House of Commons
CANADA

Standing Committee on Public Accounts

PACP • NUMBER 017 • 2nd SESSION • 39th PARLIAMENT

EVIDENCE

Tuesday, February 26, 2008

Chair

The Honourable Shawn Murphy

Standing Committee on Public Accounts

Tuesday, February 26, 2008

● (1115)

[*English*]

The Chair (Hon. Shawn Murphy (Charlottetown, Lib.)): I'd like to call the meeting to order.

I want to extend to everyone here a very warm welcome. We have a large crowd here this morning, so hopefully everyone is comfortably seated and in their places.

Ladies and gentlemen, we are here today, pursuant to Standing Order 198(3)(g), to discuss chapter 1, "Safeguarding Government Information and Assets in Contracting", of the October 2007 *Report of the Auditor General of Canada*.

We are pleased to have with us the Auditor General of Canada, Sheila Fraser. She is accompanied by the assistant auditor, Ronnie Campbell; and principal, Bruce Sloan.

From the Department of Public Works and Government Services we have the accounting officer, François Guimont. He is accompanied by Jane Meyboom-Hardy, the assistant deputy minister; and Gerry Deneault, the director general, industrial security sector.

From Defence Construction Canada we have Mr. Ross Nicholls, president and chief executive officer.

From the Department of National Defence we have Scott Stevenson, acting assistant deputy minister. We have Major-General Glynne Hines, chief of staff, assistant deputy minister, information management; and Lieutenant-Colonel Dave Shuster, director, deputy provost marshal, security.

From the Treasury Board Secretariat we have Mr. Ken Cochrane, chief information officer. He is accompanied by Mr. Pierre Boucher, senior director, identity management and security.

As I said, we have a very large crowd. They're not all at the table, but they can be called to the table should the need arise. Hopefully everyone is ready to go.

Mr. Williams.

Mr. John Williams (Edmonton—St. Albert, CPC): On a point of order, Mr. Chairman, I have a letter here addressed to you from the Minister of Public Safety regarding your letter to him and Commissioner Elliot, and a response on the Canadian Firearms Centre and the information system. As you know, I always think these things should be entered into the minutes, so if anybody wants to know what happened to any response to your letter—they didn't ignore us—we finally got it six months later. Here it is.

The Chair: Thank you very much, Mr. Williams.

Mrs. Fraser, I understand you have some opening comments, so I'm going to turn the floor over to you.

Ms. Sheila Fraser (Auditor General of Canada, Office of the Auditor General of Canada): Thank you, Mr. Chair.

We thank you for this opportunity to present the results of chapter 1 of our October 2007 report, entitled "Safeguarding Government Information and Assets in Contracting".

Joining me today are Ronnie Campbell, assistant auditor general, and Bruce Sloan, senior principal, who were responsible for this audit.

The Government of Canada's ability to protect sensitive information and assets it entrusts to Canadian industry is critical to ensuring the health, safety, security, and economic well-being of Canadians, both at home and abroad. This ability is also important for maintaining Canada's international reputation and ensuring the continued growth of international trade.

[*Translation*]

We found serious weaknesses at almost all levels in the processes set up to ensure the security of government information in assets entrusted to industry. These weaknesses range from incomplete policies, an unclear mandate, poorly defined roles and responsibilities for industrial security, to a willingness of some officials to circumvent key security procedures in order to reduce costs and avoid delays in completing projects.

We found that many who play a role in industrial security are not sure of their responsibilities. All stages of the process rely on the assumption that the proper procedures were followed at the earlier stages, but there are few mechanisms to provide assurance that this is so.

[*English*]

As a result of weaknesses in the system, many federal contracts providing access to sensitive government information and assets have been awarded to contractors whose personnel and facilities had not been cleared to the appropriate security levels. These include a number of contracts awarded by the Department of Public Works and Government Services on behalf of other government departments, and thousands of contracts for national defence construction and maintenance projects awarded by Defence Construction Canada.

Of particular concern was the failure by officials at National Defence to properly incorporate contract security requirements for the construction of the above-ground complex in North Bay, Ontario. Contracts for this project were awarded by Defence Construction Canada to unscreened contractors. As a result, Canadian and foreign workers had virtually unlimited access to the construction plans and the construction site.

[*Translation*]

I am pleased to note that Defence Construction Canada has begun to address some of the issues raised in our report. We received a detailed management action plan that outlines the actions the entity will take to address our recommendations. The committee may wish to ask the entity about the progress it has made.

National Defence has also provided us with an action plan to address our recommendations. The committee may wish to ask the department what progress has been made to date and what steps have been taken to ensure that the NORAD above-ground complex can be used for its intended purpose.

PWGSC's Industrial Security Program plays a major role in ensuring that contracts with security requirements comply with the government security policy. We found that the program's operating procedures were in draft form and did not cover key activities essential to ensuring security in contracting . In addition, the program did not have stable funding, thus limiting its ability to hire and retain enough qualified security professionals.

● (1120)

[*English*]

I'm very pleased to note that Public Works and Government Services Canada has provided us with its management action plan. Although we have not audited the plan, we did review it. We believe that if it is carried out, the plan should address the concerns raised in our report. The committee may wish to ask the department about its strategies and the progress it has made to date, particularly its progress in obtaining stable funding for the program.

We found that the government did not know to what extent it is exposed to risks as a result of less than adequate industrial security. A concerted effort to strengthen accountability, to clarify policies, and to better define roles and responsibilities for security in contracting is required to help reduce these potential risks to the national interest.

Mr. Chair, this concludes my opening statement. We would be pleased to answer any questions the committee members may have.

Thank you.

The Chair: Thank you very much, Ms. Fraser.

Before going to Mr. Guimont, I want to point out that we were exceptionally late starting this meeting, so I plan to go until a quarter after one due to the importance of the meeting.

I understand, Mr. Guimont, you have an opening statement. Go ahead.

[*Translation*]

Mr. François Guimont (Deputy Minister, Department of Public Works and Government Services): Mr. Chair, members of the committee, thank you for this opportunity to appear before you today.

The Industrial Security Program plays an important role in keeping government information and assets secure when these are entrusted to the private sector as a result of a government contract. In a nutshell, we do this by screening individuals and firms for all contracts for which PWGSC is the contracting authority, and when requested by other government departments exercising their own contracting authority.

The program processes about 2,000 security-related contracts a year, 75 % for which PWGSC is the contracting authority. We carry out this role for federal contracts and for contracts awarded to Canadian firms by the foreign governments with which we have security agreements.

While PWGSC is not the only department to perform contract security functions, as the main purchasing arm of the Government of Canada we handle many large contracts involving sensitive information and assets.

I was briefed on the initial observations and findings of the Auditor General last June, shortly after I began my duties as deputy minister of PWGSC. As the accounting officer, I took these observations seriously and began work in earnest to address the concerns raised. We did not wait until the Auditor General tabled her report.

[*English*]

Let me say before going any further that we agree with all of the Auditor General's recommendations. Our action plan has been reviewed by the Auditor General and tabled with the committee. It has four key elements that directly address her concerns.

First, we instituted a certification process to ensure that client departments clearly identify for every contract request whether there is a security requirement or not.

Second, we completed and issued an industrial security standard operating procedure that has been in draft form, and we train our people to ensure it is consistently followed.

Third, the industrial security program's information and technology systems were certified as mandated under government security policy.

Fourth, our business continuity plan now calls for daily, rather than weekly, backup of our security data.

Furthermore, recognizing the program's importance, we took additional steps. The program is undergoing an independent third party management review of its mandate, roles and responsibilities, and program delivery to be completed by March 31. IT upgrades are being made to improve the exchange of information between the department's contracting and security systems. And an advisory board comprising senior officials with experience in the security area has been struck to provide advice on the direction and policies of the program and to advance coordination and improvement of contract security across government. It held its first meeting in January.

We are also conducting a detailed review of all 3,000 current contracts with security requirements to verify that the program has fulfilled its security obligations. This review will be completed some time in August.

● (1125)

[*Translation*]

Finally, on the issue of resources to fully carry out the program's activities, the department has, year over year, reallocated resources on top of the existing base. In 2007-2008, an additional $11.2 million was allocated to contract security-related activities.

I am working diligently with my colleagues at Treasury Board Secretariat and the Privy Council Office to secure an increase in our permanent funding base for the program.

Thank you, Mr. Chair. I would be happy to answer your questions.

The Chair: Thank you very much, Mr. Guimont.

[*English*]

Mr. Nicholls, I understand you have some opening comments.

[*Translation*]

Mr. Ross Nicholls (President and Chief Executive Officer, Defence Construction Canada): Mr. Chair, honourable committee members, I am very pleased to be able to speak to you today. As some of you are not very familiar with Defence Construction Canada, I would like to take this opportunity to tell you a bit more about the company.

[*English*]

Defence Construction's mandate pursuant to the Defence Production Act is to deliver defence projects related to physical infrastructure. The corporation's been doing this for 56 years and has developed a recognized expertise in real property contracting, contract management, and in certain related areas.

Defence Construction supports the Canadian Forces and the Department of National Defence in meeting their operational requirements at site, across Canada and abroad. We currently have an office in Afghanistan supporting the mission there.

The management of industrial security for defence projects is a joint responsibility of National Defence and Defence Construction. We are accountable for ensuring the security of sensitive information and assets once the security requirements have been identified by the Department of National Defence. 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. Defence Construction uses the industrial security division of Public Works and Government Services Canada to provide the contractual clauses appropriate for identified security requirements and to process clearances for individuals and firms that are contracted to work on defence projects.

Defence Construction proactively implemented procedures to strengthen its management of industrial security during the Auditor General's audit activity. When the report was published, we accepted her recommendations to further strengthen the security management framework.

As Madam Fraser pointed out, Defence Construction shared with her its action plan to deal with her recommendations, and the plan was made available to the committee in advance of this meeting.

I would be very pleased to discuss our progress against this plan or any other aspect of the report that interests members. I'm confident that Defence Construction does its part as an integral member of Canada's defence and security team to safeguard sensitive assets and information related to defence projects.

Thank you.

The Chair: Thank you very much, Mr. Nicholls.

We're now going to hear from Mr. Scott Stevenson, the acting assistant deputy minister of the Department of National Defence. Mr. Stevenson.

Mr. Scott Stevenson (Acting Assistant Deputy Minister, Infrastructure and Environment, Department of National Defence): Thank you, Mr. Chairman.

Mr. Chairman and members of the committee, thank you very much for the invitation to brief you today on the Department of National Defence's response to the Auditor General's October 2007 audit of security and contracting.

As you know, my name is Scott Stevenson and I'm the acting assistant deputy minister for infrastructure and environment. I'm joined today by Major-General Glynne Hines, the chief of staff of the information management group at National Defence, and our departmental security officer, Lieutenant Colonel Dave Shuster.

As you know, the audit contained two recommendations directed at National Defence. The first recommendation involved ensuring that our industrial security policies and procedures are up to date and complete and that they accurately reflect our roles and responsibilities under government security policy.

[*Translation*]

The second recommendation states that we should establish an integrated framework for managing industrial security on defence projects.

In the time given me today, I would like to give you an outline of the measures that have already been adopted by National Defence to follow up on those two points.

[*English*]

We have already drafted a new industrial security chapter for our departmental security manual. At the same time, our departmental security officer is working with stakeholders within the department and other government departments to ensure that our adjustable security policy and procedures are consistent with government security policy.

Mr. Chairman, this will help to address any current misconceptions or ambiguities on the part of project authorities.

● (1130)

[*Translation*]

We have also reviewed our procurement administration manual, which details our departmental procurement procedures. The responsibility of procurement and contracting authorities to identify security requirements in any procurement activity has been explicitly defined. These changes will also be reflected in our project approval guide.

[*English*]

To ensure coherence within the department, we have established a working group, co-chaired by senior managers responsible for material acquisition and construction, to ensure that our procurement policies and procedures are both workable and consistent with government security policy.

In order to improve security awareness at all levels, we are developing a new unit security supervisor course, which will include an industrial security module. The information contained in this module will be widely communicated across the department, which will further mitigate any potential misunderstanding or misapplication of the departmental security policy and the procedures relating to the contracting process.

[*Translation*]

The department has initiated staffing action to improve oversight and compliance with our industrial security program. The additional manpower will permit us to implement a regular verification program, and we are also investigating improvements to our information systems in order to enhance oversight.

[*English*]

Finally, we are working with Defence Construction Canada, which acts as the contracting authority for the majority of defence construction projects, in order to develop an integrated framework to ensure that security requirements are met during all phases of the contractual process.

I have just outlined a number of specific actions the department has undertaken or will undertake to address the concerns raised by the audit. I can assure you that the Department of National Defence is committed to ensuring that sensitive information and assets entrusted to industry through contracting are properly safeguarded. As a result of the Auditor General's report, the Department of National Defence is making significant improvements to our security provisions.

Thank you, Mr. Chairman.

The Chair: Thank you very much.

We're now going to hear from the Treasury Board Secretariat, Mr. Ken Cochrane, who is the chief information officer.

Mr. Ken Cochrane (Chief Information Officer, Treasury Board Secretariat): Thank you, Mr. Chair, and good morning, committee members.

Thank you for the invitation to appear before your committee today to discuss the Auditor General's chapter on safeguarding government information and assets in contracting.

In chapter 1 of her 2007 report, the Auditor General makes several recommendations aimed at the Treasury Board Secretariat. We have taken action to address those concerns through our review of all management policies, known as “policy suite renewal”. My remarks today will highlight the progress we are making in this matter.

As part of policy suite renewal, the policy, standards, and guidelines on government security are currently under review, which should be competed before the end of this year. We are addressing the Auditor General's recommendations under three overarching themes.

Firstly, 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. By putting the burden of certifying the security requirements on the originator versus the contracting authority, we will increase the accountability of the group requesting the service, which has better knowledge of the specific security requirements.

Secondly, responding to another important recommendation of the Auditor General, the Treasury Board Secretariat will also require that departmental security officers implement quality assurance procedures. These procedures will be put into force by all departments and agencies and will provide for the ongoing review of contract files to ensure that they meet industrial security requirements.

Thirdly, through the renewed government security policy, standards, and guidelines, the Treasury Board Secretariat will ensure that deputy ministers have the information they need to satisfy themselves that they are fulfilling their accountabilities under the policy. Furthermore, 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.

The management accountability framework now provides for the assessment of departments' performance and effectiveness in safeguarding information, assets, and employees, as well as in ensuring the continued availability of critical services. We will assess key policy elements and ensure that security programs and systems of coordination are in place across government and that they are being administered effectively.

As we move forward in developing our new policy and standards, we are working closely with institutions to clarify requirements and guarantee that sound management practices for safeguarding government information and assets in contracting are in place.

This concludes my remarks. At this time, I would be pleased to answer questions that the committee has.

● (1135)

The Chair: Thank you very much, Mr. Cochrane.

Mr. Sweet.

Mr. David Sweet (Ancaster—Dundas—Flamborough—Westdale, CPC): Mr. Chair, this is a complex chapter, as it is, and I don't have any comments by Mr. Nicholls or Mr. Cochrane. Do we have copies of those?

The Chair: Mr. Sweet, I believe the staff is in the process of handing them out. You should have them momentarily. It's unfortunate that the meeting ahead of ours went over time.

I want to thank all the presenters. We're going to start with the first round of seven minutes.

Before we start, I would again urge all members of the committee to keep their questions relevant and to the point, and I urge all witnesses to keep their answers concise and relevant to the question being asked.

Mr. Wrzesnewskyj, you have seven minutes.

Mr. Borys Wrzesnewskyj (Etobicoke Centre, Lib.): Thank you, Chair.

I note that in chapter 1, exhibit 1.1, the Auditor General lists off the roles and responsibilities for security in contracting, and that every government department appoints a departmental security officer to establish and direct a security program.

Mr. Shuster, would you be that individual in Defence?

LCol Dave Shuster (Director, Deputy Provost Marshal Security, Department of National Defence): Yes, I am.

Mr. Borys Wrzesnewskyj: Okay.

She went on to state that you would conduct active monitoring and internal audits of security programs, including security in contracting, and report the results to the Treasury Board of Canada Secretariat.

Now, Ms. Fraser, on page 2 of your report, under the subheading, “What we found”, you stated that during one major project you found a willingness on the part of National Defence officials to circumvent key security-related procedures. Later in the chapter, you refer to the NORAD above-ground project. Is that the one you're referring to?

Ms. Sheila Fraser: Yes, that is correct, Chair.

Mr. Borys Wrzesnewskyj: Thank you.

Mr. Shuster, would that statement refer to you? Are you one of those key National Defence officials with a willingness to circumvent security-related procedures?

LCol Dave Shuster: No, I am not.

Mr. Borys Wrzesnewskyj: Ms. Fraser, to whom would that refer?

Ms. Sheila Fraser: If I could clarify this, Chair, it would not be the departmental security officer, but the people managing the specific project, and there would be separate responsibilities from the departmentals who were there.

Mr. Borys Wrzesnewskyj: I understand that at the time of the audit there had still not been a security checklist filled out for this particular highly secure, sensitive project.

Ms. Sheila Fraser: That is correct.

Mr. Borys Wrzesnewskyj: Mr. Shuster, this is probably one of the most highly secure projects you would have been involved in. Why was there no security checklist completed?

LCol Dave Shuster: If I can, I'd like to pass that question over to Major-General Hines, who is actually our subject matter expert on the above-ground complex.

Major-General Glynne Hines (Chief of Staff, Assistant Deputy Minister, Information Management, Department of National Defence): Mr. Chair, as far as the above-ground complex in North Bay goes, the original design was conceived in the late 1990s and the tendering process went on in the 2002 and beyond timeframe. 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.

Mr. Borys Wrzesnewskyj: So by the time this audit was done, sir, there still wasn't a security checklist. Either the Auditor General's statement is misleading, or you didn't get the job done in terms of the security checklist. It's one or the other.

● (1140)

MGen Glynne Hines: There was not a security requirements checklist required at that point of the construction. Appropriate security measures were taken once the building envelope had been completed and the building became a sensitive area from an operational standpoint. The contractors—

Mr. Borys Wrzesnewskyj: If I may, because we are short of time, I'll just jump back to Mr. Shuster.

Mr. Shuster, you are in charge. You are the officer in charge, and in paragraph 1.73 the Auditor General says that since 2002, out of 8,500 projects, 99% have not provided security checklists.

How did that slip by you, or will you refer this back to Mr. Hines?

LCol Dave Shuster: I'd actually probably refer it back to Mr. Stevenson to refer specifically to those 8,500 files.

Now, I'm in charge of administering the security program for the department, and whether or not the project-initiating authority actually submits a security requirements checklist is at the discretion of the project-initiating authority. So in some cases we don't necessarily know in my office that a project is even ongoing at a small base, if it's a maintenance project—

Mr. Borys Wrzesnewskyj: Mr. Shuster, you said at the discretion, I guess, of those below you in the hierarchy, and in 99% of the cases they used their discretion and decided that for these particular defence contracts it wasn't necessary to do these security checklists. The Auditor General referred to willingness on the part of Defence officials to circumvent. You use slightly different terminology. Could I get clarification on that?

Mr. Scott Stevenson: Mr. Chairman, if I may respond to that and help put the question and the observation about the 8,500 contracts between 2002 and 2007 into context, National Defence has more than 20,000 buildings, more than 13,000 works, and more than 5,000 kilometres of roads, so the construction and upkeep of those are what generates the volume of contracting.

A fraction of that has a security requirement, and I can tell you, sir, that as part of the action plan to follow up on the audit, we're reviewing those contracts to determine where there may have been any weaknesses in terms of security procedure and in fact in terms of security impacts, and so we're following up on those.

Mr. Borys Wrzesnewskyj: It's encouraging to hear that there's follow-up, but these numbers are incredibly discouraging, and the previous answers are somewhat discouraging as well because they didn't seem to indicate an acceptance of responsibility, especially in the case of this NORAD contract and what should have been one of our most secure facilities.

I understand that the facility required additional contracting and modifications so that it could be used for its intended purposes. What is the cost now of those modifications since proper security did not occur? It also says that there were foreign contractors involved in this. Who were some of the foreign contractors? Do we know?

MGen Glynne Hines: I can answer that, or at least the first part of that question, Mr. Chairman.

The NORAD facility is currently being used for its intended purpose, without any restrictions. As far as the cost of the building goes, it is my understanding, and I would have to refer to Mr. Stevenson—

Mr. Borys Wrzesnewskyj: What about the costs for the security lapses?

MGen Glynne Hines: There are no additional costs for the security lapses. There were additional security measures taken in that building that are consistent with the evolving threat. If we go back to when this building was designed in the late 1990s, subsequent to the contracting for that facility and the commissioning of that facility as a NORAD air defence centre, the threat has changed. The threat to North America, the threat that NORAD is responding to, has changed, and that has required some additional measures to be taken from an operational perspective, not related to the security of the building.

Those changes in the operational posture of that building, as a result of the post-9/11 environment that we're working in, warranted a number of both physical and technical means to be put in place to ensure the continued integrity of that facility. Those means were put in place before the building was commissioned for use by NORAD and the Canadian Air Defence Sector, and they continue to be in place and monitored today.

● (1145)

The Chair: Thank you very much, Mr. Wrzesnewskyj.

Monsieur Laforest, pour sept minutes, s'il vous plaît.

[*Translation*]

Mr. Jean-Yves Laforest (Saint-Maurice—Champlain, BQ): Thank you, Mr. Chair.

Good day to you all.

Madam Fraser, on page 3 of your report, in the section entitled "What we found", it is stated that:

> They also include thousands of contracts for national defence construction and maintenance projects across Canada awarded by Defence Construction Canada [...] It is not known to what extent government information and assets may have been exposed to risk and who is accountable for that risk.

What is stated in that paragraph is quite significant. If you do not know the extent of the risk, that means that Defence Construction Canada and the defence department were not able to give you the information that would have allowed you to assess whether there were risks or not. My predecessor spoke about the construction of a NORAD centre in North Bay. This all appears to be of some concern.

From the responses you have received to date, what has led you to conclude that there was no risk? Are there still risks out there? Is that something you can eliminate?

Ms. Sheila Fraser: Thank you, Mr. Chairman.

In the course of the audit, we noted that for the majority of construction contracts, the check list or security control list had not been completed. That was not a requirement. We believe that an analysis must be done and that there needs to be some form of assurance that an analysis was conducted. However, someone decided that additional security measures were not needed. In fact, we do not know why there is no check list; it could be because additional security measures are not needed or because of an oversight.

There was some confusion between the roles and responsibilities of Defence Construction Canada and those of the department. Who is truly responsible? Today, the corporation indicated that the responsibility to determine the security needs rested with National Defence, and that they, obviously, build according to the plans and requirements set out by the department.

We recommend that the check list be completed for all projects and that, even in those cases where there are no additional or heightened security needs, that be clearly indicated, in order to ensure that someone has reviewed the project and then come to that conclusion.

We reviewed the action plans and they seemed to be appropriate. If the measures are taken, they will satisfy our recommendations. Of course, we will have to conduct an audit at a later date to ensure that the actions have indeed been implemented.

Mr. Jean-Yves Laforest: Can you exclude the possibility that security was breached?

Ms. Sheila Fraser: In our opinion, there is a risk that security was breached.

Mr. Jean-Yves Laforest: So, risk is still present.

Ms. Sheila Fraser: We have no assurance for projects that were carried out in the past. For example, we see that work has started on a number of contracts, even with contracts classified "secret", without all the clearances having been completed. We are talking about several months of work. In other cases, there was no security assessment. Needless to say, in such cases, security might have been compromised.

Mr. Jean-Yves Laforest: My next question is for National Defence officials.

In the same report, the auditors indicated that National Defence was concerned that the lengthy security authorization process might delay the awarding of contracts, and therefore their completion. That is what some people told the Auditor General. You can read that in section 1.77. What is the policy at the Department of National Defence? Should security not come before everything else? National Defence officials say they fear it might delay the work, but it seems to me that every means available should be used to ensure that things are done in a very secure manner, even if that means project delays.

Earlier, Ms. Fraser indicated that Canadian and foreign workers had had access to plans as part of the NORAD project, among others. Are there other similar examples? Could it be that, in other cases, people were not asked to submit to security checks, and that they were able to gain knowledge of National Defence plans?

● (1150)

Mr. Scott Stevenson: Mr. Chair, as I said earlier, the Minister of National Defence has accepted all of the Auditor General's findings, whether regarding the North Bay project or those of a more general nature. We are taking this very seriously.

The paragraph you mentioned, Mr. Laforest, states that the other security measures were taken. Security guards escorted those contractors who had not received clearances. So, all other measures were taken. We did take good note of these issues, however, and our action plan states that measures are being taken to correct the problem.

Mr. Jean-Yves Laforest: I'll take your word for future projects, but can you state beyond any reasonable doubt that for projects carried out in the past, including the NORAD site in North Bay, there were absolutely no security problems? Can you assert that?

Mr. Scott Stevenson: We are reviewing all those contracts as part of our action plan. We have begun to...

Mr. Jean-Yves Laforest: I am not talking about the action plan for the future, but about past events.

Mr. Scott Stevenson: The Department of National Defence had and still has a multi-party security program. This means that everywhere National Defence is present, whether in Canada or abroad, a security system is in place.

Mr. Shuster is a key element of that system, but there are also military police officers and members of each unit's security services. If and when problems occur, a system is in place to identify and remediate them. That is all part of risk management, which is a component of the government's security framework policy. That is part of the program that we are continuing to implement.

Mr. Jean-Yves Laforest: Thank you.

[*English*]

The Chair: One more question.

[*Translation*]

Mr. Jean-Yves Laforest: That doesn't quite answer my question regarding past projects. In the case of those projects that were completed and which the Office of the Auditor General examined, can you or your colleagues assert that there were no security problems and that such an assumption can be excluded? Ms. Fraser raised an issue with quite significant security implications. Regarding the construction projects carried out in North Bay, can you reassure us and affirm that despite Ms. Fraser's reservations there were no security problems? Can you assert that?

Mr. Scott Stevenson: Coming up with an answer to that question is one of the goals of our action plan. Most of the 8,500 projects I spoke about deal with things like home roofing. We are looking to find an answer to that question.

Mr. Jean-Yves Laforest: You are still assessing all that.

Mr. Scott Stevenson: That is correct, sir.

Mr. Jean-Yves Laforest: Thank you.

[*English*]

The Chair: *Merci beaucoup, monsieur Laforest.*

Mr. Sweet, you have seven minutes.

Mr. David Sweet: Thank you, Mr. Chairman.

Thank you, Mr. Guimont, and Mr. Nicholls as well, for the proactive way you have addressed many of the concerns in sending the plans over.

There are two things that have been touched on, so I'd just like to clear them up.

Mr. Stevenson, Mr. Wrzesnewskyj was asking you some questions regarding an observation that the Auditor General made, that 99% of the contracts didn't have a checklist. It sounded to me like you put some clarity to it. You were saying that these were all the contracts that were issued, and a vast majority of them would not have had any security element.

Is that what you're saying?

● (1155)

Mr. Scott Stevenson: That's correct.

Mr. David Sweet: Mr. Hines, there were also questions around the NORAD complex. Is it being used right now? Could you tell me if it is being used for its intended purpose, as it was originally planned. Are our partners, basically the United States, happy with the facility?

MGen Glynne Hines: Yes, sir.

Earlier last year the facility was occupied by the military members from the Canadian Air Defence Sector. They are conducting the NORAD mission from there. The United States Air Force and the Department of Defense in the U.S. did their own independent inspection of the facility to warrant that it was suitable for the installation of their sensitive information systems, as is the norm in any of the facilities they use that we share in the domestic role. They did their inspections, they were satisfied, and they have given us the authority to operate their systems within the NORAD facility in North Bay.

Mr. David Sweet: Thank you.

Mr. Guimont, in your opening statement you mentioned that one of the parts of your action plan was to institute a certification process to ensure that client departments clearly identify, for every contract request, whether there's a security requirement or not. So this certification, I'm assuming, would mean that if they certify there is no security element, then they would not have to hand in a checklist. If they say that there is, then you would demand a checklist.

Is that correct?

Mr. François Guimont: Yes. Essentially, yes, from now on. We started that some months ago through an amendment to our form. They have to clearly indicate that in this contract there is no requirement. Before, that was not done, and it led to confusion. This is now done systematically.

Mr. David Sweet: The tone of a lot of the report is that departments need to comply with PWGSC. There's an element here where that's not happening. Do you feel you have the right to overwrite authority to be able to have departments comply now?

Mr. François Guimont: Actually, I would answer the following way.

Departments have to comply with the government's security policy that my colleague Mr. Cochrane spoke about. So it outlines the requirements. They have to have a departmental security officer, we heard in DND, and it's the same thing for Public Works and any other department. So it essentially sets the framework against which they have to be doing business as it relates to security requirements.

We in Public Works generate our own contracts, about 1,500 per annum. Therefore, it is a side of my department in proceeding with contracts—so-called contract authority—that this person has to say there is a requirement. When the requirement is identified, it goes to the industrial securities program segment of my department and things are done.

We also carry out so-called assessment work for departments for about 500 contracts. So per annum overall, for 2,000 contracts, 1,500 were generated by Public Works, and in 500 a department tells us it has a security requirement and would like the industrial security program to carry out the work needed to clear these individuals or companies.

That relationship, by the way, can exist between me and DCC. If DND flags a requirement and DCC says it will look into it, it can do it or come to me and I'll do it on its behalf. That is a sub-segment of the so-called 2,000 contracts we do per annum.

The point I'm making here is that departments have responsibilities under the government security policy. They can come to us in certain cases and we will do it. I generate a fair amount of work myself through the contracts that I issue.

Mr. David Sweet: On page 12, in paragraph 1.26, there's another aspect where you need to demand compliance, and that's from corporate security officers as well. When you're the contract authority and you have a contract with a private sector organization, they assign a corporate security officer. Is that correct? Am I reading that properly?

Mr. François Guimont: Yes, essentially the terminology we use in government is the departmental security officer, and when we deal with a company we call them company security officers. So it has essentially, as an image, pretty much the same responsibilities. When there's a requirement for a company to meet certain demands, we as Public Works expect those demands to be carried out as a point of entry through the company security officers.

So that's the relationship that exists.

Mr. David Sweet: The indication here in the Auditor General's observation is that frankly you don't know whether they're doing their job or not. Does part of your action plan include how you're going to enforce, for the lack of a better word, the compliance of these private contractors as well?

● (1200)

Mr. François Guimont: Yes, I understand your question.

Essentially the point you're making speaks to our enforcement and compliance responsibilities, which are discharged in part through inspections. It's not only that, frankly. The Auditor General did also pick up on certain documentation that was missing. When you look at it, we had an onus to ask the company to provide this information. I'm thinking about the security briefing, the so-called security agreement, but it's also the onus of the company to provide this information proactively.

So I'm not going to start sharing blame here. These documents should have been on file.

Normally our inspections allow us to make sure that the company security officer meets the requirements. I will give you examples. Certain sections of the company, where sensitive information may be dealt with, would have padlocks. Their ID systems will be pressure-tested to certain standards. There will be security officers with badges. I'm giving you examples of requirements that may be part of a contract clause, and we expect the company to discharge that. Our way to check this is through inspections to make sure things are happening the way they should. In the past we've carried on inspections, and we are augmenting that in other inspections that we're carrying on.

Mr. David Sweet: On page 19, there is an issue of funding and also of staffing in paragraph 1.55. It reads: "Senior Officials within the Industrial Security Program informed us that it is difficult for them to attract and retain qualified security professionals." That was attributed because of a lack of funding.

What I would like to know right now is whether, to date, the funding is in place. Are these vacancies being filled now with qualified people?

Mr. François Guimont: This has been at the core of the issues we face in this audit.

To be very clear with you, the basic financial base of that program is about $6.7 million per annum. In my career I've rarely seen a program being doubled by reallocation within a department. I guess someone can point to an exception, I'm sure, but normally a reallocation to a program is a top-up. You add 10% or a 20% because of workload, complexity, or a special project being asked of the manager.

In this case the reallocation, on average, in the last couple of years was $6 million—a $6 million reallocation, a $6.7 million base. What it speaks to is two things. First of all, the program experienced a significant workload increase as a result of 9/11. The second point is more contracting activity as a result of the economy growing.

Nobody should be surprised by that. I don't know what the curve is, but it's normal that as you have a growth in economy you can have more contracts, more activities. So that's another element.

This is compounded by the fact that if you reallocate, you reallocate on a yearly basis. So if I am the manager, I have my base of about $6.7 million, and the department, through the deputy minister, reallocates on a yearly basis about $6 million, but I can't use that base, which is a reallocation, to plan long-term staffing. It creates a vicious circle. The cash is there. The cash can be used, but you're trying to attract talent. You say, "Well, yes, I would like you to come over. We have good important work. It's actually interesting work, to be honest, but I'm giving you 12 months because we're trying to stabilize the workforce and the budget." So it creates a bit of a conundrum, where we try to staff and people come. Because it is a 12-month assignment with a potential window—it's a 12-month assignment vis-à-vis the budget you have that year—people do come and leave.

Secondly, some people have other options than having to work for 12 months. That's another thing. With people leaving, you lose corporate memory. You train them, you prepare them, they do good work, and then they potentially leave. The numbers that the Auditor General picked up are accurate: 28%, 29%, 30%. It's a significant part of the workforce that is unstable, if you wish, in the sense of contributing in a steady fashion to the outcomes they're trying to achieve.

I'm trying to explain here the dynamic vis-à-vis the resources. Now, the answer for me as the accounting officer is to work hard at getting a stable long-term multiple-year base. I've been working at this with Treasury Board, at Privy Council Office.

The Chair: Thank you very much, Mr. Guimont, and thank you, Mr. Sweet.

Mr. Christopherson, seven minutes.

● (1205)

Mr. David Christopherson (Hamilton Centre, NDP): Thank you very much, Chair.

I want to thank all of you for being here today.

I think we all should pay attention to what the Auditor General said in the third paragraph of her comments today. Given where we are in the world and what's going on, this statement, that "We found serious weaknesses at almost all levels in the processes set up to ensure the security of government information and assets entrusted to industry", is a damning one. It would be at any time, but in this day and age I'm just blown away hearing this kind of thing. When I think about all the things the public is being told they are responsible for—that security is everything, that everybody has to be on guard, that we're all supposed to be practically looking over our shoulders—the fact that we have stuff like this going on is absolutely unbelievable and totally unacceptable.

So where do we start here? Let's start with Public Works and Government Services and the industrial security program. How long has that been around?

Mr. François Guimont: Since 1941.

Mr. David Christopherson: Holy smokes! I was getting ready for somebody to say that it was a couple of years old and that's why we're in trouble; 1941 takes my breath away.

Now, during the audit, the auditor reported that the mandate was changed twice during the audit and that standard operating procedures for the program were in draft form and incomplete.

Somebody start talking. The questions are obvious. Somebody please tell me how we could have an audit going on, the mandate changes twice during the course of the audit, we have standard operating procedures in terms of the program but they're in draft form and incomplete—and you tell me it's been around since 1941. Somebody please tell me what's going on.

Mr. François Guimont: Essentially the answer lies in what I explained vis-à-vis resources. We have a program that has not been resourced at the right level.

I think the department really made efforts to top up that budget in a very responsible fashion. To give $6 million, on average, in the last couple of years to a base of $6.7 million is quite telling. It's not like $100,000 or $1 million was given. It was a substantial amount. So that's the first thing.

With regard to your point about draft policies and procedures, frankly this speaks to the fact that people were going to the more pressing and the higher priority. I am not saying that finalizing the procedures and policies is not important, but they did exist. They were in draft form, not finalized. And they have been finalized, very quickly. This was taken on as being a priority, picked up by the OAG—

Mr. David Christopherson: Except that if the Auditor General hadn't done her report, there's a good chance they'd still be out there incomplete.

Mr. François Guimont: I don't really disagree with you, frankly; it's a very good point. As the accounting officer, when I sat down with my staff, I was a bit surprised that since 1941.... But setting that aside, in recent years the program had not been audited, because probably some of these things would have been picked up.

An audit is not a bad thing. An audit says you have problems here and problems there. I'm not going to pass judgment on that. It was not audited. I would like to have seen it audited in the context of a big department. You have a risk-based approach, and someone somewhere—your own people, not the OAG—says you should be looking at that program. I think a lot of these things would have been picked up and corrected.

I just want to leave with you the thought that when people are trying to work in an environment where both the complexity and the workload have increased, they will go to the more pressing. They're trying to do a good job, and things like websites and going from a draft to a final policy will be of lesser priority even if they are, to my mind, important, critical.

There is one last point: it was done, and it was done quickly. They were draft. It's not as if they didn't exist. They were polished up, buffed up, and finalized.

Mr. David Christopherson: I want to get a little more detail, because here's what I'm worried about. If we don't find out how this happens, then how are we going to have assurances that you have mechanisms in place to make sure it doesn't happen again?

I appreciate and respect the fact that it's done and taken care of, but there are some things here we want to get to the bottom of. Again, it's nothing to do with individuals—people move and so on—but it's about positions and systems and processes being in place to adequately protect national security.

I want to go to another issue that was pointed out in the audit. There had been 24 contracts awarded before contractors were given their security clearance. This is under a "secret" level of security clearance. For four of those contracts, the work was completed before the contractor was cleared. How? How can that be?

Mr. François Guimont: I will answer the question—

● (1210)

Mr. David Christopherson: You will, you're right.

Mr. François Guimont: In the same way as I looked at the 24 contracts, I also looked at the overall sample of 86, and quite a number of them were done correctly. It was important to me because I wanted to understand if there was something systemic or systematic in the industrial security program. The answer to that is probably no, because the majority were done correctly.

In the case of those contracts that were done ahead of time—contracts awarded before security clearance was awarded correctly—the OAG picked up that at least in six cases some measures were put in place to mitigate risk. That's the first thing.

In the second phase of our action plan we looked at all those 24 contracts to see if measures had been taken. I know it was after the fact to see if measures had been taken to minimize risk, but for the 24, they had been. In the same way as the OAG looked at six, we looked at the 24. In some cases resources that had access to certain information were escorted; in some other cases the contract had started, but the sensitive information had not been used by the contractor.

Mr. David Christopherson: What would you do if you found out you had serious security problems after the fact? That's the whole point of it. You have these going through at a secret level. It's not like we are talking routine; it has "secret" stamped all over it.

This is mind-boggling. These contractors came in and did the whole job. You say there were some mitigating circumstances, but it wasn't a full security clearance. What if, when you did a full security clearance after the fact, you ran into a situation like the NORAD one? We'll come back to that in a minute, but where would you be then, and who would be responsible?

Mr. François Guimont: To pick up on that point, all 24 contracts were security cleared, so I want to leave that very clear image with you.

What I'm saying here has been said by the OAG. She acknowledges that in all those cases the clearance was given; the issue was totally timing—i.e., the contract was given before clearance—but I want to leave the very clear statement with you that clearances were provided. What I'm telling you is that for the 24 contracts, while it was not perfect because it was clearance after the fact, during that period of time there were mitigating measures. Although they were not perfect, there were mitigating measures.

Mr. David Christopherson: That does not eliminate the possibility that if you do a security review afterwards and you haven't done a full, complete testing and you do it after the fact, you could find things that send you back to square one, having to do God knows what in terms of remedying the problems, up to and including tearing down the damned building if it's serious enough.

Thanks, Chair. I'll be back for another round.

The Chair: Thank you, Mr. Guimont.

Go ahead, Mr. Holland, for seven minutes.

Mr. Mark Holland (Ajax—Pickering, Lib.): Thank you, Mr. Chair.

Thank you to the witnesses.

I'm going to continue on that point because I'm concerned about it and I'm not quite clear on the answers that have been given.

There were four specific examples in which the work was completed prior to the security clearances being issued. In these 24 contracts requiring a secret level of security clearance, the contractors had been awarded the security clearance before this had been done. That is very concerning, and I'm not hearing a lot about how you're going to rectify it. Mr. Christopher rightly asked what could have happened after they awarded this. Yes, they all received security clearance, but what happens if there had been issues? In four cases the work had already been completed, so those issues would only have been caught after the work was completed and everything was done.

This is very serious. It deeply concerns me, and I haven't really heard clearly, Mr. Guimont, how we're going to make sure it doesn't happen again, or a proper addressing of how it could have been allowed to occur in the first place.

Mr. François Guimont: We have the four-phase action plan. We have it addressing, first, all the recommendations made by the OAG. That is done. I'm not talking about a month from now or two months from now; we've done that.

There is one component related to IT that we will have completed sometime next October. This is to have a better cross-log of information between our contracting authority and the industrial security program database, which were disconnected for reasons of security. That is going to be done in October. That is the first phase.

The second phase is that we have looked at the 24 contracts to make sure we were satisfied that we would be at a low risk for breaches of security, and we're satisfied that is the case. The people in the 24 contracts were cleared. After the fact is not the ideal situation, but that is the reality.

On top of that, we've decided to look at active contracts, 3,000 of them, to make sure the elements picked up by the OAG don't replicate themselves into the active contracts. We are proceeding with that. It's a three-stage approach, and it will be completed in August. We are doing this very systematic wall-to-wall approach to make sure we're minimizing risk for the contracts. These measures are in addition to the procedures and policies we're putting in place and the management review we're carrying out on the program overall.

● (1215)

Mr. Mark Holland: This is to Ms. Fraser, because it's very important, obviously—you're hearing this as a solid refrain from the committee—that this doesn't occur again.

Are you satisfied with the actions being taken by Public Works in this matter? Do you feel that the actions they're taking are adequate to ensure that this type of thing doesn't happen again?

Ms. Sheila Fraser: We are certainly pleased with the action plans that have been presented. As was mentioned, we did review the action plan of Public Works, and it does address our recommendations. I say that, of course, under reserve. We will eventually go back and re-audit this to make sure these things are being put in place.

On this particular question, though, it would be easy to say that all the clearances have to be in place before the work begins. But sometimes that isn't the reality. What we would expect in that case is that there would be a very detailed and complete risk mitigation plan, so it would be clear up front that if the clearances aren't all in place, yes, the project may start. But what information do those contractors not get access to? What other risk mitigation techniques would be used until the security clearances come through?

I think that would be the way to probably handle that kind of situation.

Mr. Mark Holland: I would suggest that the committee is going to want to keep a close eye on this as well, to make sure that happens. I think you heard expressed today a lot of concern.

If I could, I'll go to a recent concern, related to this chapter, that was very disturbing. This is to Mr. Guimont. It is with respect to the 138 CDs that were released—in fact, most of them are still out there—which contained detailed corporate information, such as details about pricing and bidding. There were a lot of companies concerned that this would severely damage their ability to do business in Canada.

I want to know if you can tell us where that is right now. How many of these CDs have been brought back in? What work is being done to rectify this situation and to ensure that this doesn't happen again? That is something, as well, that causes a great deal of angst.

Mr. François Guimont: I must admit that I came prepared for this discussion today, so I'm not.... I will go by memory here to the extent possible, if you can bear with me.

The Chair: Mr. Guimont, if you want to, if you feel more comfortable getting back to the member with a written response, you're entitled to do that too.

Mr. François Guimont: I think it would probably be more appropriate, if you don't mind.

I know exactly what you're talking about. I know the file. My level of detail will probably not satisfy your questions.

Mr. Mark Holland: I'd appreciate getting that information. That, too, is something that greatly concerns me. While it doesn't deal specifically with this chapter, I think it is related. I haven't really had a good response to that, and I'm left feeling fairly uncomfortable about it.

The Chair: Will we have that within two weeks, Mr. Guimont?

Mr. François Guimont: Yes.

The Chair: You can file that with the clerk, and he will distribute it to all members.

Mr. Mark Holland: I know that Mr. Wrzesnewskyj is itching to ask questions. I think I have a minute or two left, if he can continue.

There you go.

The Chair: Go ahead, Mr. Wrzesnewskyj.

Mr. Borys Wrzesnewskyj: Thank you, Mr. Holland.

Mr. Hines, has the NORAD facility been compromised, or is it secure?

MGen Glynne Hines: To the best of our knowledge, the facility has not been compromised. We would not be conducting the operations we are conducting from that facility if we had any doubt as to the operational and technical integrity of the above-ground facility.

Mr. Borys Wrzesnewskyj: Let me read you something from page 25 of the Auditor General's report. She states that "National Defence does not know whether information or the building itself has been compromised".

I'm trying to square what I'm reading in the Auditor General's report with what you're telling us. You're telling us that it has not been compromised. And what the Auditor General is telling us in the report is that your officials don't know whether that facility has been compromised.

MGen Glynne Hines: We've conducted extensive physical and technical inspections of the North Bay facility, both during the construction and subsequent to the construction but prior to the commissioning of the facility. We continue to have procedural and technical means to ensure that the integrity of the facility is such that it can be used for its intended purpose.

Mr. Borys Wrzesnewskyj: So you are absolutely secure in your knowledge that the integrity of this facility has not been compromised.

MGen Glynne Hines: Absolutely.

Mr. Borys Wrzesnewskyj: That doesn't match what the Auditor General has stated in her report. And that means we have some sort of problem. Also, in your previous answer you said that some of these processes were evolving, but the Auditor General's report clearly states that on this project, officials circumvented. This wasn't a situation of evolving procedures; it was a circumvention.

How do you respond to that?

● (1220)

MGen Glynne Hines: When the construction contract was awarded, a threat risk assessment was done to determine whether or not the facility required people with security clearances to work on the initial construction phase of the building. It was deemed by the operational authority of the day that it was not required.

Mr. Borys Wrzesnewskyj: No circumvention.

MGen Glynne Hines: There was no circumvention at that point. Subsequently, during the construction of the facility, it was determined that the security measures had to be in place. Security measures were put in place to either have cleared contractors working on the facility or have those contractors working on the facility under escort. As the construction of the facility went on and we got ready to install systems, additional security measures were put in place.

It was a phased approach from the standpoint of starting from bare ground, where there were no security concerns, threats, or risks identified, to the point where systems were installed and the facility became secure and sensitive.

During these processes we continued to do testing through a variety of technical means, and we continued to do physical security inspections to ensure that the integrity of the building was maintained throughout.

The Chair: Thank you very much.

I believe Ms. Fraser has a comment on this issue.

Ms. Sheila Fraser: I hate to do this, but as you are aware, we did a report in May 2007 that commented on the NORAD project. When we did that audit—as we mention in the text box on page 25—there were serious concerns raised by National Defence about the security of that project and the ability to close the below-ground project. They were not sure at that time if they could move all the systems up. I'd be interested to know if that below-ground complex has actually been closed, because that was what the above-ground one was for.

We have summarized in this text box the concerns about whether it could be used for the intended purposes and the access that contractors, both Canadian and foreign, had to the site. When we completed this audit, they indicated that they could, with certain modifications, use the building for the intended purpose.

We had asked for details on what those modifications were. As you will see here, at the time of our audit we did not receive any detailed plans or schedules. All of this text, as is our standard process, has been agreed with by National Defence, and they have agreed with the validity of the facts.

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.

The Chair: Just to bring closure and square the circle here, I'm going to ask Mr. Stevenson to respond to those very serious statements by the Auditor General. I think the committee is owed a response, and I put the onus on you, sir.

Mr. Scott Stevenson: As I stated in response to one of the earlier questions, the department has accepted the findings. That is clear and is normal practice. I would also say that we have accepted the responsibility for resolving any of the shortcomings and weaknesses that are there.

On the specific question as to whether we can prove with 100% certainty, I think that's akin to proving the negative. On that basis we continue to do ongoing security assessments. I think that is a part of the overall approach to security, which is more of a risk management process. To arrive at a position of zero risk is the objective, but it is not necessarily an attainable one.

Mr. Chairman, I'm sorry if I haven't gone as far as what you're looking for.

The Chair: We will move on.

Mr. Poilievre is next for seven minutes.

Mr. Pierre Poilievre (Nepean—Carleton, CPC): On page 10 there is reference to the security and management contracting standard. What is the link between this standard and the government's security policy? How does one relate to the other?

Mr. Ken Cochrane: The government security policy lays out the broad elements of security that departments need to follow. The standard goes in and looks specifically at what is required when we're looking at the contracting of resources. It is a much more focused piece of material. It goes deeper into that information and talks about the requirements departments have to—

● (1225)

Mr. Pierre Poilievre: Do you mean in order to live up to the policy?

Mr. Ken Cochrane: Yes. They must identify if there are security requirements, so that responsibility is clearly with the departments. They need to complete a checklist, if they are going to Public Works, to have Public Works do the contracting for them. If they're doing their own contracting they don't necessarily need to complete a checklist, but they're still responsible for identifying security requirements.

So that's really what it does. It just narrows that and focuses in on that aspect.

Mr. Pierre Poilievre: On page 11 we have: "As an Industrial Security Program client, it accounted for about 37 percent of the contractual and pre-contractual agreements processed by the Program between 1 April 2002 and 31 March 2007."

Who are the other 63% of the clients?

Mr. François Guimont: The Public Works workload is generated by Public Works. I would have to assume that the differential between 100% would be coming from other departments to Public Works for assessment.

Mr. Pierre Poilievre: So these are client departments that have come to Public Works. Are they coming to Public Works to have the entire procurement done? Or are they coming to Public Works to have the security component?

Mr. François Guimont: Security requirement. So essentially what they are asking us to do is this. A requirement is identified, and we carry out either the clearances or the screening and we provide them with the clause that is required in order to cover the requirement that is identified.

Mr. Pierre Poilievre: Is there any good reason why departments shouldn't always use the industrial security program in cases where there is a sensitive contract?

Mr. François Guimont: No good reason that I can think of. Frankly, I've been there for years...and I will look at my colleague Gerry. I would like to think that probably the majority of sensitive contracts emanating from a department come our way for assessment. So most of the highly sensitive ones would.

The Chair: I think it's necessary to bring your colleague to the table. I know we have large crowd. Don't hesitate to bring him up, and we'll make room for him somehow, if you think it's necessary. We can't have people speaking from the audience.

Mr. Pierre Poilievre: So you're saying this 37% is in volume, not necessarily in dollar value. Were these problem contracts my colleagues have already raised managed by the program, or was the security component managed by the department itself—for example, this NORAD project?

Mr. François Guimont: No, this was contained within Defence and DCC, so we were not involved in the NORAD....

Mr. Pierre Poilievre: If the industrial security program had been retained to carry out the security components of that work, do you think we might have avoided some of the problems, at the risk of speculating?

Mr. François Guimont: I would say if a requirement had been identified, the program would have carried out the necessary assessment and clearances and all that. If the requirement had not been identified, we would not have known.

Mr. Pierre Poilievre: Ms. Fraser, are you recommending that all contracts of a sensitive nature use the industrial security program to carry out the security portion of the work?

Ms. Sheila Fraser: We haven't gone that far. We are recommending that this checklist be used and that there be a clear indication of whether a security clearance is required or not. The problem now is that the checklist is optional. So when, for example, the industrial security program gets the checklist indicating that security clearance is required, they carry it out. But if they are never advised or there's no indication, they would not know.

We think there needs to be a better system of clearly identifying if a security clearance is required or not and that this checklist not be optional.

Mr. Pierre Poilievre: On page 12 we have the following quote: "Furthermore, at the time of our audit there were no procedures for verifying that Industrial Security Program staff have received all Security Requirements Checklists from PWGSC's procurement group." Are you indicating that even when the industrial security program is managing the sensitive parts of a project, the checklist is not necessarily being carried out?

● (1230)

Mr. François Guimont: Mr. Chairman, the checking out of the "no requirement", which is what Madam Fraser and I are making reference to, was not a requirement clearly stated in the government security policy. At the time of the audit, we were of the opinion that what we had done—and probably my colleagues around the table would say that as well—was consistent with the intent of the government security policy, and I think the board would probably confirm that. We thought we were consistent.

In the dialogue with the auditors and Madam Fraser, we also concluded that there's nothing like greater certainty. For the purposes of greater certainty, say you don't have a requirement and then you thought about it, so at that time—

Mr. Pierre Poilievre: I think we're getting a little bit off track. I just want to know, are you going to make it mandatory?

Mr. François Guimont: Yes, it is mandatory now.

I was getting there, but I'll cut to the chase. We have already put in our form, in Public Works, a requirement for a "no" box. It's there.

Mr. Pierre Poilievre: Right now, I'm a great lover of the free market, but in this particular case I'm not sure the department should have a free market to use whoever they want within the government to carry out their security requirements in the case of sensitive contracts.

Shouldn't there be one central place where they all have to go when they have sensitive, even security-related contracts to execute? Should we not make it mandatory that we use the program that Public Works has, so that one branch of a procurement-based department can specialize in this highly specialized field and the other departments can take advantage of that specialization? Would that not make more managerial sense?

Mr. Ken Cochrane: Maybe, Mr. Chair, I could respond to this.

You would look at the efficiency within the system and ask that question, which I think is a legitimate one.

One of the things the Treasury Board Secretariat is actually engaged in with Public Works and the PCO is leading an initiative to look at personnel screening across the entire system. As a result of looking at personnel screening—that would be the folks who work inside the government, contractors, and other programs where screening occurs—the opportunity exists for us to look at efficiency. So that's an initiative that's under way. We haven't responded and indicated that we think we should centralize that capability, but it certainly allows us to assess the whole system of screenings in government, because a lot of this has to do with the screening of people and assurance levels to determine how we might want to manage that differently.

So a final decision hasn't been arrived at, but we are looking at it holistically across the government, partially for efficiency but also partially to ensure there are standard approaches to security screening.

The Chair: Thank you very much.

Before we start the first round, I want to follow up with you, Mr. Cochrane, and perhaps also the Auditor General, on the role of the Treasury Board in this whole issue.

When I look at the thing and I read the reports, it looks to me as if there has certainly been a lack of clarity, a lack of interpretation, with this policy. There has been non-compliance in the interest of efficiency, and general confusion.

In fairness, sir, I think since the audit has come out, and probably during the audit, there has been a lot of work done, and perhaps we may be on the right track now, but on government policy, when we look to the administrative arm of government and the Treasury Board to develop the policies and monitor and ensure that the policies are being followed consistently through all departments and agencies, that is, in my view—and I may be wrong—the role of the Treasury Board. This policy seems to have gotten seriously off the rails.

Do you, Mr. Cochrane, on behalf of the Treasury Board, accept any responsibility for this whole problem that has been allowed to develop?

My supplementary question is to the Office of the Auditor General. What role do you see for the Treasury Board in a situation like this, and in your opinion, has Treasury Board been fulfilling its role?

Mr. Cochrane.

Mr. Ken Cochrane: The responsibility of the Treasury Board Secretariat, in many different policy areas, is to fundamentally establish the management policies of the Government of Canada. What we've been doing over the course of the last two years is going through what we call policy suite renewal. The reason for that, I think, is that fundamentally when you look at the range of management policies that existed, there were some 180 management policies in the Government of Canada prior to policy suite renewal. We're actually refining that down to about 44 policies. So one of the jobs is to try to undo this web of rules and clarify what people are responsible for. That's a big part of our role, to try to clarify things much more substantially for departments.

Part of the policy suite renewal is also structuring things so that when you look at the policy you get an instant indication of whether there is something that you need to do for contracting. It's not buried somewhere. It's very clear and consistent that there's something I need to do for physical security.

So I would say that the policy material that was there was probably difficult to work with overall. We're implementing many elements that will add to the controls. One of those is to monitor—that's probably not exactly the right word—or work with departments through the management accountability framework to do regular assessments on an annual basis to determine if the policies are being followed. We can carry that to very deep levels of assurance if we choose to do so.

● (1235)

The Chair: The question was, simply, does Treasury Board accept any responsibility for this problem?

Mr. Ken Cochrane: 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.

The Chair: Ms. Fraser, do you have any comments on the role of Treasury Board? Maybe I'm confused myself. I see them having a vital role in establishing the mentoring and making sure that on a government-wide basis policies regarding the expenditure of funds and contracting are followed.

Do you have any comments in that regard?

Ms. Sheila Fraser: Thank you, Mr. Chair.

This discussion always comes back to the relative weight of responsibilities among the central agencies, the Treasury Board Secretariat and the deputy ministers and their own departments. It is up to the Treasury Board Secretariat to establish those management policies. They should be doing some monitoring, but I think at the end of the day we also have to say that it is up to the departmental heads to make sure their departments are meeting and respecting the policies that are put in place. The burden isn't only on the Treasury Board Secretariat.

Certainly in this case there is confusion in the policy. There was confusion about roles and responsibilities. I think that underlying a lot of the problems was perhaps the lack of—and I hate to use these words—importance or significance that a lot of people put on this whole area. People allowed contracts to go on for 11 months before security clearances were in place. For the program itself, I'm sure those people there did the very best they could, but when half of your funding is the temporary reallocation each year, it's very difficult. I would expect Treasury Board to perhaps ask where programs like those getting these temporary reallocations are.

If you don't have stable funding in government, it's very difficult to run these programs. If you don't have the people there to do the job.... You have to almost commiserate with these people who are trying to do the workload if they have...I think it was 28% vacancy and another 30% who are temporary people.

At the end of the day, I think there were a lot of factors that came into it. Certainly stable funding is one of the major factors in the problems that we saw.

The Chair: Thank you, Ms. Fraser.

We're going to go to the second round of four minutes. I'm going to be quite brutal on time here, gentlemen.

Mr. Hubbard.

Hon. Charles Hubbard (Miramichi, Lib.): I have four minutes?

The Chair: You have four minutes, and it goes by quickly.

Hon. Charles Hubbard: First of all, we heard all of this. Have there been incidents of problems? Are we talking about preventive measures? Can anyone say yes, we've had incidents where there were problems with security? Are we simply working towards prevention?

The second question I have to pose, after listening and watching in many of these, is on efficiency. If DND want a project, and they define it, then they work their way up through Public Works and into Treasury Board and back down to contractors. When we think of the timeframe of efficiency in terms of need and in terms of actually being able to use the asset, could Treasury Board look at that and give to our committee a timeframe of how efficient we are as a government in providing to a department the assets that it needs?

Also, in terms of bidders, in terms of industry we have today ISO qualified, we have nuclear certified, we have all of these. For the contracts issued by Public Works, are the bidders who come in certified to do what you ask them to do? Are you dealing with a lot of contractors who are going to get this qualification after they do the bid?

Maybe Mr. Guimont could identify. Is there a problem? Do we have contractors out there who are not certified, who are not qualified, but who are bidding or wasting our time or the time of the Department of National Defence? Or do we have an efficient system to deal with a fair and transparent bidding process?

● (1240)

Mr. François Guimont: Mr. Chair, essentially the answer falls into two areas.

When a requirement is identified, there's an assessment carried out, and a contract clause is put forward. In order for the successful bidder to be able to get the contract, he or she or the company has to be able to meet the security requirements. That is a requirement. In some cases we do, at the request of certain companies, provide for pre-clearances. That doesn't happen in the majority of cases, but it does happen. Therefore, a potential bidder, on a contract yet to come related to certain security requirements, may say that it's probably a good thing for them to get some clearances, approaches, or industrial securities program, and ask for a clearance. Frankly, we say there's a potential for that company to be a bidder down the road, and we will carry out a process.

Hon. Charles Hubbard: I have a limited amount of time.

There's no requirement in the bidding process for the contractor to be cleared to do the work.

Mr. François Guimont: No, it is only if there's a requirement, but it is not overall.

Hon. Charles Hubbard: DND would have that requirement. I'm surprised that this contract went to North Bay and that companies got involved that weren't certified to do it.

Now, to go a little bit further, we'll say that you have maintenance people working at DND headquarters here in Ottawa. Contracts are given for people to do maintenance. How do you deal with clarifying the security level of people who are going into DND headquarters to do that maintenance work?

Second, you hire casual people through a company here in Ottawa, and those casual people handle some very sensitive information in the IT sector. How is that managed? Within the contracts for maintenance, is there a system for the provision of casual workers who do clerical work? Are we secure in terms of the people who are entering the most sensitive part of the whole National Defence system?

LCol Dave Shuster: Our policy is actually consistent with Treasury Board's policy in the sense that individuals who have access to facilities or information, either at a classified or designated level, require the necessary clearance or reliability status. That depends, again, on the information they would have access to. So if it were even a casual employee coming into a particular job—and normally, if it's casual, it's a reliability screening—that would probably be done, in most cases, through PWGSC. We would ensure that the individual had at least a reliability screening for designated information or the proper security clearance if the person had access to classified information.

The Chair: Mr. Lake, you have four minutes.

Mr. Mike Lake (Edmonton—Mill Woods—Beaumont, CPC): This is a real eye opener for us.

I want to go back to something Mr. Poilievre was talking about earlier, which is the relationship between government security policy and the security and contracting management standard.

My understanding is that the government security policy was issued in 2002. Is that accurate?

Mr. Ken Cochrane: That's the latest version of it.

Mr. Mike Lake: When was it originally implemented?

Mr. Ken Cochrane: It's been through a number of changes over time. I think 1986 was the original timeframe. It was modified in 1986, 1994, and 2002.

Mr. Mike Lake: Now, it says that the current security and contracting management standard predates the government security policy by six years.

Mr. Ken Cochrane: It predates the current version. It was implemented in 1996.

Mr. Mike Lake: It was in 1996. The government security policy was updated in 2002. Yet the security and contracting management standard hasn't been updated since then.

Mr. Ken Cochrane: It was not modified in 2002.

Mr. Mike Lake: Yet my understanding is that the government security policy, from what you were saying earlier, is sort of the big picture, and the security and contracting management standard is sort of the detail within that big picture, in a sense.

How could you update the government security policy immediately post-9/11 and not automatically, as part of that process, update the security and contracting management standard, where the details are, including the checklist we're talking about here? It doesn't make any sense to me. We're sitting here now, five years later, and it says here that “Treasury Board Secretariat has informed us that it plans to update”. So it still hasn't happened. It doesn't make sense.

● (1245)

Mr. Ken Cochrane: A lot of things were changed in 2002 as a result of 9/11. That is one of the reasons the policy was reissued. The policy is the overarching piece that covers many different standards. Many new things went into place, like protection of personnel, identification of assets, and delivery of critical systems. Those all relate to, in many ways, the events of 9/11. IT security was implemented. Some changes were implemented to recognize the changes on the Internet, and so on.

Security screening changed a little bit. Although this particular standard didn't change, the requirement for security screening changed. Initially the standard had been at a basic level, which meant no criminal check. The change that occurred in 2002 was to increase it to include criminal checks. That also covered the contracting standard.

Mr. Mike Lake: I'm also a little bit concerned about Mr. Guimont's comment. I think when we were talking about 24 sensitive contracts, in regard to the 86, I think the quote was that quite a number were done correctly. It seems to me that this would be okay in some circumstances, but when we're dealing with sensitive contracts and the security of our country, I'm not sure that the threshold should be that we have quite a number done correctly. I would rather hear that we're shooting for perfection, not that we're doing okay.

Mr. François Guimont: I agree with you. Frankly I try to look at it as the glass half full, but on sensitive contracts I don't question the point you're making.

In the course of assembling the sample, we did pick one area that was different from high sensitivity. This was secret/top secret. It has to do with protected information, which is different, as you may imagine. It was the same pattern, which is that a contract had been awarded, work had proceeded, and we screened the person to the right protected level: protected B.

The point I'm making is that in certain circumstances there's more risk tolerance. But in other cases, I agree with you. When you're talking secret/top secret, the margin of error for documents missing or not following procedures should be close to zero. Now, that does not bring risk to zero—that's another issue—but our procedure should be followed correctly.

Mr. Mike Lake: I think the big problem is that we're looking at a real ad hoc approach to this. We're talking about various practices evolving over time. I want some assurances on three fronts, that with past, current, and future projects things have changed. For example, I'd like to know how the process is different for a project initiated today from when the Auditor General did her report. What should give us reason to be hopeful and optimistic here?

Mr. François Guimont: It's different in three ways.

First, for those contracts that we generate, our acquisition branch now systematically flags, per a policy, the requirement for security. That is not only done manually, it's going to be done through our IT system. So that's the first thing. We have reinforced the need for that through communication and discussion with our staff.

Second, the program, headed by the director general, is more systematic in making sure that security clearances have been obtained at the time of contract award, which was the issue for the 24 that were singled out. That is the second thing we are doing.

Third, as I said, we're trying to find a long-term resource base that will ensure we have continuity in the program, so that the investments we're making in people and systems today are not lost as people leave.

Mr. Mike Lake: Are those happening today?

Mr. François Guimont: All the recommendations made by the OAG have been implemented. The so-called "requirement for security checklist" is happening. Resources have come from Treasury Board in the amount of $11.2 million, so that has augmented the base of $6.7 million. These things are happening today. This is over and above what we're doing vis-à-vis the active contracts, which is looking into them to make sure they're all okay.

So new contracts are going through what I described, and we're going through past and active contracts very systematically to make sure nothing is missing. That goes back to the point made by Mr. Hubbard in terms of whether we have a level of assurance that things are okay. We're doing that.

● (1250)

The Chair: Thank you, Mr. Lake.

Merci beaucoup, Monsieur Guimont.

Monsieur Lussier.

[*Translation*]

Mr. Marcel Lussier (Brossard—La Prairie, BQ): Thank you, Mr. Chair.

My first question is for Ms. Fraser.

You said that the NORAD situation had changed since last October. In your brief this morning, you still expressed some concerns, i.e., that the NORAD complex could not be used for its intended purposes. Did the information that the Department of National Defence and Mr. Stevenson provide us with this morning on the measures taken alleviate your concerns?

Ms. Sheila Fraser: When we completed our audit, the department indicated to us that a number of measures could be taken to ensure that the facilities could be used for their intended purposes. We asked them what mitigation measures had to be taken, as well as their cost and the plan to be used. We did not have that information at the time of the audit. I trust the word of the department officials, but I would of course like to have more details on the measures that were implemented.

Mr. Marcel Lussier: Very well.

Mr. Stevenson, when do you intend to present the details regarding the measures taken to ensure that the NORAD buildings can be used for their intended purposes?

Mr. Scott Stevenson: Yes.

I was not a party to the discussions on this project involving the Office of the Auditor General and the department. If possible, I would like to gather more information on the key questions that the OAG raises in points 1.74 or 1.75.

Nevertheless, I can tell you that the expected cost of construction was $25.3 million. The final cost of construction was $24.9 million. The project's budget covered all construction costs.

Did the budget provide for additional security expenses? If possible, I would like to provide you with that information at a later date.

Mr. Marcel Lussier: Very well.

Mr. Guimont, it was said that the budget for your staff was very unstable and that there was a lack of continuity. It was also said that 12-month job offers were one of the constraints. Do the new contracts exceed 12 months?

Mr. François Guimont: Until we have a stable funding formula for the program, it will be difficult to establish a multi-year formula. So there will be constraints. Let me be very clear. I want the program to be as stable as possible, but I want to do so within the financial constraints. There has been a new allocation of approximately $6 million, but this, simply put, always impacts other departmental priorities. We of course have to ensure that we have the resources to implement our action plan.

Mr. Marcel Lussier: Did I understand correctly? Did you have $11 million? Over what period of time?

Mr. François Guimont: Basically, there are three figures. 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.

The Chair: Thank you very much, Mr. Lussier.

● (1255)

[*English*]

Mr. Fitzpatrick, go ahead for four minutes.

Mr. Brian Fitzpatrick (Prince Albert, CPC): I think everyone knows that assessments and studies can cause serious delays and can definitely drive up the cost of projects and contracts. I am curious about the extent of the process we would use in the certification process. If the department, let's say, were ordering Canadian flags or salt for the salt shakers or something along that line, how much is involved in the checklist process to determine that this really isn't a security issue and let's get on with it? How far are we going to go on the checklist of procedures in the non-sensitive areas? It seems to me we have to allow for some judgment by managers and some common sense in the system, or we could have a real problem.

What are we looking at on this checklist for non-sensitive areas?

Ms. Sheila Fraser: I absolutely agree that we don't want to burden the system with a lot of unnecessary consideration, but if people are going out to buy flags or whatever, it's pretty clear that there are no security issues there. It's when you get into defence construction contracts, for example, where we noted that for 99% of them there was no checklist done. At a minimum, there could be an indication that someone has considered the security aspects and has made a clear determination that there is no security. Previously that wasn't obvious, and so you didn't know if people had considered the security aspects.

At the risk of getting into a debate, in the NORAD project the security checklist was not completed, and there was no indication about security requirements, and so the people who were doing the contracting wouldn't know what clearances people should have. It's really up to the people who are running the projects to make that determination. Otherwise the people in Public Works, the contracting authorities, have no way of knowing—

Mr. Brian Fitzpatrick: I appreciate that. With sensitive areas we can all agree on that. I'm just a little bit cautious about making it a government-wide procedure in all government departments. You could really build an empire.

Ms. Sheila Fraser: It can be a pretty simple thing to do. When we do our own contracting—and you would suspect that in my office we don't have a lot—we have access to protected information. There is just a drop-down thing and people just have to do it. It's not a long process that they have to go through. It's simply checking another box.

Mr. Brian Fitzpatrick: Auditor General, in all seriousness, if we get into the "what ifs" that can happen—I remember reading an essay about what's involved in the manufacture of a pencil and getting it to market. If we get into all the "what ifs" that are possible in the world, you can create a pretty complicated procedure.

Maybe Mr. Guimont could comment on this area. There has to be some common sense in this whole process too, I think.

Mr. François Guimont: I very much agree with Madam Fraser. It's not one-size-fits-all, and this is important for committee members to appreciate.

I'll give you an example. If, for instance, someone requires a contract, they require a screening, a reliability check, at the lowest level—protected A—it can be done in days. If I remember, it is three days. It can be a bit more complicated, but it's measured in days. Obviously, to be clear—and this is where Madam Fraser is—if it's run-of-the-mill we can be pretty efficient and therefore not create a burden on either business or capacity for the government to issue contracts.

Where it gets to be more difficult—and this is where the OAG focused—is when you get into the more sensitive files. There, clearly, when we're talking about clearances at a secret or top secret level, we are now measuring progress in months. So this is very different.

It is very important for whoever decides there is a security requirement to make the right call, because if the call is one of top secret or secret, there will be an impact. It's not a negative impact. It's going to be a period of time to do the job correctly.

The majority of so-called screenings taking place for government activity are done at the screening level, which often is done in days. We're talking in thousands. If I remember, going on memory, it's like 50,000 clearances or reliability checks per annum. The workload is measured in days.

I don't minimize that. It has to be done, but I would like to think it is not creating a huge burden vis-à-vis the benefits.

● (1300)

The Chair: Thank you, Mr. Guimont.

Mr. Christopherson, you have four minutes.

Mr. David Christopherson: Thank you, Chair.

For the benefit of members and some of the work we have done, I want to put on the record that a page of the Auditor General's report says there was a review of all the agencies to see if they were doing security checks on contracting, and the only one that was doing it was the RCMP, so we have to give them their due where we can.

This is my second point. Deputy, with regard to your opening comments, I want to tell you how impressed I was, particularly that you caught on to this really quickly, when you were being briefed, as to where your priorities were. You got on top of this before the report was tabled, and you put in your comments, additional steps that you have taken, which is very impressive, and you didn't go out of your way to tell us how wonderful everything is and that this was a minor exception. This was a big deal, and you dealt with it that way. I, for one, am very pleased with the way you have approached this, notwithstanding the grilling we're putting you through today, but given the importance, I think you will appreciate that.

I don't want to belabour this one to death, but there are a couple of little things that concern me.

Major-General, how long was the delay and how much was the cost as a result of that delay, and how much was the cost of the modifications to the NORAD facility?

MGen Glynne Hines: What delay are we talking about?

Mr. David Christopherson: I'm talking about the delay where the report says, "In the opinion of National Defence, after more than a year of investigations and meetings, it is determined that, with modifications...". I'm assuming that if you have to have meetings about things, then you have to have modifications and you have to go back and undo work. You wouldn't normally put in your project plan four weeks to go back and fix screw-ups, so I'm assuming this went a little bit over.

MGen Glynne Hines: 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.

Some things were not put in right. We had cases where the locks were put on the wrong side of doors. We had places where conduit wasn't terminated properly in accordance with either good construction practices or the security rules we put on for the facilities. As you can appreciate, we have to make sure we know where any electrical conduit goes and that it's terminated correctly at both ends, because we're going to put communications or power cabling through that. In some cases it wasn't terminated correctly or there were junction boxes where they shouldn't have been, contrary to designs that had been approved.

So a certain amount of rework was required from a construction practices standpoint and a security standpoint, and that would have been picked up as part of the normal construction activity. The contractor would have been held responsible for fixing those things because they were implementation deficiencies, not design deficiencies.

Mr. David Christopherson: So if I'm hearing you correctly, there were no security-related matters that required modifications that were a big deal. You're telling me it was all junction boxes. You're really playing this thing down, so you'd better be prepared to defend it.

MGen Glynne Hines: I'm not saying they were all minor. They were what would be considered, on a $25 million construction project, oversights that weren't done correctly and had to be reworked.

Mr. David Christopherson: Thank you.

Auditor General, would you agree with that?

Ms. Sheila Fraser: Chair, if you agree, perhaps we could discuss this with the department. That was certainly not the impression we had when we completed our work, but we have not done a follow-up since then. Perhaps we can work with the Department of National Defence and come back to the committee with a response to that question.

Mr. David Christopherson: Am I out of time?

The Chair: Yes.

Mr. Wrzesnewskyj, you have four minutes.

Mr. Borys Wrzesnewskyj: Mr. Christopherson's opening comment about the RCMP jogged my memory. It was Mr. Crupi who was bounced out of the RCMP and ended up with the top security clearances that allowed him to work in the Canadian security establishment within National Defence. But let's set that aside.

I'm returning to page two under the heading of "What we found". You found there was willingness on the part of National Defence officials to circumvent key security-related procedures. That's pretty strong wording, and it's quite clear.

Can you provide us, perhaps in the next two weeks, with a list of circumventions that you became aware of so we can clarify this point?

● (1305)

Ms. Sheila Fraser: I believe in our audit we were aware of two. One of course was the NORAD project. The other one mentioned in paragraph 1.77 was the Shearwater hangars.

Mr. Borys Wrzesnewskyj: On the actual circumventions, perhaps we could get a little more detail, because there seems to be a disconnect in what we're hearing at the table here today.

Ms. Sheila Fraser: I would be glad to do that.

Mr. Borys Wrzesnewskyj: Mr. Shuster, in the last week we've heard from General Hillier that he's become especially sensitive to security matters. This report is quite an indictment of Defence and how it handles security.

You are the official in charge of security. Have you heard from the general as a result of this report?

LCol Dave Shuster: I have not heard from General Hillier.

Mr. Borys Wrzesnewskyj: Mr. Stevenson, have you heard from the general?

Mr. Scott Stevenson: Yes. In a follow-up to the Auditor General's report, all of the responsible officials were directed by the Chief of the Defence Staff and the deputy minister in the development of the action plan. I am here today partly because of the seriousness that the head of the Canadian Forces and the head of the department, the accounting officer—

Mr. Borys Wrzesnewskyj: When did this communication occur?

Mr. Scott Stevenson: It was in October, in following up on the report, when the department wrote to the Auditor General with the action plan and our response to it.

Mr. Borys Wrzesnewskyj: So that happened in October, but I guess Mr. Shuster wasn't made aware of this.

LCol Dave Shuster: I'm sorry, I have been involved in the action plan, but as to your question, I have not personally heard from General Hillier.

Mr. Scott Stevenson: The correspondence I'm referring to was addressed to the Vice-Chief of the Defence Staff, who in the chain of command is above Lieutenant-Colonel Shuster. So that would explain in part why he wasn't a personal addressee on that.

LCol Dave Shuster: Again, just to clarify, I was an addressee on the action plan. With regard to the action plan, I have received it, but coming from the Vice-Chief of the Defence Staff.

Mr. Borys Wrzesnewskyj: Mr. Stevenson, Mr. Shuster could previously not answer the question, who were these foreign contractors? We didn't get an answer from you when he referred that to you.

Who were these foreign contractors involved with the NORAD project?

Mr. Scott Stevenson: I don't have that information myself at this time.

The Chair: Could you get back to the committee with that list within two weeks?

Mr. Scott Stevenson: Yes.

The Chair: You have 30 seconds, Mr. Wrzesnewskyj.

Mr. Borys Wrzesnewskyj: Perhaps I'll leave it at that.

The Chair: That's generous of you.

Mr. Williams, you're up at bat for the last four minutes.

Mr. John Williams: Thank you, Mr. Chairman.

I was reading through this report, and like everybody, I find some serious problems here.

Mr. Nicholls, I don't think we've heard too much from you today, but it seems to me in your opening statement—I don't have a copy of it—you mentioned that you have a great deal of experience at Defence Construction Canada. Did you say 50 years, or was it 90 years? I can't remember which.

Mr. Ross Nicholls: The corporation, not myself. I don't have 56 years; the corporation has 56 years of experience.

Mr. John Williams: Fifty-six years of experience; you said a great deal of experience. Yet when I take a look at the section starting at paragraph 1.70 on page 23 of the Auditor General's report, you as a crown corporation should have an agreement with the Treasury Board. You don't even have an agreement regarding security with the Treasury Board. You're operating out there, having no legal liability whatsoever, and yet you tell us you have a great deal of experience.

Why has something so basic missed you for 56 years?

Mr. Ross Nicholls: The corporation has operated for 56 years under a series of memoranda of understanding with the Department of National Defence. In those memoranda—

Mr. John Williams: But why have you missed something so basic as having an agreement regarding security? Much of your work involves security. Haven't you even been focused on security?

Mr. Ross Nicholls: Absolutely. In accordance with our mandate and our working arrangement with the department, Defence Construction has always taken responsibility for industrial security on defence projects once those security requirements have been identified. The instant the department identifies the requirements, we safeguard the sensitive information—

● (1310)

Mr. John Williams: If I could interrupt, I'm quoting the Auditor General here: "However, we noted that as a Crown corporation, DCC is not subject to the Government Security Policy unless it enters into an agreement with the Treasury Board". And you haven't done that. So is this something voluntary that you've just taken upon yourself to do?

Mr. Ross Nicholls: No. We have now signed an agreement with —

Mr. John Williams: Now, after 56 years, you have the agreement in place.

Mr. Ross Nicholls: Since 1986, when the policy was around. However—

Mr. John Williams: Do you have this agreement with the Treasury Board, or do you not?

Mr. Ross Nicholls: Yes, we do.

Mr. John Williams: Madam Fraser.

Ms. Sheila Fraser: At the time of the audit, we did not find an agreement.

Mr. John Williams: Mr. Nicholls.

Mr. Ross Nicholls: To clarify, we've entered into the formal agreement with Treasury Board since the audit. Prior to that time, we always implemented the measures required by the government security—

Mr. John Williams: I still quote an arrangement that seems to have been saying, we'll look at it, don't worry. Is that right? Nothing formal, but we'll do it.

Mr. Ross Nicholls: Sir, I suggest that you look back, and you will not find a situation where we have not complied.

Mr. John Williams: That wasn't my question, Mr. Nicholls. I said you had no formal agreement with the Treasury Board to accept the responsibility for security on these buildings—

Mr. Ross Nicholls: Right.

Mr. John Williams: —after 56 years, yet in your opening statement you said you had a great deal of experience.

I see in your letter to Pierre Boucher, dated January 16, 2008—I presume this has been tabled before the committee, Mr. Chairman—you're talking about your having to address two objectives. The first is to fully integrate the requirements of security into the processes that you use to execute your role as a contracting authority, and the second is to operate the company in accordance with the DCC security policy.

Again, with 56 years, you say you have a great deal of experience, and it takes an Auditor General's report to say, hmm, since we do all these security buildings, maybe we should think about it. Why has it taken this report to wake you up to say, we should do something?

Mr. Ross Nicholls: The Auditor General quite rightly pointed out that our policies and processes were not documented or formalized in the way that they should be. By the end of March, they will be.

Once again, as suggested, our practices were in compliance. However, she quite rightly points out that they should have been more formal.

Mr. John Williams: Okay, well, I hope your next 56 years of experience will be a little more formal than the past.

Looking at paragraph 1.74, we're back to this above-ground NORAD building. Again, quoting the Auditor General, "This building was designed to house very sensitive and highly classified material".

I have heard evidence around the table saying that you built the building, and then somebody decided to change the use of it, so you had to go back to check the security of it. Was the building designed for highly sensitive information and highly classified information, or was this an afterthought, and now that we've built it, we'll use it for that?

The Chair: Go ahead, sir.

MGen Glynne Hines: The building was designed as a NORAD control centre, and it was built as a NORAD control centre, and it is currently being used for that intended purpose.

Mr. John Williams: That is avoiding my question, Mr. Chairman. My question was quite specific.

The Chair: Mr. Williams, we have had that question three or four times during the meeting. There's an unanswered question here on this NORAD thing, and we've had the dialogue with the Auditor General, and I don't think we're going to get to the bottom of that.

Okay. That, ladies and gentlemen, concludes the questions. I want to thank all members of the committee. I want to thank all witnesses.

What I propose now is to go in camera and very briefly deal with the minutes of the steering committee. But perhaps before that, I will ask if there are any closing remarks.

Ms. Fraser, have you any comments before we do that?

Ms. Sheila Fraser: I'd just like to thank the committee for its interest in this work and say that we are very pleased with the response from the departments. They have agreed with the recommendations. They have developed action plans. And in fact, in many cases they have already taken action on the issues that have been raised.

The Chair: Okay, does anyone else have any closing remarks?

Go ahead, Mr. Guimont.

Mr. François Guimont: Briefly, Mr. Chairman, we are working hard on an action plan, on a way-forward basis, on the so-called 3,000 contracts. In my remarks I committed to keeping the committee informed of what we find. I know there is interest in this, so we will be doing that.

The Chair: I want to thank you very much.

This is just a matter of housekeeping. Mr. Stevenson, could I get a commitment that you will file your action plan with the committee?

● (1315)

Mr. Scott Stevenson: Yes, Mr. Chairman. And like my colleagues, I would also like to thank the committee and all the members for their interest in this, and the Auditor General, again, for this audit, which has raised some significant issues that we are working to address.

Mr. David Christopherson: On a point of order, paragraph 1.82, which says, “The RCMP is the only organization of those we looked at where we found mechanisms for monitoring security in contracting”, is on page 27 of the Auditor General's report. Page 4 was the analyst's report.

Thank you.

Mr. John Williams: [*Inaudible—Editor*]...consideration too, Mr. Chairman?

The Chair: I don't think they exist any more, Mr. Williams.

I want to again thank you very much for your appearance here today. It has been a good meeting. There is a certain amount of follow-up. The committee will write a report and file it in the House of Commons in due course.

Thank you very much.

Okay, we're going to pause just for 20 seconds here and reopen in camera.

Mr. John Williams: We are going in camera to discuss a steering committee report. Is there a rationale for doing that? We normally do these in public.

The Chair: We can stay public, yes.

The only matter of business, colleagues, is the minutes from the subcommittee on agenda and procedure that was held yesterday, and those minutes have been circulated. There are 10 points.

Go ahead, Mr. Poilievre.

Mr. Pierre Poilievre: Mr. Williams has just taken my copy.

Mr. Chair, I note that—

The Chair: Hand them out. I just want to make sure everyone has a copy.

Mr. Pierre Poilievre: Just so we are clear, this meeting is not in camera.

The Chair: It is not in camera.

Mr. Pierre Poilievre: Mr. Chair, I thank you for giving me the floor.

I note that the steering committee concluded that this committee should authorize the clerk to use a private investigator to locate Mr. Jean-Marc Bard. Am I reading that correctly?

The Chair: It would authorize the clerk to use what I would refer to as a locator firm.

Mr. Pierre Poilievre: A locator firm. Is that...?

The Chair: Mr. Poilievre, just to elaborate—I might even get the clerk to speak on this—I don't think we do a good job locating people. We use the services of the bailiff, and he has access to the Ontario driver's licence but not to any Quebec information. Under a locator firm, they would have access to seven different public documents, and this would be a quick turnaround.

So we would try that first and then see where that leads us in this particular case.

Mr. Pierre Poilievre: Okay. But at this point we haven't been able to locate him, so we're engaging a professional firm to seek him out, track him down, and hopefully bring him in.

Some hon. members: Oh, oh!

The Chair: No, that is not quite correct.

I want to clarify the record here. There's nothing we've seen that would indicate that he's avoiding us. We just can't locate him. He may be avoiding us, but so far there's nothing to suggest that he is.

Mr. Pierre Poilievre: What about Dog, the bounty hunter? Could he be retained?

The Chair: Dog's jurisdiction is only in the United States. He doesn't take assignments in Canada.

Mr. Pierre Poilievre: Okay. So we've not been able to locate Mr. Bard to date.

On the subject of Mr. Alfonso Gagliano, he's refused to come in person? Is that the latest?

The Chair: No, he hasn't refused. He's asked if he could do it via video conference.

● (1320)

Mr. Pierre Poilievre: What is the budget for this locator firm?

The Chair: It's only $200. It's basically just checking seven different indices. I would assume it's housing records, driver's licence, etc.

Mr. Pierre Poilievre: That might be a little bit too modest, $200, if we've been trying to track this guy down for 18 months.

Mr. David Sweet: Mr. Christopherson said to go with $500.

The Chair: Any other comments?

Mr. Williams.

Mr. John Williams: I'd like to move on to point three, Mr. Chairman, addressing the leak of elements of the Barbara George report.

First, it was embarrassing. I had complimented the committee a couple of days before on how we had hung together and kept it all totally out of the media, and then, boom, it's in the media. It was shocking, disappointing, and I hope the person who leaked it is hanging their head very low indeed. It's despicable that someone who was reported to be held in contempt was reported in the newspapers with absolutely no knowledge of what was in the report themselves and no capacity to respond. They didn't know what the accusations against them were.

That was a despicable event, Mr. Chairman, and I would hope that whoever did it would stand up and do a *mea culpa*. It's not like leaking a report on the government, where things happen and where the government can respond. This was a direct condemnation by this committee on a particular person, who found all the elements of the accusation and the condemnation in the newspapers before they were even advised of what was our opinion, and therefore I found it despicable.

But unless that person is prepared to publicly stand up and accept their responsibility, I don't think there's anything we can do. I remember we had the Auditor General do an investigation into one of the leaks of her report some time ago, and that ended up just being an embarrassment, because we couldn't find anybody.

Therefore, I'm prepared to leave it as is, although I wouldn't mind passing a motion of condemnation of whomever. I hope they recognize the seriousness of this. It was on an individual; it wasn't focused on a government department and on something the government had done wrong.

There could have been no glory in it, because I didn't find any name attached to this. Nobody saw their name in lights on this, because they refused to even put their name to it—which is further condemnation of the low attempt to try to get some gratification and see something in the media that they caused when the person on whom it was focused had no capacity whatsoever to respond. That, I found, was the most despicable part of it.

The Chair: Yes, and if I may make a comment, Mr. Williams, I agree with you. It was very unfortunate in this particular set of circumstances that that leak did occur. I agree with what you're saying, that it really was a violation of the committee's privileges.

My suspicion is that when you talk to the media—and I generally make a habit in a situation like this of not talking to them—they say they have this story or that story and that they want to confirm it. I think you're better off not talking to them at all in a situation like this, and that's unfortunate.

Mr. Fitzpatrick.

Mr. Brian Fitzpatrick: I just wanted to make a comment on that too. I think that whoever did this is in contempt of the committee and is bringing disrespect to every other member on this committee; we're all painted with the same brush because this person, for whatever reason, has no ethical standards. We're just on our high horses here with government officials talking about security clearances and risk assessment, and people are even talking about zero risk concepts and guarantees, and so on; but on this committee we have somebody for whom this stuff doesn't mean one iota. If they were working for the government in the security area, you couldn't trust them any farther than you could throw a piano.

The Chair: What you're saying, Mr. Fitzpatrick, is that members of this committee would not necessarily get DND security clearance.

● (1325)

Mr. Brian Fitzpatrick: Yes, that's the unfortunate reality of it.

Mr. John Williams: Loose lips sink ships, Mr. Chairman. We all know that.

The Chair: Is there anything further on the minutes?

We'll accept a motion for their adoption.

Hon. Charles Hubbard: I move that we adopt the minutes.

The Chair: Is there any further discussion?

Hon. Charles Hubbard: Are you going with all 10 by adopting this motion?

The Chair: We're not going to go over them point by point. Do you have any—

Hon. Charles Hubbard: But I think we're hearing that some people are concerned about a couple of them.

Mr. Brian Fitzpatrick: There's nothing we can do about it.

Hon. Charles Hubbard: No? We'll go with all 10. Okay.

I have moved the motion.

The Chair: Most of them are housekeeping matters, sir.

(Motion agreed to)

The Chair: We will be here on Thursday. We have, I believe, two reports that are revisions of previous reports. So there are four reports. They've all been circulated or were sent out this morning, so you have them in your offices now.

We will see you on Thursday at 11.

Mr. David Sweet: Sorry, Mr. Chair, but whom have we confirmed for next Thursday?

The Chair: We have confirmed the two witnesses.

Mr. David Sweet: The two, as in...?

The Chair: Ms. Cochrane and Gary Polachek.

The meeting is adjourned.

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

Publié en conformité de l'autorité du Président de la Chambre des communes

Also available on the Parliament of Canada Web Site at the following address:
Aussi disponible sur le site Web du Parlement du Canada à l'adresse suivante :
http://www.parl.gc.ca
