HOUSE OF COMMONS
CANADA

CHAPTER 1, "SAFEGUARDING GOVERNMENT INFORMATION AND ASSETS IN CONTRACTING," OF THE OCTOBER 2007 REPORT OF THE AUDITOR GENERAL OF CANADA

Report of the Standing Committee on Public Accounts

Hon. Shawn Murphy, MP
Chair

APRIL 2010

40th PARLIAMENT, 3rd SESSION

Published under the authority of the Speaker of the House of Commons

Additional copies may be obtained from: Publishing and Depository Services
Public Works and Government Services Canada
Ottawa, Ontario K1A 0S5
Telephone: 613-941-5995 or 1-800-635-7943
Fax: 613-954-5779 or 1-800-565-7757
publications@tpsgc-pwgsc.gc.ca
http://publications.gc.ca

Also available on the Parliament of Canada Web Site
at the following address: http://www.parl.gc.ca

CHAPTER 1, "SAFEGUARDING GOVERNMENT INFORMATION AND ASSETS IN CONTRACTING," OF THE OCTOBER 2007 REPORT OF THE AUDITOR GENERAL OF CANADA

Report of the Standing Committee on Public Accounts

Hon. Shawn Murphy, MP
Chair

APRIL 2010

40th PARLIAMENT, 3rd SESSION

STANDING COMMITTEE ON PUBLIC ACCOUNTS

40th PARLIAMENT, 3rd SESSION

CHAIR

Hon. Shawn Murphy

VICE-CHAIRS

David Christopherson

Daryl Kramp

MEMBERS

Josée Beaudin

Earl Dreeshen

Derek Lee

Bev Shipley

Hon. Stéphane Dion

Meili Faille

Andrew Saxton

Terence Young

CLERK OF THE COMMITTEE

Joann Garbig

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Maria Edwards

Alex Smith

STANDING COMMITTEE ON PUBLIC ACCOUNTS

40th PARLIAMENT, 2nd SESSION

CHAIR

Hon. Shawn Murphy

VICE-CHAIRS

David Christopherson

Daryl Kramp

MEMBERS

Bonnie Crombie

Meili Faille

Derek Lee

Pascal-Pierre Paillé

Andrew Saxton

Bev Shipley

John Weston

Terence Young

CLERK OF THE COMMITTEE

Joann Garbig

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Andrew Kitching

Alex Smith

STANDING COMMITTEE ON PUBLIC ACCOUNTS

39th PARLIAMENT, 2nd SESSION

CHAIR

Hon. Shawn Murphy

VICE-CHAIRS

Jean-Yves Laforest

David Sweet

MEMBERS

Mauril Bélanger

Brian Fitzpatrick

Mike Lake

Pierre Poilievre

Borys Wrzesnewskyj

David Christopherson

Mark Holland

Marcel Lussier

John G. Williams

CLERK OF THE COMMITTEE

Justin Vaive

Joann Garbig

LIBRARY OF PARLIAMENT

Parliamentary Information and Research Service

Lydia Scratch

Alex Smith

THE STANDING COMMITTEE ON PUBLIC ACCOUNTS

has the honour to present its

FIFTH REPORT

Pursuant to its mandate under Standing Order 108(3)(*g*), the Committee has studied Chapter 1, “Safeguarding Government Information and Assets in Contracting,” of the October 2007 Report of the Auditor General of Canada and has agreed to report the following:

INTRODUCTION

The federal government uses a wide range of classified and protected information and assets in the process of governing the country. The government frequently contracts with the private sector for the provision of goods and services, and in many cases contractors have access to protected or classified information and assets of the government. It is vital that the government protects the security of government information and assets made available to contractors, who potentially have access to sensitive information related to the health, safety, security, and economic well-being of Canadians. Security of government information is an integral part of maintaining public trust in government institutions. Ensuring an effective security regime also allows Canadian companies to access significant international contracting opportunities.

Security has been given renewed importance in the past few years, and the Office of the Auditor General (OAG) tabled an audit in October 2007 on the federal government's ability to safeguard its information and assets when contracting for goods and services.[1] The House of Commons Standing Committee on Public Accounts had a hearing on this audit on 26 February, 2008.[2] The Committee heard from numerous witnesses representing the organizations involved in the audit—from the Office of the Auditor General of Canada: Sheila Fraser, Auditor General of Canada; from the Treasury Board Secretariat: Ken Cochrane, Chief Information Officer; from Public Works and Government Services Canada: Gerry Deneault, Director General, Industrial Security Sector; François Guimont, Deputy Minister; from the Department of National Defence: Glynne Hines, Chief of Staff, Office of the Assistant Deputy Minister, Information Management; Dave Shuster, Director, Deputy Provost Marshal, Security; Scott Stevenson, Acting Assistant Deputy Minister, Infrastructure and Environment; from and Defence Construction Canada: Ross Nicholls, President and Chief Executive Officer.

[1] Auditor General of Canada, October 2007 Report, "Chapter 1, Safeguarding Government Information and Assets in Contracting."
[2] House of Commons Standing Committee on Public Accounts, 39th Parliament, 2nd Session, Meeting 17.

As the Committee was concerned about the evidence it heard at this hearing and because it was disturbed by the discovery of building blueprints in the trash, the Committee held a subsequent meeting on 3 June 2008.[3] At this hearing the Committee heard from several officials from the Office of the Auditor General: Sheila Fraser, Auditor General of Canada; Hugh McRoberts, Assistant Auditor General; and Bruce Sloan, Principal. From the Department of National Defence, the Committee heard from Robert Fonberg, Deputy Minister; Lieutenant General Walter J. Natynczyk, Vice-Chief of the Defence Staff; Scott Stevenson, Assistant Deputy Minister, Infrastructure and Environment; Dan Ross, Assistant Deputy Minister, Materiel; Major General Glynn Hines, Chief of Staff, Office of the Assistant Deputy Minister, Information Management; Colonel Michael Day, Commander, Canadian Special Operations Forces Command; Lieutenant Colonel Dave Shuster, Director, Deputy Provost Marshal Security. Defence Construction Canada was represented by Ross Nicholls, President and Chief Executive Officer.

BACKGROUND

In order to ensure that sensitive information and assets of the government are properly protected, the Treasury Board adopted a Government Security Policy. Under this policy each government department is responsible for protecting sensitive information and assets under its control throughout the bidding, negotiating, awarding, carrying out, and terminating of any contract it manages.

Public Works and Government Services Canada (PWGSC) is the lead department for procurement in the federal government and accounts for 90% of the dollar value and 10% of the total volume of contracts. Given the importance of PWGSC to the contracting process, the audit focused on how PWGSC delivers its Industrial Security Program and how it carries out its role as the lead contracting authority for the government. As other departments also handle sensitive contracts, the audit looked at whether the roles and responsibilities for security in government contracting are clear, and whether PWGSC, National Defence, the Royal Canadian Mounted Police, and

[3] Meeting 36.

Defence Construction Canada have procedures to ensure that they fulfill these roles and responsibilities. The audit also examined the role of the Treasury Board Secretariat in monitoring how the Government Security Policy is implemented.

The audit makes ten recommendations, and the Committee supports all of these recommendations. Nonetheless, there are several areas the Committee would like to explore further in order to ensure accountability for taking action to rectify the weaknesses identified by the OAG.

TREASURY BOARD SECRETARIAT

The Treasury Board's Government Security Policy sets out the government's objectives for industrial security. The audit found that the Security and Contracting Management Standard, which supplements the Policy, is a mixture of required and recommended procedures that has led to confusion about responsibilities under the Policy.[4] In addition, departments were interpreting the Standard as requiring the completion of a Security Requirements Checklist only for projects where they have identified a security requirement. (The Checklist identifies security requirements at the start of the contractual process.) However, the OAG believes that this could result in diminished accountability for decisions regarding security because an incorrect decision by a project authority that security is not an issue could pose a risk.

The Government Security Policy requires that a departmental security officer in each department establish and direct a security program. The audit found that management oversight of industrial security was lacking in the departments audited.[5]

The audit also examined the Treasury Board Secretariat's monitoring of industrial security and concluded that its activities are not sufficient to provide assurance that the government's security objectives are being met.[6] The Secretariat had conducted a survey of departmental security officers which indicated a high degree of compliance

[4] Ibid., paragraph 1.18.
[5] Ibid., paragraph 1.81.
[6] Ibid., paragraph 1.88.

with the Policy's security requirements. However, this is not consistent with the findings of the audit.

Ken Cochrane, Chief Information Officer at the Treasury Board Secretariat, described the actions his department was taking in response to the audit:

> The new government security policy will clarify the requirements under the standard on security in contracting. This will ensure that the project authorities who originate the contracts will be the ones who certify the security requirements needed. … The Treasury Board Secretariat will also require that departmental security officers implement quality assurance procedures. … The Treasury Board Secretariat has added an indicator under MAF, the Management Accountability Framework, to assess the compliance of departments and agencies with security requirements.[7]

The Committee appreciates the actions that the Secretariat is taking to clarify the requirements of the Policy and the associated Standard. However, the Committee believes that the Secretariat must take responsibility for the lack of clarity in the first place, as it is the Secretariat that developed them. Also, when the Policy was updated in 2002, the Standard was not similarly revised, even though it had been in place since 1994. When pressed on the issue of responsibility, Mr. Cochrane said, "I think it's a big integrated system, so if there's some lack of clarity in the work that we've done in the past, then we obviously have a role to play in this overall."[8]

The Committee believes that the Secretariat must be more proactive in ensuring that the requirements of Treasury Board policies are clear and that departments understand their responsibilities, because otherwise it would not be reasonable to hold departments to account for following those policies. Nonetheless, the Committee does not have a lot of confidence in the Secretariat's ability to monitor compliance or its willingness to hold departments to account for a failure to comply with Treasury Board policies. The Secretariat has added an indicator to the Management Accountability Framework to assess departmental compliance with security requirements, but given the Secretariat's poor track record in monitoring compliance, as was noted by the OAG,

[7] Meeting 17, 11:30 am.
[8] Ibid., 1:35 pm.

and the Committee's scepticism in the effectiveness of the Management Accountability Framework, the Committee would like to see the results of the assessment against this new indicator. The Committee recommends:

RECOMMENDATION 1

That the Treasury Board Secretariat provide the Public Accounts Committee with consolidated results of the next Management Accountability Framework's assessment of departments' and agencies' compliance with security requirements.

PUBLIC WORKS AND GOVERNMENT SERVICES CANADA

PWGSC established an Industrial Security Program to manage its security responsibilities. The Program is intended to ensure that companies and personnel requiring access to sensitive government information and assets are appropriately screened and receive security clearances. The Program also identifies the appropriate security terms and conditions to be included in each contract and ensures that contractors comply with the security requirements. This Program processes about 2,000 security-related contracts per year. PWGSC is the contracting authority for 75% of these contracts and the remaining 25% are handled at the request of other departments.

The audit found serious weaknesses in the Industrial Security Program. The Program's mandate was changed twice during the course of the audit; the departmental policy on industrial security and its supply manual were in the process of being revised; and standard operating procedures for the Program were in draft form and incomplete. Moreover, the audit found that a number of sensitive contracts requiring the "secret" level of security clearance were awarded before contractors were cleared to the security level required in the contract, and in some cases work was completed in full before the contractor was cleared. Also, a number of critical steps in the industrial security process, such as having contractors sign a Security Agreement, were not consistently followed. In the opinion of the OAG, PWGSC had not exercised due diligence in its duties.

While PWGSC's Deputy Minister and Accounting Officer, François Guimont, pointed out that the security elements of most contracts were handled appropriately, the Committee is deeply troubled by the weaknesses in the Industrial Security Program and is very concerned that some officials appeared to be willing to circumvent key security procedures in order to reduce costs and avoid delays in completing projects. Mr. Guimont assured the Committee that mitigating measures were put in place, but there would seem to be little point in putting security requirements into a contract if the work can completed before the proper security clearances are obtained. The Committee believes that it is unacceptable that any sensitive contracts were allowed to proceed without the proper security clearances in place. Mr. Guimont also told the Committee that all of the contracts were eventually security cleared; however, the Committee cannot help but wonder what PWGSC would have done if they found security problems after the fact. Failing to follow the security procedures means that there is a significant risk to the security of government information and assets.

The Committee appreciates that PWGSC has undertaken a number of actions since the audit. Prior to the hearing, PWGSC helpfully provided the Committee with a detailed action plan with timelines and information on the status of actions taken. Many of the actions have already been completed. The Committee hopes that more departments would provide detailed action plans in a timely manner. Additionally, as part of its action plan PWGSC decided to examine contracts outside of the scope of the audit. PWGSC is reviewing 3,000 active contracts with security requirements to verify that it has fulfilled its security obligations, and it is undertaking a third party management review of the Program's mandate, roles and responsibilities, and program delivery.

The Committee has subsequently received updated information from PWGSC on the status of actions it has taken, and this information can be found in the Addendum to the report.

The Committee was told that one of the core issues facing the Industrial Security Program was inadequate funding. The audit noted that several business cases prepared for the department identified resource challenges and noted that funding was insufficient to manage the increase in business volumes since the events of September 11, 2001.[9] This has made it difficult for the Program to attract and retain qualified security professionals. Mr. Guimont told the Committee that having an insufficient number of staff contributed to the problems identified by the OAG. The lack of staff meant that Program managers were unable to devote resources to clarifying the Program's mandate and finalizing policies and procedures. It may also explain some of the instances of failing to complete all of the steps in the industrial security process.

Mr. Guimont told the Committee that he had authorized the reallocation of funding to the Program in order to make up for the shortfall. However, the reallocations were almost 100% of the base funding. Mr. Guimont described the funding pressures:

> Base funding for the program is $6.7 million. Over the past few years, we allocated another $6 million on average within the department. Recently, in September, we received $11.3 million from Treasury Board for the contract security program. There was an increase from Treasury Board, but those funds run out at the end of the fiscal year. On March 31, I will have to find either a long-term or short-term solution to ensure continued progress with the program.[10]

The concern with reallocations is that they do not allow managers to offer permanent positions to their employees. Also, they may deprive other programs within the department of much needed funding. Additional stable, long-term funding is necessary for the Program to perform effectively. The Office of the Auditor General recommended that PWGSC ensure that the Program has adequate resources to meet its program objectives.[11] The Committee supports this recommendation, but as long-term funding must come from the Treasury Board, the Committee recommends:

[9] Chapter 1, paragraph 1.54.
[10] Meeting 17, 12:50 pm.
[11] Chapter 1, paragraph 1.59.

RECOMMENDATION 2

That the Treasury Board approve stable, long-term funding to Public Works and Government Service's Industrial Security Program to enable it to meet its objectives.

The Industrial Security Program currently manages contracts for which there is a security element when the contracting authority is PWGSC or at the request of other departments. This means that other departments handle many of their own contracts with a security element, even though they may not have the necessary expertise to implement the Government Security Policy. Given the Program's expertise in security, it could potentially be beneficial for the Program to handle all government contracts of a sensitive nature. It would also ensure a consistent approach to security in government contracting. When asked whether there was any reason that all contracts of a sensitive nature should not go through the Industrial Security Program, Mr. Guimont replied, "No good reason I can think of."[12] On the other hand, as it may not be appropriate to impose a one-size-fits-all solution on all departments, the Committee believes that this is an idea that should be studied further. The Committee recommends:

RECOMMENDATION 3

That Public Works and Government Services Canada and the Treasury Board Secretariat review whether all contracts with a requirement of "secret" level of security or higher should be processed by the Industrial Security Program, and report to the Public Accounts Committee by 31 August 2010 on the results of this review.

DEPARTMENT OF NATIONAL DEFENCE AND DEFENCE CONSTRUCTION CANADA

The Department of National Defence has been among the departments with the highest number of sensitive contracts processed by the Industrial Security Program. National Defence also ensures the security of a large number of contracts awarded within its own delegated contracting authority. The audit found that National Defence

[12] Meeting 17, 12:25 pm.

has a fairly comprehensive policy on security in contracting, but the policy has not been revised to reflect a number of important security updates issued by the Treasury Board Secretariat.[13] Additionally, its manual of operating procedures for procurement was incomplete at the time of the audit, and the Security Requirements Checklist was not used consistently within National Defence.

Defence Construction Canada is a Crown corporation with contracting authority for government defence projects. It awards and manages contracts for the construction and maintenance of infrastructure, almost exclusively on behalf of National Defence. As a Crown corporation, it is not subject to the Government Security Policy. However, Ross Nicholls, the President and Chief Executive Officer of the Corporation told the Committee that:

> The Corporation has always implemented measures consistent with the Government Security Policy to safeguard those assets and information. Furthermore, we have agreed with Treasury Board Secretariat to apply the Government Security Policy to all our operations related to the delivery of defence projects.[14]

While the Committee appreciates the Corporation's efforts to reach an agreement with the Secretariat, the Committee is rather concerned that this agreement was only reached after an audit by the OAG, even though the Corporation has been in existence for 56 years.

The audit also found that National Defence did not provide a Security Requirements Checklist for 99% of the contracts awarded by the Corporation.[15] The Committee was told that most of the contracts involved routine construction and maintenance to National Defence's many buildings and roads and consequently security would not be an issue. While many of the contracts may indeed be routine, the Committee has difficulty believing that regular access to military bases, where most of these buildings and roads would be located, would not require some sort of security

[13] Chapter 1, paragraph 1.63.
[14] Meeting 17, 11:25 am.
[15] Chapter 1, paragraph 1.73.

review. More importantly, if a Checklist was not completed, there is no way of knowing whether or not security was an issue or whether contractors were cleared to appropriate security levels. Given the sensitivity of the sites and the information at stake, the Committee finds the approach of National Defence to security in contracting alarmingly casual. This led to serious concerns with security at the NORAD facility, which is discussed below.

The Committee believes that both National Defence and the Corporation need to make serious efforts to improve their practices with respect to security in contracting. It should be noted that both organizations provided the Committee with an action plan to address the findings of the OAG. They also provided the Committee with updated action plans at the meeting on 3 June. The Auditor General said:

> We have looked at the action plans of both Defence Construction and the Department. We believe that they address the issues that we raised in our audits. As I always say we are cautiously optimistic that they will be put into place because obviously some of the deadlines are out further and we haven't gone back to actually check that everything will be done, but it does look very promising.[16]

The Committee has subsequently received updated information from the Department of National Defence and Defence Construction Canada on the status of actions they have taken, and this information can be found in the Addendum to the report.

CONSTRUCTION PRACTICES ON DEFENCE PROJECTS

While the Department of National Defence appears to be taking the findings of the OAG seriously, there are a couple of incidents that call into question the Department's ability to address the problems with its approach to security.

The North American Aerospace (NORAD) Above Ground Complex in North Bay, Ontario was intended to replace the underground complex which housed the NORAD air surveillance and control system to secure North American airspace. According to the

[16] Meeting 36, 44:45 am.

audit, National Defence did not analyze potential security risks before awarding contracts for construction of the facility.[17] This resulted in unscreened contractors and workers having access to the plans and construction site. The Auditor General told the Committee that, "There is a risk that security was breached."[18]

Concerns about security led to questions about whether or not the facility could be used for its intended purpose. After a series of investigations, National Defence concluded that the facility, with modifications, could be used for its intended purpose, but at the time of the audit, National Defence had not provided the OAG with detailed plans, schedules, and costs for the required modifications. The construction of this facility is presented by the OAG as an example of what can happen as a result of a failure to identify industrial security requirements during the pre-contract stage, as required by the Government Security Policy.

However, at the Committee's first hearing on the audit, National Defence's subject matter expert on the NORAD facility, Major General Glynne Hines, suggested to the Committee that construction on the facility proceeded normally. He said:

> For the initial construction activity that took place, there was an original threat risk assessment done relating to that facility, and it was determined at that time that a Security Requirements Checklist was not required to initiate the construction of the building. During the construction of the building, as is normal, a security review was conducted, and it was determined that additional security would be required, as the building envelope had been constructed, and as we were getting ready to do the fit-up of equipment, which would cause the building to go from an unclassified, no-clearance-required nature to a classified, clearance-required nature. At that time, when the security requirement became evident during the construction, and prior to installing the systems, contractors with security clearances were required to be on site or workers on site were required to be under escort.[19]

He further explained the approach, "It was a phased approach from the standpoint of starting from bare ground, where there were no security concerns, threats, or risks

[17] Chapter 1, paragraph 1.74.
[18] Meeting 17, 11:45 am.
[19] Ibid., 11:35 am.

identified, to the point where systems were installed and the facility became secure and sensitive."[20]

MGen Hines told the Committee that there have been no additional costs for the security lapses. Instead, "There were additional security measures taken in that building that are consistent with the evolving threat [related to the post-9/11 environment]."[21] He also seemed to be unaware of any delay. "I'm not aware what the timeline was for any delay; however, modifications that are performed and reworking that has to be done are regrettably all part of normal construction practices."[22] There were certain implementation deficiencies, such as power cables that were not terminated correctly or junction boxes where they should not have been, but not design deficiencies.

Ms. Fraser was very concerned about the testimony of MGen Hines. She said, "So there seems to be a little confusion here, but certainly when we did that original audit there were concerns about the use of that building."[23] Ms. Fraser suggested that her office work with the Department of National Defence to clarify their respective understanding of the security problems related to the NORAD facility.

Subsequent to the hearing, the Committee received correspondence from the Auditor General and the Deputy Minister of National Defence. In her letter, the Auditor General said that documents received from National Defence during the audit indicated that officials determined that budget and timeline for the construction project were given priority over security concerns.

In his letter to the Committee, the Deputy Minister of National Defence, Robert Fonberg, apologized to the Committee for any misunderstanding the testimony of MGen Hines may have caused and assured the Committee that there was no intention to mislead. Mr. Fonberg noted that the Department's longstanding practice with respect to

[20] Ibid., 12:20 pm.
[21] Ibid., 11:40 am.
[22] Ibid., 1:00 pm.
[23] Ibid., 12:20 pm.

construction projects has been to treat the construction of a building's shell as unclassified work. Additional security measures are taken to control the site when secure systems are installed. The Deputy Minister acknowledged that this approach to the NORAD complex was inappropriate and a Security Requirements Checklist should have been completed before the contract was tendered. Further, none of the on-site contractors possessed valid security clearances, with the exception of the architects. Corrective measures have since been taken, such as installing special monitoring equipment, to mitigate potential security concerns, at an initial cost of $515,000 and annual recurring costs of $84,000.

The Committee is astonished that security was not identified as an issue at the outset of constructing a highly sensitive NORAD facility. At the very least, this demonstrates a lax attitude towards security by the Department of National Defence. Additionally, allowing unsecured contractors to have access to the construction site and building plans indicates that security practices were deficient, and finding electrical systems installed contrary to design is alarming. If the Department had taken security more seriously at the outset, it would not have had to perform extensive physical and technical inspections before occupying the facility, at a significant cost to Canadian taxpayers. This incident clearly demonstrates a lack of judgement by those involved. What is even more disturbing is that this may not be an isolated incident.

While the Deputy Minister acknowledged at the 3 June hearing that it was a mistake to not classify the blueprints for the NORAD facility, the earlier testimony of MGen Hines suggests a culture within the Department where it continues to be normal and appropriate to not consider security issues from the outset of construction. The Committee expected that the Department would have learned from this mistake and improved its practices and culture, but a recent incident demonstrates that the Department still does not pay sufficient attention to security issues during the construction of sensitive facilities.

In March 2008, a defence analyst with the Rideau Institute on International Affairs found in the garbage blueprints for the new facility for the Canadian Joint Incident Response Unit in Trenton, Ontario. This Unit is the military's main responder to chemical, biological, and radioactive threats; it includes more than 100 personnel and an array of technical equipment. According to a media report, the design plans "show the electrical grid scheme for the unit's computers and details about sewer systems, areas for workshops, sea container loading docks, and offices for the unit's various troops. There is also a blueprint for the storage bay for the unit's robots, which are designed to detect chemical and biological agents."[24]

The Deputy Minister of National Defence told the Committee that Treasury Board policies were followed in this case, and a Security Requirements Checklist was completed prior to awarding the contract for the design and construction of the facility. As it was concluded that the blueprints contained no classified information, there was no requirement for contractual security provisions relating to their preparation and subsequent handling. The Deputy Minister speculated that perhaps non-classified documents should be handled differently, but the Committee believes that this is not the relevant issue at hand. Rather, the question is why the blueprints were not deemed to be classified material in the first place. While there was an improvement in that a Checklist was actually completed, the approach to security during construction at the Department remains the same—the shells of buildings have no security issues. Yet, it is very difficult for the Committee to believe that the blueprints for the military's main responder to chemical, biological and radioactive threats should not be secure, especially in an era of heightened security awareness for possible terrorist threats.

The Committee believes that it is not sufficient to hide behind procedure and process. The processes must be conducted in a way that takes security seriously from the beginning to the end of the construction of a new facility. As the Auditor General said:

[24] David Pugliese, "Elite military unit's blueprints for new HQ found in trash can; Passerby finds anti-terror force's plans discarded on Bank Street," *Ottawa Citizen*, March 20, 2008, page A1.

> The issue comes back to under the current practices or the practices at that time of the department, what they would do is the shells of the buildings in most cases would not be considered classified and it was only when they started to do the fit-up of what goes inside that then they would look at classification and one of the issues, I think, that is coming out of all this is maybe they should be considering what is going to happen inside that building much sooner in the process.[25]

The Committee agrees, and consequently recommends:

RECOMMENDATION 4

That the Department of National Defence undertake thorough assessments of security issues that take into account a building's future use before constructing new facilities.

CONCLUSION

The federal government regularly contracts with the private sector for the provision of goods and services, and when it does so, it is essential that government departments and agencies establish mechanisms to ensure the security of information and assets entrusted to private contractors. However, the Office of the Auditor General found weaknesses at almost all levels in those processes. Some officials were willing to circumvent key security procedures in order to reduce costs and avoid delays in completing projects.

The Committee is alarmed that security would not have been taken more seriously by government departments, especially given today's heightened awareness of the importance of security. The Committee is encouraged that PWGSC has taken significant steps to improve the weaknesses found in its Industrial Security Program; although, the Committee is rather concerned that the weaknesses even existed. It is rather disturbing to learn that government officials were allowing work to proceed on contracts even though the security provisions of the contract had not yet been met. While it is possible to put in place security mitigation measures, the Committee cannot help but wonder what the government would do should security be breached when work

[25] Meeting 36, 12:05 pm.

had begun prior to obtaining the appropriate security clearances. Once security has been breached, it is too late to put in place mitigation measures.

The Department of National Defence and Defence Construction Canada have also committed to improve their security practices, but the Committee was very troubled by the casual, if not careless, attitude of National Defence towards security. This was especially evident for the NORAD facility which needed substantial security reviews and modifications in order to for the facility to be used for its intended purpose. This would not have been necessary if National Defence had taken security more seriously at the outset. Given the strategic importance of the information and assets held by National Defence, it should be a leader in ensuring security rather than a laggard.

Lastly, the Committee notes that the Treasury Board Secretariat needs to take responsibility for ensuring that Treasury Board policies are clear, departments understand their obligations under those policies, and departments are in fact following those policies.

ADDENDUM

The House of Commons Standing Committee on Public Accounts Committee began its study of the Auditor General's October 2007 audit on Safeguarding Government Information and Assets in Contracting in February 2008, and held a subsequent hearing on the issue in June 2008. Due to the dissolution of Parliament in September 2008 for an election, the Committee was unable to present its report on the issue in the House of Commons. When the Committee was reconstituted in the 40th Parliament, it did not want to lose its work on this important issue and thus brought the study forward. As a significant amount of time had passed, the Committee asked the organizations involved to provide an update on actions taken in response to the audit. Treasury Board of Canada Secretariat, Public Works and Government Services Canada, the Department of National Defence, and Defence Construction Canada provided information to the Committee during the summer of 2009. As the Committee does not want to alter the original intention of its report based on the audit and the evidence heard, the information received is included in this addendum to the report.

In its submission to the Committee, Treasury Board of Canada Secretariat noted that the Government Security Policy, which is now referred to as the Policy on Government Security, was renewed and came into effect on 1 July 2009. The government has also created two associated directives: the Directive on Departmental Security Management and the Directive on Identity Management. According to the Secretariat, these instruments have addressed previous ambiguities in language and accountabilities have been clarified. In August 2008, the Secretariat issued the Security Policy Implementation Notice, which clarifies direction on interpreting the existing standard with respect to using the Security Requirements Checklist and identifies the responsibility of Departmental Security Officers for performance measurement and evaluation. Lastly, the Secretariat incorporated the Security and Business Continuity indicator into the Management Accountability Framework in 2007-2008.

Public Works and Government Services Canada (PWGSC) provided an update to its action plan. Almost all of the elements of this action plan have been completed. Of note is that PWGSC plans to move to cost-recovery for the Industrial Security Program beginning on 1 April 2010, and a third party review of the Program was completed on 31 March 2008. Work is continuing on certification of the information technology environment.

According to the update provided by the Department of National Defence, all of its actions are completed, including updating the Departmental Security Manual and the Procurement Administration Manual, as well as reviewing 100 randomly chosen construction and maintenance contracts between 2002 and 2007. The Department was waiting to release updates to its Departmental Security Policy until the Government Security Policy had been released.

Defence Construction Canada informed the Committee that it had signed an updated Memorandum of Understanding with the Department of National Defence on 2 June 2008, which includes a section to ensure that security requirements are identified and managed through the contracting process. Additionally, a special examination of the Corporation conducted by the Office of the Auditor General found that the Corporation had taken “strong action,” and would need to closely monitor the effectiveness of its security actions. Lastly, the Corporation engaged its internal auditor to conduct an audit of industrial security, which concluded that the Corporation had completed all of the tasks set out in its security action plan.

APPENDIX A
LIST OF WITNESSES

Organizations and Individuals	Date	Meeting
39th Parliament, 2nd Session		
Defence Construction Canada	2008/02/26	17
Ross Nicholls, President and Chief Executive Officer		
Department of National Defence		
Glynn Hines, Chief of Staff Office of the Assistant Deputy Minister, Information Management		
Dave Shuster, Director Deputy Provost Marshal Security		
Scott Stevenson, Assistant Deputy Minister Infrastructure and Environment		
Department of Public Works and Government Services		
Gerry Deneault, Director General Industrial Security Sector		
François Guimont, Deputy Minister and Deputy Receiver General for Canada		
Office of the Auditor General of Canada		
Sheila Fraser, Auditor General of Canada		
Treasury Board Secretariat		
Ken Cochrane, Chief Information Officer		
Defence Construction Canada	2008/06/03	36
Ross Nicholls, President and Chief Executive Officer		
Department of National Defence		
Michael Day, Commander Canadian Special Operations Forces Command		
Robert Fonberg, Deputy Minister		
Glynn Hines, Chief of Staff Office of the Assistant Deputy Minister, Information Management		
WalterJ. Natynczyk, Vice-Chief of the Defence Staff		
Dan Ross, Assistant Deputy Minister (Materiel)		
Dave Shuster, Director Deputy Provost Marshal Security		
Scott Stevenson, Assistant Deputy Minister Infrastructure and Environment		
Office of the Auditor General of Canada		
Sheila Fraser, Auditor General of Canada		
Hugh McRoberts, Assistant Auditor General		
Bruce Sloan, Principal		

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the Committee requests that the government table a comprehensive response to this Report.

A copy of the relevant Minutes of Proceedings (40th Parliament, 3rd Session: Meeting No 2; 40th Parliament, 2nd Session: Meeting No. 43); 39th Parliament, 2nd Session: Meetings Nos. 17 and 36) is tabled.

Respectfully submitted,

Hon. Shawn Murphy, MP

Chair