agreements with partners in the critical infrastructure; the first such agreement has recently been signed. Further, an incident response pilot has been launched with a number of partners, the lessons from which will greatly improve both response capability and cyber security readiness for all partners.

Protecting government information systems

3.53 In the National Security Policy (2004) and Canada's Cyber Security Strategy (2010), the government stated its commitment to better protect its information systems from cyber attacks. These systems include, for example, the networks where the government stores sensitive information during its daily operations and the networks that ensure that paycheques and employment insurance benefits are distributed on time. The security of government systems is necessary for the continued delivery of services upon which Canadians rely and for the continued and effective functioning of government.

3.54 To better protect its systems and improve the timely sharing of cyber threat information between departments, the government set out three objectives:

- strengthen the security of government systems,
- clarify roles and responsibilities for protecting government systems, and
- enhance awareness of information technology (IT) security in government departments.

Government information systems have been vulnerable to intrusion

3.55 We examined the government's progress in meeting these three objectives to protect its information systems, recognizing the rapidly evolving cyber threats. We found that since 2001, there has been limited progress on achieving these objectives, although there has been more progress recently to protect government information systems.

3.56 **System security.** The intrusion into government systems in January 2011 showed existing weaknesses in protecting these systems (Exhibit 3.3). Since that time, the government has taken additional steps to secure its systems. Communications Security Establishment Canada (CSEC) officials told us that the January 2011 incident would not have been detected without the enhancements that CSEC had made to its monitoring and that these enhancements have increased CSEC's success in stopping subsequent attempted attacks.

3.57 In 2010, in support of the Cyber Security Strategy, the government committed $90 million toward achieving the strategy's objectives. It began phasing in this funding over the next five years, to be followed by recurring amounts of $18 million each year. That same year, lead security agencies assessed the security risks to government systems to obtain funding to implement the Cyber Security Strategy.

3.58 The lessons learned exercise that was done after the January 2011 intrusion revealed ongoing vulnerabilities to government systems. As a result, new funding was approved in April 2012 to bolster the capacity of Public Safety Canada, CSEC, the Treasury Board of Canada Secretariat, and Shared Services Canada to detect cyber threats and enhance the government's ability to protect its systems. About $31 million was allocated to these four departments for the 2012–13 fiscal year to provide additional resources to support the implementation of the Cyber Security Strategy.

3.59 **Roles and responsibilities.** The Policy on Government Security states that all deputy heads of federal departments must manage security activities so that information, assets, and services are safeguarded. However, the large number of departments and agencies involved has created challenges in sharing threat information and coordinating actions. Several departments and agencies—called lead

Exhibit 3.3 **Government of Canada information systems were the target of an intrusion**

In January 2011, departments of the federal government were the target of a cyber incident of significant scope. The intrusion was aimed at gaining access to and control of information systems, and extracting sensitive information contained within those systems.

As soon as the intrusion was detected, mitigation measures were taken to prevent any further damage, such as blocking staff access to the Internet. Affected departments deployed resources in response to the intrusion, resulting in several million dollars in IT equipment and urgent IT security enhancements, overtime, and lost productivity. Full employee access to the Internet was restored only in September 2011.

The intrusion also attracted national and international media attention, raising questions about the government's ability to protect sensitive government information.

security agencies—have been tasked under the policy to lead and coordinate activities and deliver services to assist in the shared protection of government systems. Exhibit 3.4 highlights these responsibilities. Under the leadership of the Treasury Board of Canada Secretariat, these responsibilities have been further defined and explained in the government's IT Incident Management Plan.

3.60 We found that the IT Incident Management Plan, which was released in 2009 after the Policy on Government Security was revised, contained aspects that did not comply with the policy. For example, departmental roles as described in the policy were different from the descriptions in the Incident Management Plan. The review of the events in January 2011 noted that because of this confusion, information about the cyber threat had not been shared quickly enough with appropriate departments.

3.61 The IT Incident Management Plan was updated in May 2012. This updated version clarifies roles and responsibilities of lead security agencies and addresses the need for timely reporting of incidents.

Exhibit 3.4 Many lead security agencies are involved in protecting government systems from cyber threats

Agency	Responsibilities
Privy Council Office	Advising and supporting the Prime Minister and Cabinet on national security matters, coordinating the related activities of departments and agencies, and providing government-wide policy direction on national security and intelligence priorities
Treasury Board of Canada Secretariat	Setting government-wide direction, establishing priorities, and defining and formalizing IT security requirements for departments of the Government of Canada
Public Safety Canada	Coordinating activities related to IT incidents affecting the Government of Canada and monitoring IT threats to services to Canadians or government operations
Communications Security Establishment Canada	Leading and coordinating departmental activities to help ensure the protection of IT systems of importance
Public Works and Government Services Canada	Delivering IT security services, such as ensuring the confidentiality, integrity, and availability of common IT services provided to departments
Canadian Security Intelligence Service	Providing intelligence reports and assessments relating to IT security to help ensure the protection of the Government of Canada's critical services and systems
Royal Canadian Mounted Police	Providing services related to law enforcement and investigations including computer forensics and cyber crime

Source: Adapted from the Policy on Government Security, 2009

Treasury Board of Canada Secretariat officials told us that, in their view, this revised plan better reflects more recent practices and structural changes within the government, such as the creation of Shared Services Canada.

3.62 **Awareness of IT security.** Lessons learned from the January 2011 intrusion also showed that sensitive information was being stored on government systems that did not meet appropriate information technology security safeguards. As a result, some of this sensitive information that was not appropriately protected against unauthorized access was vulnerable to compromise. Treasury Board of Canada Secretariat officials told us that a renewed emphasis on increasing awareness of best practices for IT security is now being implemented across the government.

The Policy on Government Security does not reflect current roles and responsibilities for information technology security

3.63 Shared Services Canada (SSC) is a federal department established in August 2011. In a presentation to the Standing Committee on Government Operations and Estimates in December 2011, the Minister responsible said that "Shared Services Canada was established earlier this year to reduce duplication in Government of Canada information technology, or IT, infrastructure services, to modernize the way we deliver services to Canadians, and to improve the security of federal IT infrastructure."

3.64 We examined whether SSC's leadership and coordination roles and responsibilities in protecting the Government of Canada's information technology assets and systems have been defined and implemented.

3.65 SSC provides IT security for email systems, data centres, and electronic networks for 43 departments. As part of the government's revised IT Incident Management Plan, SSC is tasked with IT security roles and responsibilities covering other departments. We found that since SSC was created after the release of the Policy on Government Security, SSC is not referenced as a lead security agency within that policy. The discrepancy between the revised IT Incident Management Plan and the Policy on Government Security could create confusion about the IT security role that SSC is expected to play under the IT Incident Management Plan and other government policies.

3.66 Government officials told us that consolidating the government's IT services under SSC is a unique opportunity to develop a new conceptual design for the implementation of information technology in

the federal government that would embed security at its core. At a meeting of the Standing Committee on Government Operations and Estimates in December 2011, the Minister responsible for SSC said that "The consolidation of services and assets will strengthen our efforts to ensure that government IT infrastructure is reliable and secure." This consolidation aims to improve security by improving control of access. The federal government expects this consolidation to be achieved by 2020.

3.67 Recommendation. Treasury Board of Canada Secretariat, in cooperation with Shared Services Canada, should update relevant policies and plans to reflect the new information technology security roles and responsibilities of Shared Services Canada.

The Department's response. Agreed. Treasury Board Secretariat has revised the Government of Canada (GC) Information Technology (IT) Incident Management Plan, which defines the roles and responsibilities of Shared Services Canada (SSC) with respect to incident management. The GC IT Incident Management Plan was approved by the Chief Information Officer (CIO) of Canada in May 2012. Additionally, the Secretariat is updating the Policy on Government Security to reflect the role of SSC as one of the lead federal IT security agencies and to define its associated IT security roles and responsibilities. The updated policy is expected to be published in 2013.

Conclusion

3.68 Since 2001, the Government of Canada has made commitments to address the cyber threats to Canada's critical infrastructure. Despite several past strategies and funding, we found that progress in achieving these commitments has been slow. Since 2010, with the announcement of Canada's Cyber Security Strategy and of the National strategy and action plan for critical infrastructure, we found that the government has made progress in securing its systems against cyber threats and in improving communications and building some partnerships with owners and operators of critical infrastructure.

3.69 The government determined in 2001 that through partnerships with critical infrastructure owners and operators, it could help to protect Canada's critical infrastructure by sharing information and providing technical support. These partnerships were to be set up by organizing 10 sector networks. However, the government has made little progress in building these partnerships through the use of the sector networks. This lack of progress restricts one of Public Safety Canada's principal

mechanisms for communicating with critical infrastructure owners and operators as outlined in the Cyber Security Strategy.

3.70 The Government of Canada created the Canadian Cyber Incident Response Centre (CCIRC) in 2005 to be the focal point for monitoring systems and providing advice on mitigating cyber threats to critical infrastructure. The Centre was to operate 24 hours a day, 7 days a week, and was to direct the national response to cyber security incidents. After seven years of existence, CCIRC still does not monitor cyber threats to critical infrastructure full time. Not being able to operate at all times reduces CCIRC's ability to gain a complete situational awareness of the national and international cyber threat environment. The limited hours of operation also hamper CCIRC's ability to provide timely and relevant information and analyses to critical infrastructure stakeholders. A lack of timely and relevant information and analyses affects the ability of critical infrastructure owners and operators to react to cyber attacks that may cause disruptions.

3.71 The lessons learned exercise that was done after the January 2011 intrusion on government systems reported that the systems were vulnerable. Despite the Government of Canada's commitments and investments in system security, which date back to 2001, cyber incidents were not reported in a timely manner and cyber threat information was not properly shared with appropriate departments. Also, good IT security practices were not consistently followed. Lead security agencies have begun to take action by updating the government's IT Incident Management Plan. The government has allocated more funds to bolster its capacity to detect cyber threats and is renewing its emphasis on increasing employees' awareness of IT security best practices.

3.72 Since 2001, we found that selected departments and agencies of the federal government have made limited progress in leading and coordinating activities, with partners, to secure Canada's critical infrastructure from cyber threats. Since 2010, with the release of the Cyber Security Strategy and the National strategy and action plan for critical infrastructure, there have been several accomplishments on the part of government to improve communications and build partnerships, and to enhance the monitoring of government systems.

About the Audit

All of the audit work in this chapter was conducted in accordance with the standards for assurance engagements set by The Canadian Institute of Chartered Accountants. While the Office adopts these standards as the minimum requirement for our audits, we also draw upon the standards and practices of other disciplines.

Objectives

The objective of our audit was to determine whether selected departments and agencies of the federal government are leading and coordinating activities, with partners, to secure Canada's critical infrastructure from cyber threats.

Scope and approach

Our audit covered the planning, management, and delivery of Public Safety Canada's responsibilities to lead the efforts of federal entities to protect the Government of Canada's critical infrastructure from cyber threats, and to provide leadership and coordinate federal efforts with those of the provinces and territories as well as private sector owners of critical infrastructure. It focused primarily on preventive and preparedness efforts required to protect Canada's critical infrastructure against cyber threats. We also looked at how Public Safety Canada is increasing awareness of cyber threats and promoting safe cyber security practices.

The audit team interviewed staff, mostly senior management and analysts, from Public Safety Canada, Communications Security Establishment Canada, and officials from the Chief Information Officer Branch. Other personnel interviewed included representatives from Shared Services Canada and the Canadian Security Intelligence Service.

Specific audit questions were also directed to the Privy Council Office for its role in providing strategic guidance; the Department of Justice for its role in providing legal advice and opinions in supporting elements pertaining to threat-based information sharing, particularly sensitive information, between federal departments and agencies and with other stakeholders; and the Royal Canadian Mounted Police for its supporting role in collecting and acting upon information on cyber incidents related to critical infrastructure.

Finally, we carried out interviews at Industry Canada, Natural Resources Canada, the Department of Finance and with private sector owners and operators of critical infrastructure assets and systems.

The audit did not examine matters of provincial or territorial jurisdiction, or provincial and territorial or private sector critical infrastructure protection efforts. It did not examine any classified systems or new legislative authorities provided to law enforcement agencies to combat cyber crime.

Criteria

Criteria	Sources
To determine whether selected departments and agencies are leading and coordinating federal government activities to secure Canada's critical infrastructure against cyber threats, in partnership with provinces, territories, the private sector, and selected international partners, we used the following criteria:	
Selected departments and agencies are leading federal government activities with partners to secure Canada's critical infrastructure from cyber threats.	• *Emergency Management Act* • *Department of Public Safety and Emergency Preparedness Act* • Canada's Cyber Security Strategy, Public Safety Canada • Policy on Government Security, Treasury Board, 2009 • National strategy and action plan for critical infrastructure, Public Safety Canada • National Security Policy: Securing an Open Society, Public Safety Canada
Selected departments and agencies are coordinating the activities of partners in securing Canada's critical infrastructure from cyber threats.	
To determine whether leadership and coordination roles and responsibilities for securing the Government of Canada's critical infrastructure against cyber threats are being exercised as defined, we used the following criteria:	
The leadership role in securing the Government of Canada's critical infrastructure against cyber threats is being exercised as defined.	• *Department of Public Safety and Emergency Preparedness Act* • *Emergency Management Act* • *Financial Administration Act* • Policy on Government Security, Treasury Board, 2009 • National strategy and action plan for critical infrastructure, Public Safety Canada • Canada's Cyber Security Strategy, Public Safety Canada
Activities to secure the government's critical infrastructure against cyber threats are being coordinated as defined.	• *Department of Public Safety and Emergency Preparedness Act* • *Emergency Management Act* • *Financial Administration Act* • *National Defence Act* • National Security Policy, Public Safety Canada • Policy on Government Security, Treasury Board, 2009 • Federal Policy for Emergency Management, Public Safety Canada • Policy on Management, Resources and Results Structures, Treasury Board • National strategy and action plan for critical infrastructure, Public Safety Canada • Canada's Cyber Security Strategy, Public Safety Canada
To determine whether Public Safety Canada is helping to increase the awareness of Canadians against cyber threats, we used the following criteria:	
Public Safety Canada is promoting an increased awareness of cyber crimes and the use of safe cyber security practices.	• *Emergency Management Act* • Policy on Government Security, Treasury Board, 2009 • Canada's Cyber Security Strategy, Public Safety Canada

Management reviewed and accepted the suitability of the criteria used in the audit.

Period covered by the audit

The audit covered the period between the January 1999 release of The Report of the Special Senate Committee on Security and Intelligence and 31 May 2012. Audit work for this chapter was completed on 17 July 2012.

Audit team

Assistant Auditor General: Wendy Loschiuk
Principal: Edward Wood
Director: Jean Goulet

Donna Ardelean
Jenna Lindley
Steven Mariani
Catherine Martin
Jeffrey Roy

For information, please contact Communications at 613-995-3708 or 1-888-761-5953 (toll-free).

Appendix List of recommendations

The following is a list of recommendations found in Chapter 3. The number in front of the recommendation indicates the paragraph where it appears in the chapter. The numbers in parentheses indicate the paragraphs where the topic is discussed.

Recommendation	Response
Protecting critical infrastructure from cyber threats	
3.25 Public Safety Canada should develop an interdepartmental action plan with deliverables and timelines for Canada's Cyber Security Strategy (2010) to guide the implementation of the strategy and measure progress. **(3.22–3.24)**	Agreed. Public Safety will release an interdepartmental action plan. This action plan will be based on the implementation plan that was developed prior to the launch of the Cyber Security Strategy in October 2010. Since some of the activities in that plan were of a sensitive nature and dealt with issues related to national security, the plan was not publicly released. Public Safety Canada is currently leading the development of a horizontal performance measurement strategy to measure and report on the progress made against commitments in the implementation plan.
Partnering to protect critical infrastructure	
3.37 Public Safety Canada should ensure that all sector networks are fully established and operating as outlined in the National strategy and action plan for critical infrastructure so that they can be an effective tool in helping to secure critical infrastructure in order to deliver the objectives of Canada's Cyber Security Strategy. **(3.31–3.36)**	Agreed. The sector networks provide a useful mechanism to deliver the private sector engagement objectives of Canada's Cyber Security Strategy, including sharing information on cyber threats and partnering with critical infrastructure sectors to conduct risk management activities. The Department will continue to work with lead federal departments and agencies to strengthen the sector networks, share information with sector stakeholders, including cyber threat information, and provide tools to support each sector's risk management efforts. Recognizing that each sector is unique and that representation is not expected to be uniform across each of the critical infrastructure sectors, Public Safety Canada will also provide guidance to lead federal departments and agencies on appropriate coverage for sector networks by December 2013.

Recommendation	Response
Monitoring cyber threats to critical infrastructure	
3.52 Public Safety Canada should increase the Canadian Cyber Incident Response Centre's ability to maintain situational awareness of cyber threats to Canada's critical infrastructure and to increase the Centre's ability to communicate this information to critical infrastructure owners and operators. **(3.39–3.51)**	Agreed. To enhance support for critical infrastructure and other partners, Public Safety Canada is augmenting CCIRC's operational capacity and capabilities, strengthening its policies and processes, and improving its information-sharing partnerships. In 2012, the government allocated an additional $13 million over five years to extend CCIRC's operational hours to 15 hours a day, 7 days a week. CCIRC's capabilities have been bolstered through the acquisition of a world-class malware analysis laboratory from the Communications Research Centre and the deployment of an industrial control systems test bed. CCIRC's mandate has been updated to provide greater clarity to internal and external partners. Standard procedures and policies are being updated where necessary to support the expansion of CCIRC's operations, ensuring that CCIRC provides value-added services that are efficient, effective, and consistent. Finally, CCIRC is improving information sharing with the introduction of the CCIRC Community Portal, a secure environment for collaboration, and the creation of formal information-sharing agreements with partners in the critical infrastructure; the first such agreement has recently been signed. Further, an incident response pilot has been launched with a number of partners, the lessons from which will greatly improve both response capability and cyber security readiness for all partners.
Protecting government information systems	
3.67 Treasury Board of Canada Secretariat, in cooperation with Shared Services Canada, should update relevant policies and plans to reflect the new information technology security roles and responsibilities of Shared Services Canada. **(3.63–3.66)**	Agreed. Treasury Board Secretariat has revised the Government of Canada (GC) Information Technology (IT) Incident Management Plan, which defines the roles and responsibilities of Shared Services Canada (SSC) with respect to incident management. The GC IT Incident Management Plan was approved by the Chief Information Officer (CIO) of Canada in May 2012. Additionally, the Secretariat is updating the Policy on Government Security to reflect the role of SSC as one of the lead federal IT security agencies and to define its associated IT security roles and responsibilities. The updated policy is expected to be published in 2013.