2007

Report of the

Auditor General of Canada

to the House of Commons

OCTOBER

Chapter 1

Safeguarding Government Information and Assets in Contracting

Office of the Auditor General of Canada

The October 2007 Report of the Auditor General of Canada comprises Matters of Special Importance, Main Points—Chapters 1 to 7, Appendices, and seven chapters. The main table of contents for the Report is found at the end of this publication.

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

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

Office of the Auditor General of Canada
240 Sparks Street, Stop 10-1
Ottawa, Ontario
K1A 0G6

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

Ce document est également publié en français.

Cat. No. FA1-2007/3-1E
ISBN 978-0-662-46982-7

Chapter

1

Safeguarding Government Information and Assets in Contracting

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

Table of Contents

Safeguarding Government Information and Assets in Contracting

Main Points

What we examined

The Government of Canada uses a wide range of classified and protected information and assets to help govern the country. Our audit examined how the federal government ensures the security of sensitive information and assets that it makes available to industry in the course of contracting. The Government Security Policy and its related operational and technical standards prescribe safeguards to help make the contracting process and internal government operations more secure. These safeguards are designed to preserve the confidentiality, integrity, availability, and value of information and assets, and to assure the continued delivery of services.

Safeguarding sensitive information and assets entrusted to industry is a complex task; it involves coordinating the efforts of many government departments, agencies, Crown corporations, and private sector companies. We looked at the delivery of the Industrial Security Program by Public Works and Government Services Canada. This program was set up to safeguard classified and protected information and assets of the Canadian government, NATO, and foreign governments when entrusted to private sector organizations because of project or contract requirements. It does this by ensuring that the organizations have obtained the necessary security clearances, that contracts contain the necessary security clauses, and that contractors comply with these clauses.

We looked at the policies and procedures of the three federal organizations with the highest numbers of contracts processed by the Industrial Security Program—Public Works and Government Services Canada (PWGSC), National Defence, and the Royal Canadian Mounted Police (RCMP)—to determine whether these policies and procedures support the organizations' roles and responsibilities for industrial security under the Government Security Policy. We reviewed the role played by Defence Construction Canada as the contracting authority for defence projects. We also examined the Treasury Board of Canada Secretariat's role in monitoring the implementation and effectiveness of the Government Security Policy.

Our audit was not designed to assess whether or not breaches of security actually have occurred.

Why it's important

Keeping sensitive government information and assets secure, whether held within government or entrusted to industry, is critical to supporting the Government of Canada's objectives and the health, safety, security, and economic well-being of Canadians at home and abroad.

The security clearances granted by government departments can give Canadian companies access to contracting opportunities, in Canada and abroad, that are worth billions of dollars. Security screening is thus essential to ensuring that Canadian and foreign government information and assets entrusted to these companies are secure.

The government's ability to protect sensitive information and assets that it entrusts to Canadian industry is also important to its international reputation and the continued growth of international trade. Accordingly, before contractors are given access to government facilities or to sensitive information, they must be screened for security at the appropriate level. This is done to ensure the proper protection of information that can range from private information on citizens' to Cabinet confidences or national security information. The integrity of the industrial security process is therefore an integral part of maintaining public trust in Canadian institutions.

What we found

- Our observations in the organizations we examined indicate that there are serious weaknesses in the processes that are supposed to ensure the safeguarding of sensitive government information and assets entrusted to industry. 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 have been followed at the earlier stages; however, there are few mechanisms to provide assurance that this is so. Moreover, in at least one major project, we noted a willingness on the part of some National Defence officials to circumvent key security-related procedures in order to reduce costs and avoid project delays.
- 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 level. These include some contracts awarded by PWGSC for projects with clearly identified security requirements that had not all been met by the time the contract was completed. They also include thousands of contracts for National Defence construction and maintenance

projects across Canada awarded by Defence Construction Canada without the contractors' security clearances having been verified. It is not known to what extent government information and assets may have been exposed to risk and who is accountable for that risk.

- PWGSC's Industrial Security Program has significant weaknesses. Its operating procedures are in draft form and do not cover some key activities that are essential to ensuring the security of information. In addition, key activities are not carried out consistently. These activities include obtaining signed agreements from contractors confirming that they have acknowledged and understood their responsibilities and have accepted the transfer of responsibility for safeguarding sensitive government information. Few procedures exist for ISP staff to determine whether the Program has processed all contracts, within its responsibilities, that contain security requirements.
- PWGSC has yet to secure stable funding for the Industrial Security Program, relying on temporary funding from the Deputy Minister's reserve for close to one-third of the Program's permanent workforce. At the time of our audit, approximately 28 percent of the positions in the Program were vacant and about 32 percent of the positions were filled by temporary staff. Senior officials told us that the lack of stable funding limits their ability to offer permanent employment, making it difficult to attract and retain qualified security professionals.

The departments have responded. The departments agree with all our recommendations. Their detailed responses follow each recommendation throughout the chapter.

Introduction

The Government Security Policy establishes objectives for security in contracting

1.1 The government frequently contracts with private sector individuals and organizations who can provide expertise or economies of scale not found in government. Such contracting helps the government to deliver its programs and services effectively and efficiently and to meet its objectives. In many cases, the federal government has to entrust **protected** or **classified information and assets** to a contractor so that the contracted work can be completed.

1.2 The objective of the Government Security Policy as it pertains to contracting is to ensure that **sensitive information and assets** of the government are properly protected when entrusted to industry. This is to be accomplished by ensuring that each individual and organization that will have access to or will possess sensitive information and assets has first received the necessary security screening or clearance. According to Public Works and Government Services Canada (PWGSC), to date almost 5,800 private sector organizations and more than 370,000 individuals in Canada contracted by the federal government have received security clearances through the Industrial Security Program delivered by PWGSC.

1.3 The Government Security Policy is intended to support the **national interest** and the achievement of the government's objectives by safeguarding employees and assets and assuring the continued delivery of federal services.

1.4 Each federal department is responsible for protecting sensitive information and assets under its control—not only in its own operations but throughout the bidding, negotiating, awarding, carrying out, and terminating of any contracts it manages.

1.5 The main roles and responsibilities in the Government of Canada for **security in contracting** are summarized in Exhibit 1.1.

Assets—Tangibles or intangibles belonging to the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence, and international reputation.

Sensitive information and assets—Information and assets that are either protected or classified.

Protected information and assets—Information and assets related to the non-national interest that, if compromised, would reasonably be expected to cause injury to the non-national interest. Information and assets designated "protected" require more than basic protection.

Classified information and assets—Information and assets related to the national interest that, if compromised, would reasonably be expected to cause injury to the national interest. Information and assets designated "classified" require more than the protection provided for protected information and assets.

National interest—Concerns the defence and maintenance of the social, political, and economic stability of Canada.

Security in contracting (Industrial security)—Ensuring that protected or classified information and assets entrusted to industry through contracts are safeguarded.

Key elements of security in contracting

1.6 Various parties and procedures help to ensure that security concerns are addressed when awarding a contract.

1.7 **The project authority.** In departments, the project authority (the person initiating the project) is responsible for analyzing risks before the contracting process begins and identifying the necessary security requirements, if any. A critical task for departmental project

Exhibit 1.1 Roles and responsibilities for security in contracting

Government entity	Roles and responsibilities
Treasury Board	• Approves the Government Security Policy.
Treasury Board of Canada Secretariat	• Provides strategic direction, leadership, advice, and assistance on security and service delivery issues. • Develops and updates the Government Security Policy. • Provides policy guidance and interpretation to departments on how to implement the policy. • Monitors how the policy is implemented and whether policy objectives have been achieved. • With input from departments, produces a mid-term report to the Treasury Board on the effectiveness of the policy.
Public Works and Government Services Canada	• Consults with the Treasury Board of Canada Secretariat and other departments, to develop operational standards and technical documentation on security in contracting. • Administers the Industrial Security Program. • Provides advice to departments on the operational standards and technical documentation on security in contracting. • Develops and provides training in security in contracting. • Maintains a database of private-sector organizations and individuals who are security screened for access to sensitive government information and assets. • Ensures compliance with the Government Security Policy in contracts that are outside delegated contracting responsibilities of departments, and that would allow access to sensitive government assets. • On request, ensures compliance with the Government Security Policy in contracts that are within delegated contracting responsibilities of departments, and which involve access to sensitive government assets.
All government departments	• Appoints a departmental security officer to establish and direct a security program. • Conducts active monitoring and internal audits of its security program (including security in contracting) and reports the results to the Treasury Board of Canada Secretariat. • Protects sensitive information and assets under its control. • As the project authority, identifies sensitive information and assets warranting safeguards, whether a contract is within or outside its delegated contracting responsibilities. It also establishes the required level of security for a contractor.
Contracting authority	• Ensures security screening of private sector organizations and individuals who have access to protected and classified information and assets. • Ensures safeguarding of government assets, including IT systems. • Specifies the necessary security requirements in the terms and conditions of any contractual documentation. • Ensures that the contractor meets the appropriate security requirements or requests that PWGSC perform this task and document the results. • Completes scheduled and unscheduled inspections of contractors' work sites.
Departmental security officer	• Establishes and directs a security program that ensures coordination of all policy functions and implementation of policy requirements, which includes security in contracting.

Source: Government Security Policy and the Security and Contracting Management Standard and Results for Canadians: A Management Framework for the Government of Canada

Security Requirements Checklist—A form that project authorities, departmental security officers, procurement officers, or other government employees in the contracting process use to identify security requirements at the start of any contractual or pre-contractual process.

authorities is to complete a **Security Requirements Checklist** (the Checklist) and forward it to the contracting authority.

1.8 The Security Requirements Checklist. The completed Checklist is the basis for defining the terms and conditions to be included in contracts in order to meet the necessary security requirements. The Checklist allows the contracting authority to discharge its responsibilities. Departments (project authorities) must use the Checklist to define the security requirements for contracts when PWGSC is the contracting authority. It is recommended, but not mandatory, that the Checklist also be completed when a department retains contracting authority.

1.9 The contracting authority. The contracting authority, whether PWGSC or another government entity, or a department entering into a contract within its own delegated authority, is responsible for ensuring that

- private sector organizations and individuals who will have access to sensitive information and assets are screened at the appropriate security level,
- contract documentation includes the terms and conditions needed to meet security requirements, and
- sensitive government information and assets are safeguarded.

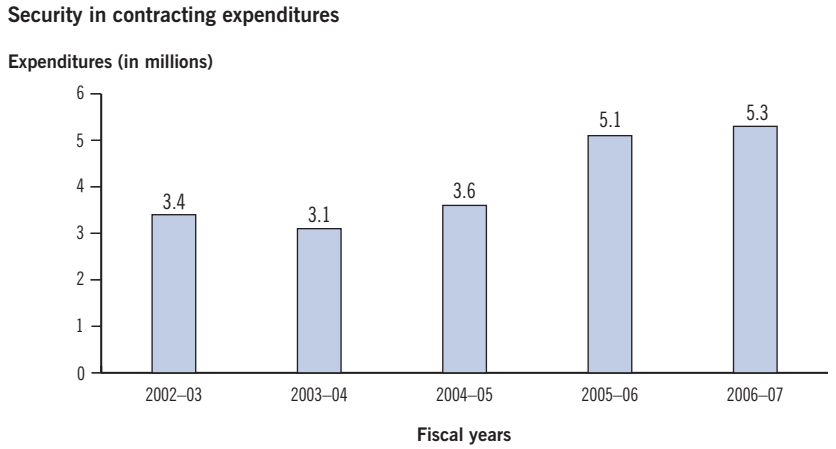
1.10 The Industrial Security Program. Public Works and Government Services Canada's Industrial Security Program is intended to ensure that all contracts with security requirements and for which the Department is the contracting authority comply with the Government Security Policy throughout the contracting process. Upon request, the Program also handles the security requirements of contracts awarded by other government departments under their own contracting authority.

1.11 The Industrial Security Program is intended to ensure the screening and security clearance of companies and personnel requiring access to sensitive government information and assets. This process is designed to ensure that companies involved in sensitive federal and foreign government contracts are registered in the Program and meet the security requirements identified by client departments. The Program also identifies the appropriate security terms and conditions to be included in each contract, either when PWGSC is the contracting authority or when the Program is requested to do so by other government departments. The Program is intended to ensure that the facilities of contractors who must hold or process sensitive

information while performing work for the government have been cleared before sensitive information can be stored on site. It then conducts follow-up inspections to ensure that contractors continue to comply with the security requirements in their contracts.

1.12 PWGSC's spending for the security in contracting portion of the Industrial Security Program has increased since the 2002–03 fiscal year (Exhibit 1.2).

Exhibit 1.2 Spending on security in contracting has increased



Source: The Finance Branch of Public Works and Government Services Canada

Focus of the audit

1.13 The audit focused on how Public Works and Government Services Canada delivers its Industrial Security Program and how it carries out its role as the lead contracting authority for the government. To assess the effectiveness of the Program's practices and procedures, we looked at what we considered to be among the highest-risk files processed by the Program.

1.14 We looked at whether the roles and responsibilities for security in government contracting are clear and whether PWGSC, National Defence, and the RCMP have procedures to ensure that they fulfill these roles and responsibilities. In addition, we looked at the role of Defence Construction Canada as the contracting authority for government defence projects.

1.15 We also examined the role of the Treasury Board of Canada Secretariat in monitoring how the Government Security Policy is implemented and whether the government's overall industrial security objectives are achieved.

1.16 Our audit was not designed to assess whether or not breaches of security actually have occurred. More details on the audit objectives, scope, approach, and criteria are in **About the Audit** at the end of this chapter.

Observations and Recommendations

Industrial security policy framework

The industrial security policy framework has weaknesses

1.17 The Government Security Policy (the Policy) sets out the government's objectives for industrial security and establishes who is responsible for achieving them. We expected the framework to be clear and consistent, but we found that certain weaknesses in the framework have led to uncertainty about responsibilities and accountability for security in contracting and about the effectiveness of the industrial security process.

1.18 The Government Security Policy's contracting standard is ambiguous. Under the Policy, the contracting authority is responsible for ensuring industrial security. The Policy is supplemented by operational and technical standards that direct and guide its implementation. For example, the Security and Contracting Management Standard requires that the project authority use the Security Requirements Checklist (the Checklist) to define any security requirements of contracts for which Public Works and Government Services Canada (PWGSC) is the contracting authority. The wording of the Standard recommends but does not require that the project authority forward the completed Checklist to PWGSC. If the project authority does not forward the Checklist, PWGSC cannot fulfill its role as contracting authority—to ensure that all sensitive contracts it awards contain appropriate security provisions. This mixture of required and recommended procedures in the Standard has contributed to confusion about responsibilities under the Policy.

1.19 In addition, we noted that PWGSC, National Defence, and the Royal Canadian Mounted Police (RCMP) were interpreting the Standard as requiring them to complete a Checklist only for projects where they have identified a security requirement. PWGSC has informed us that it has been implementing the Policy and its related Security and Contracting Management Standard consistent with this interpretation. While the Treasury Board of Canada Secretariat has agreed the PWGSC's interpretation is reasonable, the Secretariat has acknowledged that the language in the Standard may lead to uncertainty or ambiguity about what project authorities are actually responsible for. In our view, this interpretation is not consistent with

the responsibilities established for PWGSC by the Policy. An interpretation that does not require a Checklist for all contracts can result in significant risks to the government and in diminished accountability for decisions made. For example, an incorrect decision by a project authority that security is not an issue for a given contract could pose a risk—namely, that a contractor could be given access to sensitive information without having received appropriate security clearance. The Treasury Board of Canada Secretariat has informed us that it plans to update the current Security and Contracting Management Standard, which predates the Government Security Policy by six years.

1.20 We also noted that the Government Security Policy and its Security and Contracting Management Standard clearly establish responsibilities for the contracting authority that, in practical terms, are difficult to carry out. For example, the Policy requires the contracting authority to "ensure the safeguarding of government assets, including IT systems," but the contracting authority may not have access to or control over the assets involved in a particular contract.

1.21 **Recommendation.** The Treasury Board of Canada Secretariat should ensure consistency among the Government Security Policy and the associated directives, standards, and guidelines.

Treasury Board of Canada Secretariat's response. Agreed. The Treasury Board Secretariat is in the process of reviewing the policy on government security. The current policy was issued in 2002 and is due for renewal at the five-year mark. The review is currently under way, and the new policy is expected to be completed at the end of summer 2008.

Under the Policy Suite Renewal initiative, the structure of policy instruments is being clarified, and ambiguity in the language in the policy on government security is being addressed. The accountabilities of deputy heads are also being clarified, in terms of delineating mandatory requirements from guidelines and best practices.

Public Works and Government Services Canada

Roles and responsibilities for security in contracting are unclear

1.22 Clearly defined roles and responsibilities provide the basis for developing standard operating procedures and service standards. They can also provide the basis for monitoring and measuring performance. Public Works and Government Services Canada (PWGSC) has roles and responsibilities on a number of levels that involve security in contracting:

- Acting as the lead federal department for procurement on behalf of other departments, it accounts for about 90 percent of the total

dollar value and about 10 percent of the total volume of government contracts.

- It is also responsible for delivering the Industrial Security Program.
- 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.

1.23 We found that PWGSC's roles and responsibilities for security in contracting are not clearly understood within the Department. In our interviews with key officials of PWGSC and of the Industrial Security Program in particular, we noted some confusion about the scope of the Department's responsibilities for industrial security. We found, for example, that Program officials' interpretation of the Industrial Security Program's mandate was revised twice during our audit, in response to our questions about the scope of the Program. At the start of the audit, the stated mandate was to ensure security in all government contracts. This was later revised to include only contracts awarded by PWGSC and then revised again to include, when requested, contracts awarded by other government departments. Revisions to the interpretation of the Industrial Security Program's mandate were communicated publicly through website descriptions of the Program's responsibilities.

Policies and procedures for industrial security are incomplete and inadequate

1.24 PWGSC's staff need sufficient and appropriate guidance to ensure that sensitive information and assets entrusted to industry through contracting are properly safeguarded. This would include clear and comprehensive policies and standard operating procedures accurately reflecting the Department's roles and responsibilities for industrial security under the Government Security Policy.

1.25 We found that PWGSC's policies and procedures for industrial security are incomplete and do not adequately address some areas. For example, at the completion of our audit, the departmental policy on industrial security was outdated and was being revised. In addition, the Department's Supply Manual lacks procedures needed to guide PWGSC staff in their industrial security responsibilities. For example, the Supply Manual does not require the contracting officer to ensure that a Security Requirements Checklist (the Checklist) is forwarded for every requisition and contractual amendment, but only for those where security requirements have been identified. This is particularly important because PWGSC is not in a position to know whether the proposed

procurement would provide a contractor with access to sensitive information or assets that are managed by the client department.

1.26 We also found that standard operating procedures for the Industrial Security Program are in draft form and incomplete. The Program has developed a table of contents for its procedures manual, which indicates what the manual should contain, but it has not developed all the standard procedures that it has determined are necessary to manage the Program. The draft procedures do not yet cover some activities essential to the proper functioning of the Program. For example, through signed agreements, PWGSC transfers responsibility for safeguarding sensitive government information to company security officers of organizations under contract with the federal government. However, the Department's procedures provide limited guidance for Industrial Security Program staff on how to determine whether or not company security officers are complying with these agreements. 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.

1.27 In our view, the lack of adequate procedures and controls for industrial security, both within PWGSC and among PWGSC, its client departments, and contractors, means that the Department cannot always ensure that the appropriate procedures have been followed to safeguard sensitive government information in the hands of contractors. The gaps in policies and procedures are one consequence of not having clearly defined and understood roles and responsibilities for security in contracting.

Practices in place for industrial security are not being followed

1.28 In the absence of complete standard operating procedures to guide industrial security activities in PWGSC, various practices have evolved over time. We looked at a sample of files to determine whether the Department is assured that its staff follow both the procedures currently set out in the Supply Manual and the practices that have emerged in the Industrial Security Program. Rigorous compliance with industrial security policies and procedures is essential to the protection of sensitive government information and assets.

1.29 We found that the Department lacks a means to know whether its staff are following its industrial security procedures and practices; we found that in general, staff are not following them consistently. Some Industrial Security Program managers we interviewed told us that they and their staff viewed the draft procedures only as guidelines.

The inconsistencies we noted in our review of the sample of files corroborated, in our opinion, the view expressed by these managers. We found a number of departures from industrial security practices and procedures, which are discussed in the following paragraphs.

1.30 Sensitive contracts have been awarded before contractors have met all the security requirements in the contract. We looked at the files of all contractors who had been cleared to the "secret" level, with document safeguarding capability; who had been entered into the Industrial Security Program database after 1 April 2002; and who had received at least one contract or pre-contractual agreement by 31 March 2007. We considered these files among the highest-risk files processed by the Program, given that the contractors could have access to and possession of information classified as "secret."

1.31 Of the 55 contractors whose files we reviewed, 48 had been awarded a total of 86 sensitive contracts and subcontracts at varying security levels. We found that PWGSC had awarded 24 of these sensitive contracts before the contractors were cleared to the security level required in the contract; 16 of these 24 contracts were for work at the "secret" level or above. Although all these contractors subsequently received the required level of security clearance, the contracts were awarded on average about 11 months before the clearances were completed.

1.32 The work under four of the twenty-four contracts noted above had been completed in full before the contractor was cleared to the security level required in the contract, and the Industrial Security Program provided us with a list of three more that its system had flagged for follow-up. In four of these seven contracts, PWGSC was unable to demonstrate that the contractors did not access sensitive information or assets during the life of the contract. For the remaining three contracts, although some evidence of mitigation measures was provided, PWGSC was unable to demonstrate that it sought and obtained assurance from the client departments that appropriate mitigation measures were in place at the time the contract was awarded or during the life of the contracts. The Industrial Security Program has the ability to track such contracts and those awarded with clearances pending; however, it does not systematically follow up to ensure that risk mitigation measures are in place.

1.33 The Government Security Policy requires the contracting authority to ensure the safeguarding of government information and assets. We expected that PWGSC, as the contracting authority, would caution client departments not to give a contractor access to sensitive

information or assets until the appropriate security clearance had been granted and that it would obtain assurance of this from client departments. We found that the Industrial Security Program routinely warns PWGSC procurement officers that no contract or pre-contractual agreement may be awarded before verifying that the security requirements of the contract have been met. However, we found little or no evidence that client departments have received similar warnings. In addition, we found little to no evidence that PWGSC had asked its client departments to indicate to it that they would take the necessary steps to ensure that contractors would not access sensitive information and assets before being granted a security clearance. In 6 of the 24 contracts awarded before the contractors were cleared to the security level required in the contract, PWGSC was able to provide evidence that mitigation measures were in place. However, in 4 of the 6 cases, the Department had not obtained this evidence at the time the contract was awarded.

1.34 We reviewed information on two contracts at National Defence and one at the RCMP that had been awarded by PWGSC before the contractors were cleared to the security level required in the contract. Both National Defence and the RCMP provided evidence that the contractors had been denied access to sensitive information and assets until appropriate security clearances were granted.

1.35 Inappropriate use of delay clauses in sensitive contracts. PWGSC faces a number of challenges in carrying out its responsibilities in its role as service provider for contracting and in administering the Industrial Security Program. It not only must ensure security in contracting, but also must provide timely service to departments, as the government's main contracting authority. The Department has been using **delay clauses** in contracts that involve sensitive information, so that it can award contracts while security clearances are being applied for and processed. The Department has informed us that in many situations, work can begin under a contract before the contractor needs access to the required sensitive information and assets.

Delay clauses—A provision inserted in a sensitive contract that allows a contractor to start work before meeting all the necessary security requirements. Access to sensitive information and assets may not be granted until the security requirements have been met.

1.36 The Government Security Policy states that before any contracted work begins, a contractor must be granted a security clearance at the appropriate level. In special circumstances and supported by a threat and risk assessment, the Policy's Contracting and Management Standard allows the use of a delay clause in contracts that provide access to protected information and assets. Such a clause must stipulate that the security requirements must be met within six months after the contract is awarded or, if the contract is for less than six months, before the contract's half-way point. The Standard

does not stipulate that delay clauses can be used in contracts that provide access to classified information and assets.

1.37 Of the 86 sensitive contracts awarded to the contractors whose files we reviewed, 27 contained delay security clauses, 8 of which required classified security clearance. Industrial Security Program officials informed us that the Program does not request a threat and risk assessment when delay clauses are used in a contract, even though this is a specific requirement of the Standard. We also found that 25 of the 27 contracts specified no time frame for meeting the security requirements but rather stated that the contractor "shall eventually" receive a valid security clearance at the required level. We also reviewed the invoices for 8 of the 24 contracts awarded before the contractors were cleared to the security level required in the contract. We found that in 6 cases, work had commenced before the contractor met all the security requirements of the contract. In our opinion, these practices are not in accordance with the Government Security Policy.

1.38 Critical steps in the industrial security process are not consistently followed. We identified a number of situations in which documents central to the industrial security process were missing or incomplete. For example, we found that the Industrial Security Program had granted "secret" security clearances to 24 of the 55 contractors whose files we reviewed, even though two documents that are key to the clearance process were incomplete or not on file at the time of our review:

- The Security Screening Certificate and Briefing Form, to be signed by the contractor's company security officer, both acknowledging the statutory and administrative requirements associated with the security clearance and agreeing to comply with them. This document was not signed in 23 of the 24 files in question.
- The Security Agreement that each company under contract with the government is required to enter into with PWGSC. The Security Agreement transfers to the company's security officer the responsibility for safeguarding sensitive government information. A company must return the signed Security Agreement to the Industrial Security Program within a period specified by PWGSC, normally 30 days of receiving its security clearance letter. PWGSC advises companies that failure to return the signed agreement within the specified period will result in the suspension of the company's security clearance. This document was not on file in 6 of the 24 files in question, and in none of the 6 cases was the security clearance suspended.

1.39 These key documents must be signed by both PWGSC and the contractor to complete the security clearance process. By signing the Security Screening Certificate and Briefing Form, the company security officer attests that he or she understands and accepts responsibility to safeguard sensitive government information and assets to which he or she has access. Signing of the Security Agreement by both parties is necessary to establish the legal agreement between PWGSC and the contractor, which requires the contractor to safeguard the government's sensitive information and assets. Where PWGSC has not obtained a signed Security Agreement from a contractor, it has not completed one of the critical steps in its processes for ensuring the safeguarding of government information and assets.

1.40 We advised the Industrial Security Program that these 29 documents were either incomplete or not on file; program officials subsequently obtained copies of 13 Security Screening Certificate and Briefing Forms and 4 Security Agreements from the contractors' company security officers. Program officials could not provide 10 Security Screening Certificate and Briefing Forms and 2 Security Agreements. These documents did not exist and could not be found in the files of either the Program or the contractors.

1.41 In the absence of ensuring that these documents were signed and returned, the security screening process for these contractors was not completed. In addition, since Security Agreements did not exist, the Program should have suspended the security clearances held by two of these contractors.

1.42 Failure to maintain adequate documentation is a significant weakness in the Department's security clearance processes. PWGSC failed to monitor the completion of critical steps in the industrial security process. In our view, the Department has not exercised due diligence in its duties.

1.43 Renewal inspections are not conducted on time. The Government Security Policy requires that departments ensure the continued reliability and loyalty of individuals and organizations who have been given security clearances. The Industrial Security Program's draft procedures for ensuring such continued reliability require that, where a contractor's facilities have been cleared to safeguard "secret" level information on site, they must be re-inspected every 12 months at a minimum. We found that only 40 percent of the completed inspections were within the established 12-month time frame.

1.44 Officials of the Industrial Security Program told us that their inability to complete renewal inspections within the 12-month standard

was the result of a backlog of various types of activities that developed after several years of underfunding prior to 2005. The Program subsequently developed a strategy to prioritize inspections. Officials noted that additional temporary funding in 2005 allowed them to address the higher-risk inspections in the backlog. However, overdue renewal inspections were considered only a medium risk, and starting in January 2005, the 12-month standard period was extended by four to six months. In March 2006, the Program reverted back to the 12-month cycle for renewal inspections. According to data provided by the Program, we determined that it was able to meet the applicable standard in 86 percent of cases.

1.45 Overall, those renewal inspections that were overdue were about 10 months late, on average. At the time of our audit, the renewal inspections of the facilities of 7 of the 55 contractors whose files we reviewed were outstanding.

1.46 The Industrial Security Program can not ensure that it receives the information needed to carry out its duties. To ensure the integrity of the industrial security process, the Government Security Policy requires that a Security Requirements Checklist (the Checklist) be completed for all contracts when PWGSC is the contracting authority. PWGSC must rely on client departments to identify on the Checklist any security requirements for their contracts and forward it to PWGSC procurement officers. Industrial Security Program staff rely on these procurement officers to forward the Checklist and other contract-related documents to them for processing. The Checklist informs the Program of the need to initiate the necessary clearances for the contractor's personnel and facilities and to identify the appropriate security terms and conditions to be included in the contract.

1.47 This process makes it very difficult for PWGSC to fully discharge its responsibilities. Without mechanisms in place to ensure that client departments and its own procurement group are meeting their obligations, PWGSC is not in a position to ensure that all sensitive contracts it awards have sufficient and appropriate security safeguards.

1.48 Moreover, we found that all organizations in our audit were interpreting the Government Security Policy and its related Security and Contracting Management Standard to mean that they were required to complete a Checklist only for projects with a security requirement—an interpretation that in our view is not consistent with the requirements of the Government Security Policy.

1.49 We were unable to conclude whether all Security Requirements Checklists received by PWGSC were forwarded to and processed by the Industrial Security Program because PWGSC's database on all contracts it has awarded (the Acquisition Information System, or AIS) does not identify all those with security requirements. Department officials told us that security information is not captured in the AIS on a consistent basis because the related data elements are not mandatory. Accordingly, there is currently no means of identifying all contracts awarded by PWGSC that contain security requirements.

1.50 At the time of our audit, the Industrial Security Program did not have mechanisms in place to ensure that it received for processing all contracts and pre-contractual agreements that had security requirements. The Program has stated that since the completion of our field work, it has begun to compare information captured by PWGSC procurement officers with agreements it processes.

1.51 **Recommendation.** Public Works and Government Services Canada should ensure that before it awards a contract, it has received from the client department a completed Security Requirements Checklist identifying the necessary security requirements, or a certification that there are none.

Public Works and Government Services Canada's response. Agreed. PWGSC has interpreted and applied the Government Security Policy in a manner that is consistent with the interpretation of the Treasury Board Secretariat, National Defence, and RCMP, as noted in paragraph 1.19. As also noted, the OAG interprets the Government Security Policy in a different manner. The OAG has made a recommendation to the Treasury Board Secretariat on this issue in paragraph 1.78, and the chapter notes that the Treasury Board Secretariat plans to update the Standard. PWGSC will comply with the Treasury Board Secretariat-revised Standard. In the meantime, PWGSC will implement a certification process.

1.52 **Recommendation.** Public Works and Government Services Canada should ensure that it completes the development and approval of standard operating procedures for the Industrial Security Program and that they are consistently followed.

Public Works and Government Services Canada's response. Agreed. Industrial Security Program procedures are being finalized and will be issued in final form by September 30, 2007. Further, PWGSC has established a robust action plan to address the recommendations and all the other weaknesses identified in this report. Internal Audit will follow up to monitor implementation.

Public Works and Government Services Canada has yet to establish a stable infrastructure for managing the Industrial Security Program

1.53 **Human and financial resources.** We looked at the infrastructure established within Public Works and Government Services Canada (PWGSC) to support the Industrial Security Program. Like any program, the Program requires appropriate personnel and adequate financial resources; it also needs a secure information technology network to help it meet its mandate under the Government Security Policy.

1.54 We were provided with business cases prepared by Consulting and Audit Canada for the Industrial Security Program since 2004. These business cases identified resource challenges and noted that funding was insufficient to manage the increase in business volumes since the events of September 11, 2001, and their impact on security awareness. However, at the time of our audit, PWGSC had not allocated the funding levels to the Program that these business cases had identified as necessary. The Department has indicated that in June 2007 it submitted a request to the Treasury Board of Canada Secretariat for additional funding. According to the Department, the Industrial Security Program's current annual funding of $3 million covers about 42 of the 61 full-time equivalent (FTE) positions it had on 31 March 2007. The funding for the remaining 19 staff members comes from a departmental reserve on a year-to-year basis. Additionally, 29 positions were funded through temporary help.

1.55 Senior officials within the Industrial Security Program informed us that it is difficult for them to attract and retain qualified security professionals. They attribute this problem to the lack of sufficient and stable funding for the Program, which limits their ability to offer permanent employment to potential candidates. At 31 March 2007, according to the Department, roughly 28 percent of the positions in the Program were vacant and about 32 percent of the positions were filled with temporary staff.

1.56 **Information technology environment.** We examined the two primary information systems that support the Industrial Security Program. We expected that, given the sensitive nature of the information they contain, the Program would be able to demonstrate that its information technology systems met the security requirements of the Government Security Policy and the Management of Information Technology Security standard (MITS).

1.57 The Industrial Security Program's information resides on a separate network within the Department. Although access to information is controlled, and no incidents or security breaches have been reported, the Industrial Security Program was unable to provide evidence that its information systems have been certified as meeting the government's MITS standard. Program officials told us that the certification process had been delayed pending the availability of funding and resources.

1.58 We also found that the Department does not have a comprehensive disaster recovery plan for the information technology systems of the Industrial Security Program. In the event of a disaster, the absence of such a plan would impair its ability to resume operations within its recovery-time objectives. Up to five days of data could be lost if the current computing facilities were to become unusable or inaccessible.

1.59 **Recommendation.** Public Works and Government Services Canada should ensure that the Industrial Security Program has adequate resources to meet its program objectives.

Public Works and Government Services Canada's response. Agreed. PWGSC has long recognized the need for long-term stable funding to maintain the integrity of this program. The Department has allocated significant resources from its own reserves to maintain program integrity. While PWGSC will lead the effort in securing a long-term resource base, funding allocations are a joint responsibility with central agencies. The Department has initiated discussions with the central agencies on the subject of long-term stable funding.

1.60 **Recommendation.** Public Works and Government Services Canada should ensure that its secure information technology environment for the operations of the Industrial Security Program is certified, as mandated by the Government Security Policy. It should also review its departmental business continuity plan to determine whether it makes adequate provisions for the Industrial Security Program.

Public Works and Government Services Canada's response. Agreed. PWGSC is meeting the Treasury Board of Canada Secretariat timetable for the Management of Information Technology Security Action Plan, and it is expected that final certification will be completed by October 30, 2007. A review of the business continuity plan is currently under way and will be completed by September 30, 2007.

Other government organizations

National Defence and the Royal Canadian Mounted Police lack adequate guidance for industrial security activities

1.61 Over the last five years, National Defence and the Royal Canadian Mounted Police (RCMP) (together with Public Works and Government Services Canada) were among the departments with the highest number of sensitive contracts processed by the Industrial Security Program. In addition, both organizations also ensure the security of a large number of contracts awarded within their own delegated contracting authorities.

1.62 The staff of both National Defence and the RCMP need adequate guidance to ensure that sensitive information and assets are properly safeguarded. We expected that their security policies and procedures would be clear and comprehensive and would accurately reflect industrial security roles and responsibilities under the Government Security Policy.

1.63 National Defence policies and procedures are outdated and incomplete. We found that National Defence has a fairly comprehensive policy on security in contracting. However, the policy has not been revised to reflect a number of important security updates issued by the Treasury Board of Canada Secretariat over the last five years. For example, the policy has not incorporated the requirement that all individuals with regular access to federal information or physical assets and buildings have the required minimum security clearance. The implications of this requirement are substantial for the National Defence branches responsible for construction and maintenance projects. According to National Defence officials, it is costly, time-consuming, and administratively very difficult to properly incorporate security into a construction project. The departmental security officer told us that National Defence's industrial security policies are scheduled for revision and should be included in a new National Defence Security Manual planned for release in November 2007.

1.64 We also found that National Defence's Procurement Administration Manual, its main manual of operating procedures for procurement, was incomplete at the time of our audit. Departmental officials informed us of gaps in the Manual and noted that they were currently revising or creating sections to more adequately cover industrial security activities and the use of the Security Requirements Checklist. In addition, we noted that the Manual did not provide guidance to staff on security requirements for construction projects. The section on construction contracts awarded by Defence

Construction Canada (the contracting authority for defence construction projects) was developed during the time of our audit. However, the changes to the Manual have yet to be officially approved by Department.

1.65 We noted that Security Requirements Checklists have not been used consistently in National Defence. For example, one of the branches responsible for construction projects did not, with few exceptions, prepare a Checklist for any contracts issued between April 2002 and June 2006. Yet other branches in the Department accounted for about 36 percent of the Checklists processed by the Industrial Security Program during the same period.

1.66 During our audit, National Defence approved an interim directive to address the lack of clear and up-to-date guidance to staff about security requirements for construction projects. The Department also provided us with proposed revisions to existing policies on industrial security. While we did not review either of these in detail, they appear to be more comprehensive.

1.67 RCMP guidance is limited and not consistently followed. We found that the RCMP has only a few policies and procedures in place for industrial security, and those that do exist are inadequate. For example, the RCMP's Administration Manual does not specify who is responsible for completing the Security Requirements Checklist or to whom it must be forwarded for approval. We also found information in other department documents that conflicts with the guidance provided in the Manual. For example, the Manual states that a Checklist must be completed for all contracts for goods, services, and construction projects, regardless of whether or not security requirements exist. However, a document developed by the quality assurance group of the RCMP's procurement branch specifically states that a Checklist is required only for contracts for services and not for goods or construction projects. Officials told us they do not follow the Administration Manual because the requirement to complete a Checklist for all contracts is not administratively practical.

1.68 During our audit, the RCMP began to address the lack of clear and up-to-date guidance to staff and provided us with proposed revisions to existing policies and new draft policies for industrial security. While we did not review them in detail, these draft policies appear to be more comprehensive.

1.69 Recommendation. In completing their reviews of their industrial security policies and procedures, National Defence and the

Royal Canadian Mounted Police should each ensure that the policies and procedures are up-to-date and complete and that they accurately reflect the organization's roles and responsibilities under the Government Security Policy. These policies and procedures should be well communicated to staff and followed consistently.

National Defence's response. Agreed. The Defence Security Manual will have a revised chapter concerning Industrial Security. The Departmental Security Officer will also continue to work with stakeholders within National Defence to ensure that industrial security and the Government Security Policy are adequately reflected within departmental policy and procedures.

Royal Canadian Mounted Police's response. Agreed. The RCMP is in the process of reviewing and updating the internal policies and procedures related to contracting and industrial security requirements. In carrying out this activity, the RCMP will ensure that the policies and procedures are up-to-date and complete and that they accurately reflect the organization's roles and responsibilities under the Government Security Policy. Appropriate communication and monitoring actions will follow to ensure consistent application.

Contractors without appropriate security clearances received National Defence contracts

1.70 We looked at the industrial security procedures followed by National Defence for selected construction projects to see whether security requirements had been met during the contracting process. We found that industrial security was not considered on several construction projects.

1.71 **Industrial security at Defence Construction Canada.** Defence Construction Canada (DCC), a Crown corporation, is the contracting authority for government defence projects. It awards and manages contracts for the construction and maintenance of infrastructure. National Defence is the client for virtually all of DCC's business.

1.72 Under the Government Security Policy, the contracting authority is responsible for ensuring that individuals and corporations have been screened for security at the appropriate level, that sensitive information and assets are safeguarded, and that contract documentation includes the necessary security terms and conditions. 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 of Canada Secretariat. We found that there was neither an agreement with the Secretariat nor a Memorandum of

Understanding with National Defence that clearly establishes these responsibilities. In the absence of such agreements, no responsibility or obligation for industrial security has been formally conferred on DCC.

1.73 Since 1 April 2002, DCC has awarded more than 8,500 contracts on behalf of National Defence. The Corporation provided us with data indicating that National Defence had not provided a Security Requirements Checklist for about 99 percent of these contracts. As a result, neither the Department nor DCC had any assurance that contractors who received these contracts had been cleared to the appropriate security levels, as required by the Government Security Policy. To varying degrees, these contractors had free access to construction sites and project information that in many cases were sensitive. It is unknown whether or not information and assets have been compromised.

1.74 As a result of a failure to identify industrial security requirements during the pre-contract stage, as required by the Government Security Policy, unscreened contractors and workers had access to the plans and construction site of the North American Aerospace Defense (**NORAD**) Above Ground Complex in North Bay, Ontario. This building was designed to house very sensitive and highly classified material. Consequently, National Defence had to carry out an assessment to determine what additional steps were needed to ensure that the building could be used for the intended purposes (see "Results of missing security checks at NORAD Above Ground Complex," on page 25).

NORAD—A combined command established by mutual agreement between Canada and the United States. Based on available information, NORAD provides warning and assessment of air threats to the responsible authorities of each nation.

1.75 **Recommendation.** Defence Construction Canada and National Defence should establish an integrated framework for managing industrial security on defence projects in accordance with the requirements of the Government Security Policy.

National Defence's response. Agreed. National Defence will work with Defence Construction Canada to establish an integrated framework for managing industrial security on defence projects. In conjunction with the review of industrial security policies and procedures mentioned in our response to recommendation 1.69, National Defence will also assess whether sufficient direction is being provided with respect to defining and communicating our industrial security needs to Defence Construction Canada. In this regard, the Department has already released some interim direction on this subject that affects past, current, and future major construction and maintenance agreements.

Defence Construction Canada's response. Agreed. DCC supports the recommendation and will pursue an agreement with National Defence to clarify our respective roles and responsibilities in the management of industrial security and will develop internal security policies and procedures to ensure National Defence security requirements are met.

Results of missing security checks at NORAD Above Ground Complex

The NORAD Above Ground Complex in North Bay, Ontario, was intended to replace the underground complex housing the NORAD air surveillance and control system to secure North American airspace. This facility has an operationally vital role in North American security.

Given the intended purpose of the building, and as required by the Government Security Policy, a Security Requirements Checklist should have been completed for the Above Ground Complex to identify security requirements for the project and ensure that they were addressed before any contract was awarded. However, National Defence did not analyze the potential risks before awarding contracts. We noted that the departmental security office was aware that a Checklist had not been completed for the project. Nonetheless, due to time and budget constraints, the construction was completed without one. As a result, neither National Defence nor Defence Construction Canada ensured that security clearances had been completed for either the companies or site workers before construction began. At the time of our audit, the Industrial Security Program had not been asked to complete the security clearances for the majority of the 16 construction contractors and their personnel who had worked on the Above Ground Complex, including the main electrician.

In our May 2007 Report, Chapter 6, Modernizing the NORAD System in Canada, we reported that because a review of the building security requirements had not been completed prior to construction, several security concerns arose when the facility was being built. These concerns led to questions about the building and whether or not it can be used for the intended purposes. For example, Canadian and foreign contractors who were not cleared had access to the building plans and the construction site. National Defence does not know whether information or the building itself has been compromised.

In the opinion of National Defence, after more than a year of investigations and meetings, it has determined that, with modifications, the building can be used for its intended purpose. It expects the majority of the modifications and systems to be in place by mid-September 2007. At the time of our audit, the Department had not yet provided us with detailed plans, including security considerations, schedules, and costs for the required modifications.

1.76 Re-assessment of project security requirements. As a result of missing security checks for the construction of the NORAD Above Ground Complex, the Infrastructure and Environment Branch of National Defence reviewed recent and active projects to assess the security requirements of each. According to department officials, this Branch accounts for about 40 percent of the Department's construction and maintenance contracts. During its review, the Branch identified 176 projects at various stages of development. The Branch provided us with information indicating that it has recently completed or will

complete a Security Requirements Checklist after-the-fact for over 100 of these projects.

1.77 Although National Defence has indicated that it is identifying security requirements for projects already under way, there is still a risk that contracts will be awarded before the contractors' clearances have been completed. Department officials indicated that the lengthy process of completing the security screening of contractors was causing delays in the awarding of contracts. In the case of one project, the departmental security officer issued a waiver allowing contracts to be awarded before the contractors had received the appropriate security clearances, in order to maintain project timelines and to avoid having the Department incur penalties for delaying the contractors' work. Department officials noted that they are taking steps to compensate for the lack of security clearances for projects under way, by either removing sensitive information from documents or escorting and supervising individuals on work sites. In our opinion it is important for the Department to recognize and build into its processes, the time and costs associated with implementing proper security before and during construction projects.

1.78 **Recommendation.** The Treasury Board of Canada Secretariat should revise the Government Security Policy's standard on security in contracting to require that for every proposed procurement, departments identify the security requirements by completing a Security Requirements Checklist or else certify that there are no security requirements. The Checklist or the certification should be provided to the contracting authority along with the contract requisition form.

Treasury Board of Canada Secretariat's response. Agreed. The Treasury Board Secretariat will update the Standard on Security in Contracting in order to clarify this requirement, as part of the renewed policy on government security.

Industrial security oversight

Departmental security officers in the three organizations lack assurance that government requirements for industrial security are being met

1.79 The Government Security Policy requires that a departmental security officer in each department establish and direct a security program. The program should ensure that all security policy functions, including security in contracting, are coordinated and that departments fulfill all security policy requirements. In addition, departments must actively monitor their security programs and carry out internal audits of them.

1.80 We examined the policies and procedures that Public Works and Government Services Canada (PWGSC), National Defence, and the Royal Canadian Mounted Police (RCMP) have to support departmental security officers in their responsibilities. We also interviewed the departmental security officers to determine whether they have established mechanisms to provide them with assurance that sensitive information and assets entrusted to industry are adequately protected.

1.81 We found that management oversight of industrial security in each of these organizations was lacking. Specifically, we found that the departmental security officers in all three organizations had few mechanisms, such as a contract **quality assurance** program, to provide them with assurance, for example, that a Security Requirements Checklist has been completed for all contracts. The departmental security officers noted that industrial security had not been identified as a major departmental risk. We found no evidence of regular reporting to departmental security officers on industrial security and no formal challenge functions to identify non-compliance with critical procedures.

Quality assurance—A practice that allows management to re-examine transactions and to monitor compliance with policies and procedures.

1.82 The RCMP is the only organization of those we looked at where we found mechanisms for monitoring security in contracting. The RCMP's procurement branch has a Contract Quality Assurance program that conducts post-contract reviews. According to RCMP documents, a recent review looked at whether 679 contracts awarded by the RCMP between January 2005 and March 2007 had met two criteria for industrial security—completion of a Security Requirements Checklist where security requirements have been identified, and contract terms and conditions that reflect the identified security requirements. The review found that approximately 15 percent of the 180 contracts with security requirements did not have a Checklist on file. In about 10 percent of the contracts that required and had a Checklist on file, the security requirements identified in the Checklist were not reflected in the terms and conditions of the contract.

1.83 **Recommendation.** The Treasury Board of Canada Secretariat should require that departments and agencies implement a quality assurance program that includes reviewing contract files to verify that they meet industrial security requirements.

Treasury Board of Canada Secretariat's response. Agreed. The Treasury Board Secretariat will include this requirement in the responsibilities of departmental security officers under the renewed policy on government security.

The Treasury Board of Canada Secretariat's monitoring of industrial security objectives is insufficient

1.84 We examined how the Treasury Board Secretariat ensures that departments are complying with the industrial security requirements of the Government Security Policy. We also looked at how it monitors the effectiveness of the Policy.

1.85 The current practices of the Treasury Board Secretariat—carrying out a security survey, meeting with departmental security officers to discuss the Government Security Policy, and communicating regularly with members of the security community— are not sufficient to provide assurance that the government's industrial security objectives are being met government-wide. Nor do the departmental security officers have the necessary mechanisms in place to provide such assurance, as we have already noted.

1.86 Although the Government Security Policy requires that each department complete an internal audit of its departmental security program, Secretariat officials told us that it has received only five internal audit reports on these programs since 2002—and only one of them touched on security in contracting. None of the three organizations we examined had completed an audit of either its security program or industrial security. Therefore, they were unable to provide reports or formal assurance to the Secretariat that they were meeting the industrial security objectives of the Policy.

1.87 The Treasury Board Secretariat produced a report for the Treasury Board on the effectiveness of the Policy, based on a survey of departmental security officers and interviews with them. It noted that in general, the majority of departments and agencies were not meeting the requirements of the Policy. However, it also noted a high degree of departmental compliance with the Policy's security requirements for contracts awarded by PWGSC as the contracting authority, which is not consistent with the findings of our audit.

1.88 In our opinion, based on the information the Secretariat receives from departments, it can determine neither that the Government Security Policy is being implemented properly nor that the objectives of the Policy are being met government-wide.

1.89 **Recommendation.** The Treasury Board of Canada Secretariat should ensure that it obtains timely and sufficient information from deputy heads of federal organizations to ensure that they are fulfilling their obligations under the Government Security Policy.

Treasury Board of Canada Secretariat's response. Agreed. The specific accountabilities of deputy heads will be clarified in the renewed policy. Furthermore, Treasury Board Secretariat is adding an indicator under the Management Accountability Framework to assess the departmental performance against the Business Continuity and Security requirements.

Conclusion

1.90 We have concluded that roles and responsibilities for security in the federal government's contracting are unclear and that accountability is lacking. The government does not know to what extent it is exposed to risks as a result of less-than-adequate industrial security—in particular, the awarding of contracts to individuals and firms who have not been properly cleared for security.

1.91 Weaknesses in the process set up to ensure security in contracting are present in the three organizations we audited and at almost all levels within them. 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.

1.92 We have also concluded that the Treasury Board of Canada Secretariat cannot provide the government with assurance that the process for ensuring security in contracting is adequate to meet the government's industrial security objectives. A key reason for this is that departments do not routinely provide the Secretariat with complete and accurate summary information on measures taken within their own organizations to ensure industrial security.

1.93 In addition, we found that Public Works and Government Services Canada does not have adequate policies and procedures in place to support its Industrial Security Program. The current standard operating procedures are incomplete and in draft form. As a result, informal practices have evolved within the Program, and even these are not followed consistently.

1.94 Failing to protect information entrusted to individuals and companies under contract to the government can pose serious risks to the national interest. A concerted effort to strengthen accountability, to clarify policies, and to better define roles and responsibilities for security in contracting is required to help to reduce these risks.

About the Audit

Objectives

The objectives of the audit were to determine whether

- the roles and responsibilities for security in government contracting are clear, and if entities have procedures in place to meet these roles and responsibilities;
- the Treasury Board of Canada Secretariat has assurance that the government's industrial security objectives are being met on a government-wide basis; and
- Public Works and Government Services Canada has adequate procedures in place for its Industrial Security Program, and is following them.

Scope and approach

In our audit, we reviewed departmental policies, procedures, and practices of Public Works and Government Services Canada (PWGSC), National Defence, and the Royal Canadian Mounted Police (RCMP) to determine if they were clear and consistent with the Treasury Board policies. We also looked at them to determine if they had been properly communicated to all parties involved in safeguarding sensitive government information and assets entrusted to contractors engaged by the federal government, so that they were fully aware of their roles and responsibilities. Specifically, we examined the roles and responsibilities of the three departments and the role of the Treasury Board of Canada Secretariat for security in contracting under the Government Security Policy. In addition, we reviewed the policies and procedures of Defence Construction Canada (DCC), the procurement agent for government defence projects related to industrial security.

The audit team interviewed officials at PWGSC in the following directorates: Corporate Security; Canadian and International Industrial Security; and Electronics, Munitions and Tactical Systems Procurement. We interviewed officials at National Defence in the following groups: Deputy Provost Marshal Security, Assistant Deputy Minister (Materiel), and Assistant Deputy Minister (Infrastructure and Environment). We also interviewed officials at the RCMP in the Assets and Procurement Branch and the Security Unit. In addition, the team interviewed personnel at DCC.

We examined the Treasury Board Secretariat's role in monitoring the implementation and effectiveness of the security in contracting requirements of the Policy, and in reporting on the results to the Treasury Board. We reviewed authoritative documentation to assess whether the Secretariat fulfills its roles and responsibilities for policy oversight and how it accomplishes this.

Finally, we focused on the specific activities of PWGSC in its delivery of the Industrial Security Program. This included a detailed examination of the operating procedures in place to administer the Program, as well as a review of the financial resources, personnel, and information technology infrastructure in place within PWGSC to support the Program in discharging its industrial security responsibilities. We did not examine the international components of PWGSC's Industrial Security Program; nor did we look at the activities of the Controlled Goods Program. Our audit was not designed to assess whether or not breaches of security actually have occurred.

We selected for review files of all organizations who had been cleared, with Document Safeguarding Capability, to the "secret" level; who had been entered into the Industrial Security Program database for the first time on or after 1 April 2002; and who had received at least one contract prior to 31 March 2007. Files for the 55 contractors were compared against the Program's standard operating procedures and established practices to ensure compliance.

Our audit covered transactions during the period from 1 April 2002 to 31 March 2007.

Criteria

We expected to find that

- roles and responsibilities within the federal government for industrial security are clear,
- entities have adequate procedures in place to discharge their industrial security responsibilities under the Government Security Policy,
- the Treasury Board of Canada Secretariat monitors departmental compliance with the industrial security requirements of the Government Security Policy,
- the Treasury Board of Canada Secretariat monitors the effectiveness of the Government Security Policy and reports on the results to the Treasury Board,
- PWGSC's operating procedures for the Industrial Security Program ensure completeness and accuracy of information required to fulfill its mandate,
- PWGSC's operating procedures for the Industrial Security Program allow the Department to know whether company security officers are in compliance with the Industrial Security Manual,
- PWGSC has assurance that its standard operating procedures for the Industrial Security Program are being followed,
- PWGSC has adequate staff to administer the Industrial Security Program, and
- PWGSC is safeguarding its own information.

Audit work completed

Audit work for this chapter was substantially completed on 17 August 2007.

Audit team

Assistant Auditor General: Ronnie Campbell
Principal: Bruce C. Sloan
Director: Karen Hogan

Mathieu Lefèvre
John McGrath
Étienne Robillard
Julie Taylor

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

Appendix List of recommendations

The following is a list of recommendations found in Chapter 1. The number in front of the recommendation indicates the paragraph where it appears in the chapter. The numbers in parentheses indicate the paragraphs where the topic is discussed.

Recommendation	Response
Industrial security policy framework	
1.21 The Treasury Board of Canada Secretariat should ensure consistency among the Government Security Policy and the associated directives, standards, and guidelines. **(1.17–1.20)**	The Treasury Board Secretariat is in the process of reviewing the policy on government security. The current policy was issued in 2002 and is due for renewal at the five-year mark. The review is currently under way, and the new policy is expected to be completed at the end of summer 2008. Under the Policy Suite Renewal initiative, the structure of policy instruments is being clarified, and ambiguity in the language in the policy on government security is being addressed. The accountabilities of deputy heads are also being clarified, in terms of delineating mandatory requirements from guidelines and best practices.
Public Works and Government Services Canada	
1.51 Public Works and Government Services Canada should ensure that before it awards a contract, it has received from the client department a completed Security Requirements Checklist identifying the necessary security requirements, or a certification that there are none. **(1.22–1.50)**	Public Works and Government Services Canada's response. Agreed. PWGSC has interpreted and applied the Government Security Policy in a manner that is consistent with the interpretation of the Treasury Board Secretariat, National Defence, and RCMP, as noted in paragraph 1.19. As also noted, the OAG interprets the Government Security Policy in a different manner. The OAG has made a recommendation to the Treasury Board Secretariat on this issue in paragraph 1.78, and the chapter notes that the Treasury Board Secretariat plans to update the Standard. PWGSC will comply with the Treasury Board Secretariat-revised Standard. In the meantime, PWGSC will implement a certification process.

Recommendation	Response
1.52 Public Works and Government Services Canada should ensure that it completes the development and approval of standard operating procedures for the Industrial Security Program and that they are consistently followed. **(1.22–1.50)**	Industrial Security Program procedures are being finalized and will be issued in final form by September 30, 2007. Further, PWGSC has established a robust action plan to address the recommendations and all the other weaknesses identified in this report. Internal Audit will follow up to monitor implementation.
1.59 Public Works and Government Services Canada should ensure that the Industrial Security Program has adequate resources to meet its program objectives. **(1.53–1.55)**	PWGSC has long recognized the need for long-term stable funding to maintain the integrity of this program. The Department has allocated significant resources from its own reserves to maintain program integrity. While PWGSC will lead the effort in securing a long-term resource base, funding allocations are a joint responsibility with central agencies. The Department has initiated discussions with the central agencies on the subject of long-term stable funding.
1.60 Public Works and Government Services Canada should ensure that its secure information technology environment for the operations of the Industrial Security Program is certified, as mandated by the Government Security Policy. It should also review its departmental business continuity plan to determine whether it makes adequate provisions for the Industrial Security Program. **(1.56–1.58)**	PWGSC is meeting the Treasury Board of Canada Secretariat timetable for the Management of Information Technology Security Action Plan, and it is expected that final certification will be completed by October 30, 2007. A review of the business continuity plan is currently under way and will be completed by September 30, 2007.

Recommendation	Response
Other government organizations	
1.69 In completing their reviews of their industrial security policies and procedures, National Defence and the Royal Canadian Mounted Police should each ensure that the policies and procedures are up-to-date and complete and that they accurately reflect the organization's roles and responsibilities under the Government Security Policy. These policies and procedures should be well communicated to staff and followed consistently. **(1.61–1.68)**	The Defence Security Manual will have a revised chapter concerning Industrial Security. The Departmental Security Officer will also continue to work with stakeholders within National Defence to ensure that industrial security and the Government Security Policy are adequately reflected within departmental policy and procedures. The RCMP is in the process of reviewing and updating the internal policies and procedures related to contracting and industrial security requirements. In carrying out this activity, the RCMP will ensure that the policies and procedures are up-to-date and complete and that they accurately reflect the organization's roles and responsibilities under the Government Security Policy. Appropriate communication and monitoring actions will follow to ensure consistent application.
1.75 Defence Construction Canada and National Defence should establish an integrated framework for managing industrial security on defence projects in accordance with the requirements of the Government Security Policy. **(1.70–1.74)**	National Defence will work with Defence Construction Canada to establish an integrated framework for managing industrial security on defence projects. In conjunction with the review of industrial security policies and procedures mentioned in our response to recommendation 1.69, National Defence will also assess whether sufficient direction is being provided with respect to defining and communicating our industrial security needs to Defence Construction Canada. In this regard, the Department has already released some interim direction on this subject that affects past, current, and future major construction and maintenance agreements. DCC supports the recommendation and will pursue an agreement with National Defence to clarify our respective roles and responsibilities in the management of industrial security and will develop internal security policies and procedures to ensure National Defence security requirements are met.

Recommendation	Response
1.78 The Treasury Board of Canada Secretariat should revise the Government Security Policy's standard on security in contracting to require that for every proposed procurement, departments identify the security requirements by completing a Security Requirements Checklist or else certify that there are no security requirements. The Checklist or the certification should be provided to the contracting authority along with the contract requisition form. **(1.61–1.77)**	The Treasury Board Secretariat will update the Standard on Security in Contracting in order to clarify this requirement, as part of the renewed policy on government security.
Industrial security oversight	
1.83 The Treasury Board of Canada Secretariat should require that departments and agencies implement a quality assurance program that includes reviewing contract files to verify that they meet industrial security requirements. **(1.79–1.82)**	The Treasury Board Secretariat will include this requirement in the responsibilities of departmental security officers under the renewed policy on government security.
1.89 The Treasury Board of Canada Secretariat should ensure that it obtains timely and sufficient information from deputy heads of federal organizations to ensure that they are fulfilling their obligations under the Government Security Policy. **(1.84–1.88)**	The specific accountabilities of deputy heads will be clarified in the renewed policy. Furthermore, Treasury Board Secretariat is adding an indicator under the Management Accountability Framework to assess the departmental performance against the Business Continuity and Security requirements.

Report of the Auditor General of Canada to the House of Commons—October 2007

Main Table of Contents