HOUSE OF COMMONS
CANADA

Chapter 1, Information Technology Security of the February 2005 Report of the Auditor General of Canada

Report of the Standing Committee on Public Accounts

John Williams, M.P.
Chair

June 2005

The Speaker of the House hereby grants permission to reproduce this document, in whole or in part for use in schools and for other purposes such as private study, research, criticism, review or newspaper summary. Any commercial or other use or reproduction of this publication requires the express prior written authorization of the Speaker of the House of Commons.

If this document contains excerpts or the full text of briefs presented to the Committee, permission to reproduce these briefs, in whole or in part, must be obtained from their authors.

Also available on the Parliamentary Internet Parlementaire: http://www.parl.gc.ca

Available from Communication Canada — Publishing, Ottawa, Canada K1A 0S9

Chapter 1, Information Technology Security of the February 2005 Report of the Auditor General of Canada

Report of the Standing Committee on Public Accounts

John Williams, M.P.
Chair

June 2005

STANDING COMMITTEE ON PUBLIC ACCOUNTS

CHAIR

John Williams

VICE-CHAIRS

Mark Holland
Benoît Sauvageau

MEMBERS

Dean Allison

Gary Carr

David Christopherson

Brian Fitzpatrick

Sébastien Gagnon

Daryl Kramp

Walt Lastewka

Shawn Murphy

Borys Wrzesnewskyj

CLERK OF THE COMMITTEE

Elizabeth B. Kingston

PARLIAMENTARY INFORMATION AND RESEARCH SERVICE
LIBRARY OF PARLIAMENT

Brian O'Neal
Marc-André Pigeon

THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

has the honour to present its

FOURTEENTH REPORT

Pursuant to Standing Order 108(3)(*g*), the Standing Committee on Public Accounts has considered Chapter 1 of the February 2005 Report of the Auditor General of Canada and has agreed to report the following:

TABLE OF CONTENTS

LIST OF RECOMMENDATIONS

RECOMMENDATION 1

That Treasury Board Secretariat accelerate the timetable for the development and implementation of all remaining IT security standards with the goal of having them completed well in advance of the December 2006 deadline it has established.

RECOMMENDATION 2

That beginning in September 2005 Treasury Board Secretariat submit semi-annual status reports to the Standing Committee on Public Accounts on the development and implementation of remaining IT security standards.

RECOMMENDATION 3

That Treasury Board Secretariat submit a detailed action plan to the Standing Committee on Public Accounts specifying the measures it will take to implement the recommendations made by the Auditor General of Canada. The action plan must include target implementation dates and must be provided to the Standing Committee on Public Accounts no later than 30 September 2005.

RECOMMENDATION 4

That Treasury Board Secretariat adhere to the requirements of the Government Security Policy as stated in Appendix A of the Policy, paying close attention to its duty to provide "advice and assistance on security" and to monitor "the implementation of the [P]olicy and the state of security in the Government of Canada."

RECOMMENDATION 5

That the Treasury Board Secretariat provide, in its annual departmental performance reports, information on its monitoring activities with respect to its obligations as set forth in Appendix A of the Government Security Policy. Reference must be made to the frequency and scope of monitoring, the results, and corrective measures taken. This reporting should begin with the report for the period ended 31 March 2005.

RECOMMENDATION 6

That the Government of Canada review the adequacy of resources and authorities available to the Office of the Chief

Information Officer to lead government-wide IT security efforts, explore the option of consolidating resources and authorities to take full responsibility for government-wide IT security in the hands of a single entity, and report the results to the Standing Committee on Public Accounts no later than 31 December 2005.

RECOMMENDATION 7

That Treasury Board Secretariat identify the reasons for turnover in the position of Chief Information Officer, analyze the results, and report its findings, along with an action plan listing the steps it will take to extend the tenure of this officer to a minimum five-year term, to the Standing Committee on Public Accounts no later than 31 December 2005.

RECOMMENDATION 8

That Treasury Board Secretariat develop and implement a plan for an awareness of the importance of IT security among senior departmental managers, with an emphasis on deputy ministers, and provide the Standing Committee on Public Accounts with a copy of this plan no later than 30 September 2005.

RECOMMENDATION 9

That a mandatory direct reporting relationship be established for departmental security officers and departmental IT security co-ordinators to their deputy ministers.

RECOMMENDATION 10

That departmental security officers be positioned at a strategic level within departments and agencies so that they can have meaningful influence over department-wide IT security strategies and input into budgeting decisions affecting security.

RECOMMENDATION 11

That departments and agencies be required to develop business continuity plans on a priority basis and to test these plans at least every two years, with the results to be communicated to the Office of the Chief Information Officer at Treasury Board Secretariat.

RECOMMENDATION 12

That the Office of the Chief Information Officer conduct a government-wide review to ascertain the total level of human, technological, and financial resources that are being devoted in fiscal year 2005-06 to IT security in departments and agencies, that it analyze the results to determine whether they are appropriate, and that it report the results to Parliament by 30 April 2006.

CHAPTER 1, INFORMATION TECHNOLOGY SECURITY OF THE FEBRUARY 2005 REPORT OF THE AUDITOR GENERAL OF CANADA

> A general lack of concern for IT security risks leaves systems vulnerable, where weaknesses could be exploited. As a result, sensitive data, including information on the privacy of Canadians, payroll and financial transactions, program information, and other mission-critical data are at increased risk of unauthorized disclosure, modification, or loss — possibly without being detected.[1]

INTRODUCTION

In her April 2002 Report, the Auditor General presented the results of an audit of information technology (IT) security in the federal government. The findings were sobering. The government's IT security standards were incomplete and many existing standards were out of date. There was no plan in place to update them. The 2002 Government Security Policy, a recent revision of the 1994 policy, would not be fully effective in the absence of these updated standards.

The Auditor General also discovered that the government had not been monitoring its 1994 IT security policy, with the result that the government did not have

> enough information to assess the overall state of IT security. It does not have an adequate basis for determining whether current practices across government are acceptable, nor does it have an appropriate baseline for measuring future progress.[2]

Mrs. Fraser noted that the revised (2002) policy called for a report on its effectiveness but not before summer 2004. In her view, a report was needed sooner. It was produced in draft form in May 2005.

Many government services are available in electronic format that Canadians can, from their homes or workplaces, access via their computers and other devices. The combination of low cost, and easy, fast availability to a widely scattered population makes the growth of the number of services provided in this way a certainty. As this expansion takes place, the vulnerability of the electronic delivery and storage systems has become a major concern. In the extreme, cyber attacks could result in personal information falling into the wrong hands, the destruction of vital data, the release of sensitive information on government operations, or the shutdown of internal government systems.

[1] Office of the Auditor General of Canada, *Status Report*, February 2005, Chapter 1, paragraph 37.

[2] Office of the Auditor General of Canada, *Report of the Auditor General of Canada to the House of Commons*, April 2002, Chapter 3, paragraph 3.3.

The Committee decided to review the results of a follow-up audit of the Auditor General's 2002 audit of IT security precisely because vulnerabilities in these systems pose enormous potential risks to the health and safety of Canadians, and to the functional ability of government.

To assist it with its review, the Committee met with Auditor General Sheila Fraser on 23 March 2005. The Auditor General was accompanied by Mr. Douglas Timmins (Assistant Auditor General), Mr. Richard Brisebois (Principal), and Mr. Guy Dumas (Director) of the Office of the Auditor General of Canada. At the same meeting, the Committee also heard from Helen McDonald, Acting Chief Information Officer for the Government of Canada, who is with the Treasury Board Secretariat. Mr. Simon Gauthier, Deputy Chief Information Officer, and Mr. Pierre Boucher, Acting Senior Director, Enterprise Architecture and Standards, also with Treasury Board Secretariat, appeared with Ms. McDonald.

OBSERVATIONS AND RECOMMENDATIONS

Subsequent to its review, the Committee has serious concerns that need resolution in the following areas: the current status of the standards used to support IT security; the role of Treasury Board Secretariat in monitoring the state of IT security; the role of departments and agencies; and, the resources available to support IT security.

IT Security Standards

The government's IT security standards are meant to establish minimum requirements that all departments and agencies must meet to ensure that their systems are secure from outside intrusion and data loss. In 2002, the Auditor General told Parliament that these standards were out of date, a troubling observation in light of the rapid change that characterizes information technology. In 2005, the Auditor General found that some improvement had taken place, but that overall the government had made "unsatisfactory progress" in strengthening IT security since her 2002 audit. (1.1)

The Government Security Policy (the Policy) establishes broad requirements for security in a range of areas including information technology. These requirements are supported by "security standards" that stipulate what departments and agencies must do to meet the Policy's minimum requirements. The presence of standards also, in the Auditor General's words, "… promote consistency in security measures across departments and sharing of best practices." (1.25)

In 2002, when the revised Policy came into force, many of the 40 supporting standards for IT security were not yet developed while some were outdated. The government published the *Management of Information Technology Security* (MITS) standard in May 2004. MITS covered 28 standards out of a total of 40, leaving 12 to be completed. Departments and agencies must await the completion of these standards in order to determine the extent to which they are in compliance with the Policy.

Treasury Board Secretariat (TBS, the Secretariat) has indicated that it will prioritize the 12 remaining standards according to a plan that it will make available early in fiscal year 2005-06. Acting Chief Information Officer Helen McDonald informed the Committee that 3 of the 12 standards are now in draft form and that TBS is proposing to have all of them completed by December 2006 at the latest.

Treasury Board Secretariat has set December 2006 as the date by which it expects departments and agencies to be compliant with the MITS standard. TBS indicates that it will monitor both the development of the remaining standards and departmental compliance with them.

This testimony needs to be put in context. When former Chief Information Officer Michelle d'Auray spoke to the Committee about the 2002 audit of IT security, she agreed that the government needed to accelerate the work on standards. Ms. d'Auray also told the Committee — over two years ago —that the government had "now developed a comprehensive plan that prioritizes the development of key standards."

There are thus three issues involved. The first concerns the timely completion of standards without which departments and agencies lack formal guidance on the minimal levels of security they need for their IT systems — and without which the actual status of government-wide IT security cannot be fully determined. Second is the high turnover in the position of Chief Information Officer that undermines the ability of the incumbent to make accurate, knowledgeable forecasts of the time and effort needed to bring about urgent change. And the last, linked to the second, has to do with the credibility of similar statements being issued by TBS today.

The current environment is unforgiving of delay. The urgency with which government addresses IT security must reflect this. Accordingly, the Committee recommends the following:

RECOMMENDATION 1

That Treasury Board Secretariat accelerate the timetable for the development and implementation of all remaining IT security standards with the goal of having them completed well in advance of the December 2006 deadline it has established.

It is difficult, in a dynamic environment, to make accurate estimates about the length of time it will take to complete complex projects. However, when Treasury Board Secretariat officials make commitments before a parliamentary committee, they must strive to be accurate and, afterward, they must make every possible effort to ensure that their commitments are met. When, for various reasons, estimates turn out to be overly optimistic and compromise commitments based on them, then Parliament must be informed. This is the only way in which accountability can be fully exercised and in which credibility can be earned — or, in this instance, regained. Consequently, the Committee recommends:

RECOMMENDATION 2

That beginning in September 2005 Treasury Board Secretariat submit semi-annual status reports to the Standing Committee on Public Accounts on the development and implementation of remaining IT security standards.

The Committee also notes that, as in 2002, the Secretariat has agreed to all of the Auditor General's recommendations. Since the Committee's enthusiasm regarding this response is constrained by the unacceptable results of the recent audit, it recommends:

RECOMMENDATION 3

That Treasury Board Secretariat submit a detailed action plan to the Standing Committee on Public Accounts specifying the measures it will take to implement the recommendations made by the Auditor General of Canada. The action plan must include target implementation dates and must be provided to the Standing Committee on Public Accounts no later than 30 September 2005.

The Role of Treasury Board Secretariat

The office of the Chief Information Officer is located in Treasury Board Secretariat, the central agency that holds main responsibilities for coordinating, leadership, oversight, and monitoring of IT security across government.

The Secretariat is instructed by the Government Security Policy (the Policy) to monitor the results of departmental internal IT security audits and to produce a mid-term report to Treasury Board on the effectiveness of the Policy.

It was therefore worrisome to discover that the Secretariat "is not adequately fulfilling its role" of monitoring and overseeing the state of security in departments and agencies. (1.23) The audit found, for example, that the Secretariat has "no formal process in place for getting departments and agencies to submit their [internal IT security] audit reports or analyzing the security findings" they contain. (1.72) While the Secretariat has only received 10 audit reports on IT security since 2002, (1.72) the Auditor General found that 37 departments and agencies had audited their IT security systems in the last two years. (1:70) In other words, the Secretariat had no formal means it could use to compel the production of IT security audit reports. This appears to be the result of the Secretariat's zeal for placing the entire burden of compliance with its policies on the shoulders of the departments and agencies and then hoping for the best.

The Committee believes strongly that, as in so many other areas under its responsibility, Treasury Board Secretariat must abandon its passive approach and actively monitor the application of the policies it promulgates. The Committee therefore recommends:

RECOMMENDATION 4

That Treasury Board Secretariat adhere to the requirements of the Government Security Policy as stated in Appendix A of the Policy, paying close attention to its duty to provide "advice and assistance on security" and to monitor "the implementation of the [P]olicy and the state of security in the Government of Canada."

RECOMMENDATION 5

That the Treasury Board Secretariat provide, in its annual departmental performance reports, information on its monitoring activities with respect to its obligations as set forth in Appendix A of the Government Security Policy. Reference must be made to the frequency and scope of monitoring, the results, and corrective measures taken. This reporting should begin with the report for the period ended 31 March 2005.

The Committee is concerned about the capacity of the Secretariat to do what the Policy calls for. It notes the small number of staff assigned to the Office of the Chief Information Officer (CIO) and the frequent turnover in the CIO position. It also notes that responsibility for IT security is divided between Treasury Board Secretariat and 10 lead agencies. Paul Rummell, a former Chief Information Officer has said that the government will continue to have problems with IT security unless a single agency is created that is accountable for policy and operations.[3] Although the Auditor General found that inter-agency co-operation and coordination have improved, the Committee shares concerns similar to those voiced by Mr. Rummell. The Committee accordingly recommends:

RECOMMENDATION 6

That the Government of Canada review the adequacy of resources and authorities available to the Office of the Chief Information Officer to lead government-wide IT security efforts, explore the option of consolidating resources and authorities to take full responsibility for government-wide IT security in the hands of a single entity, and report the results to the Standing Committee on Public Accounts no later than 31 December 2005.

[3] "Feds respond to Auditor General's IT security critique," ITBusiness.ca, 18 February 2005.

RECOMMENDATION 7

That Treasury Board Secretariat identify the reasons for turnover in the position of Chief Information Officer, analyze the results, and report its findings, along with an action plan listing the steps it will take to extend the tenure of this officer to a minimum five-year term, to the Standing Committee on Public Accounts no later than 31 December 2005.

The Role of Departments and Agencies

Under the Government Security Policy, deputy ministers are responsible for their department's ability to meet the requirements of the Policy and its supporting standards. This responsibility encompasses the performance of threat and risk assessments to determine whether departments need safeguards in addition to those prescribed by the Policy. The Policy also directs departments to conduct active monitoring and internal audits of their security systems on an ongoing basis and to report the results to Treasury Board Secretariat.

The Auditor General reported that departmental IT systems are "vulnerable to breaches in security," and that the majority of departments "do not meet the minimum standards" set by Treasury Board Secretariat for IT security. (1.3) The Committee was particularly concerned when it learned that senior management in many departments and agencies "is not aware of the IT security risks and does not understand how breaches of security could affect operations and the credibility of government." (1.4)

Yet deputy ministers bear the responsibility for determining the emphasis departments place on IT security and the level of resources that will be allocated for this purpose. Improvements are unlikely to occur unless deputy ministers are fully aware of the actual status of IT security in their departments and the risks associated with unresolved vulnerabilities.

Under the Government Security Policy, Treasury Board Secretariat is responsible for coordinating the provision of security training and awareness. The Secretariat is aware of the need to promote an awareness of the importance of IT security at the senior levels and is requiring that deputy ministers sign off on action plans for compliance with security standards in the fall of 2005. The Committee believes that these actions should be part of a wider effort to instil a greater awareness among senior managers and recommends:

RECOMMENDATION 8

That Treasury Board Secretariat develop and implement a plan for an awareness of the importance of IT security among senior departmental managers, with an emphasis on deputy ministers, and provide the Standing Committee on Public Accounts with a copy of this plan no later than 30 September 2005.

Each department and agency has a departmental security officer and an IT security coordinator but there is no assurance that they report directly to the deputy minister. Since direct access to the deputy minister is necessary to promote awareness of, and responsiveness to, IT security status and needs, the Committee recommends:

RECOMMENDATION 9

That a mandatory direct reporting relationship be established for departmental security officers and departmental IT security coordinators to their deputy ministers.

The Committee also notes that departmental security officers are not, in some cases, in a position to influence department-wide security-related decisions. This is a serious oversight that needs to be corrected as quickly as possible. The Committee accordingly recommends:

RECOMMENDATION 10

That departmental security officers be positioned at a strategic level within departments and agencies so that they can have meaningful influence over department-wide IT security strategies and input into budgeting decisions affecting security.

Despite the best precautions and monitoring, there remains a good chance that critical departmental IT systems might be shut down by a cyber attack. This is why the Government Security Policy requires departments and agencies to develop business continuity plans that will allow them to continue functioning in the event that such an attack takes place. The audit found that more than half of departments (53 out of 82, or 65 %) had such plans but only 24 had tested them over the last two years. This is unacceptable. The Committee recommends:

RECOMMENDATION 11

That departments and agencies be required to develop business continuity plans on a priority basis and to test these plans at least every two years, with the results to be communicated to the Office of the Chief Information Officer at Treasury Board Secretariat.

The Resources Available to Support IT Security

The decisions about resource allocation within departmental operating budgets are in the hands of deputy ministers. This audit shows that many deputy ministers are either unaware of the status of IT security inside their departments or do not assign sufficient importance to it. This finding suggests that departmental IT security is not receiving the resources needed to defeat the growing challenges it confronts. The Committee therefore recommends:

RECOMMENDATION 12

That the Office of the Chief Information Officer conduct a government-wide review to ascertain the total level of human, technological, and financial resources that are being devoted in fiscal year 2005-06 to IT security in departments and agencies, that it analyze the results to determine whether they are appropriate, and that it report the results to Parliament by 30 April 2006.

CONCLUSION

In Canada and elsewhere there is a high level of awareness of the vulnerabilities that surround the use of computer-based communications and data storage and data transmission systems. Threats to these systems have been expanding in harmony with our society's — and our governments' — growing reliance on these systems to manage and deliver an enormous array of public and private transactions and services. Many of the transactions are of a confidential commercial or financial matter, or are matters of public health and safety.

The federal government is the largest entity in Canada. The number and nature of its exchanges with groups and individuals is enormous and — in a country whose citizens are dispersed across great distances — sure to expand. These services will grow more sophisticated, more widespread, and from the perspective of individual consumers, less expensive and easier to obtain and use.

Apart from the extent of its involvement in the accumulation of sensitive data, the government is, in turn, one of the largest providers of services and information to Canadians via electronic means. Many of these services are considered vital, including the issuance of Canada Pension Plan, Employment Insurance and other benefits, payments to suppliers, cash transfers to other levels of government, and inter-governmental and intra-governmental communications that touch on health, safety, and other important matters.

Against this backdrop, there is a pronounced need for the highest possible level of security to protect these interactions, and the resulting accumulation of data, against intrusion. A weakness or a breakdown in federal government IT security would have serious implications for Canadians and the availability of all manner of services upon which they depend. Further, as in any democratic system, institutions of government function only to the extent that they are perceived as legitimate and worthy of trust by their citizens. Government, as custodian of some of its citizens' most private information, must therefore guard that information with utmost caution. Otherwise, in the words of the Auditor General: "If security weaknesses allowed someone to access a database or confidential information, Canadians' trust in government would be greatly eroded." (1.4)

From the Committee's perspective, it is not possible to underestimate the potential adverse consequences of a failure to adequately protect government

IT systems against intrusion or breakdown. Those entrusted with the protection of those systems — at central agencies and in senior managerial positions in departments and agencies — need to be fully aware of the significant risks resulting from a failure to exercise proper monitoring of IT security systems and to take immediate corrective action when vulnerabilities are discovered.

Weeks following the Committee's review, the results of an internal audit obtained through an access to information request shows that there is indeed reason for concern. According to newspaper reports, a 2004 internal audit at the Canada Revenue Agency found that "laptops used outside the office were not locked up properly, confidential information was kept on computers that were vulnerable to hacking and workers did not know they are required to report criminal activity." Of 3,000 workers surveyed, more than half did not know how to report a security incident. Managers "said they were unsure about whether, and how, to monitor the department's electronic systems."[4] As the newspaper report noted, four computers stolen from the Revenue Agency's office in Laval, Québec, in 2003 contained information on 120,000 Canadians, including their social insurance numbers. This report, and the results of the Auditor General's investigation clearly show that IT security vulnerabilities are spread across all government entities, including large ones responsible for handling the most sensitive personal information of Canadian citizens.

The Committee fully expects, therefore, that the Government of Canada and Treasury Board Secretariat will assign urgent priority to acting on commitments to resolve IT security vulnerabilities, implementing the Auditor General's recommendations, and ensuring that Canadians have secure, trustworthy electronic access to government programs and services.

[4] Security report blasts tax collectors, *Globe and Mail*, 25 April 2005.

APPENDIX A
LIST OF WITNESSES

Associations and Individuals	Date	Meeting
Office of the Auditor General of Canada	23/03/2005	25
Richard Brisebois, Principal		
Guy Dumas, Director		
Douglas Timmins, Assistant Auditor General		
Treasury Board of Canada Secretariat		
Pierre Boucher, Senior Director, Architecture, Standards and Engineering		
Simon Gauthier, Deputy Chief Information Officer		
Helen McDonald, Chief Information Officer		

REQUEST FOR GOVERNMENT RESPONSE

In accordance with Standing Order 109, the Committee requests that the government table a comprehensive response to the report.

A copy of the relevant Minutes of Proceedings (*Meeting Nos. 25 and 40 including this report*) is tabled.

Respectfully submitted,

John Williams, M.P.
Chair

MINUTES OF PROCEEDINGS

Wednesday, June 1, 2005
(*Meeting No. 40*)

The Standing Committee on Public Accounts met *in camera* at 3:32 p.m. this day, in Room 237-C Centre Block, the Chair, John Williams, presiding.

Members of the Committee present: Dean Allison, Gary Carr, David Christopherson, Brian Fitzpatrick, Sébastien Gagnon, Mark Holland, Daryl Kramp, Hon. Shawn Murphy, Benoît Sauvageau, John Williams and Borys Wrzesnewskyj.

Acting Member present: Hon. Robert Thibault for Hon. Walt Lastewka.

In attendance: *Library of Parliament*: Brian O'Neal, Analyst.

Pursuant to Standing Order 81(7), the Committee resumed consideration of the Report on Plans and Priorities 2005-2006 of the Office of the Auditor General of Canada.

The Committee commenced consideration of a draft report.

It was agreed, — That the Committee adopt the draft report as the Report to the House.

It was agreed, — That, pursuant to Standing Order 109, the Committee request that the Government table a comprehensive response to the report.

It was agreed, — That the Chair, Clerk and analysts be authorized to make such grammatical and editorial changes as may be necessary without changing the substance of the report.

It was agreed, — That the Chair present the Report to the House at the earliest opportunity following the expiry of the forty-eight (48) hour revision period.

It was agreed, — That the Clerk and the analysts, in consultation with the Chair, issue a news release.

Pursuant to Standing Order 108(3)(g), the Committee resumed consideration of Chapter 1, Information Technology Security of the February 2005 Report of the Auditor General of Canada referred to the Committee on February 15, 2005.

The Committee commenced consideration of a draft report.

It was agreed, — That the Committee adopt the draft report as the Report to the House.

It was agreed, — That, pursuant to Standing Order 109, the Committee request that the Government table a comprehensive response to the report.

It was agreed, — That the Chair, Clerk and analysts be authorized to make such grammatical and editorial changes as may be necessary without changing the substance of the report.

It was agreed, — That the Chair present the Report to the House at the earliest opportunity following the expiry of the forty-eight (48) hour revision period.

It was agreed, — That the Clerk and the analysts, in consultation with the Chair, issue a news release.

At 4:43 p.m., the Committee adjourned to the call of the Chair.

Elizabeth B. Kingston
Clerk of the Committee