CHAPTER 2

Status Report on Security in Contracting

Performance audit reports

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

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

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

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

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

Cat. No. FA1-2013/1-2E-PDF
ISBN 978-1-100-21902-8
ISSN 1701-5413

Table of Contents

Status Report on Security in Contracting

Main Points

What we examined

The government regularly contracts with private sector firms and their staff to undertake work or obtain expertise to meet its objectives. These individuals and firms may be required to access protected or classified government information and assets to complete the work they have been contracted to do.

The guidelines and standards for government security activities that departments are expected to follow are set out in the Treasury Board Policy on Government Security (2009), which replaced the 2002 Government Security Policy. Public Works and Government Services Canada (PWGSC) is responsible for providing leadership and for coordinating activities that help ensure the application of security safeguards in the contracting process within the scope of the Industrial Security Program.

Departments are individually responsible for protecting sensitive information and assets under their control, and this requirement applies at all stages of the contracting process. They rely on the personnel security of the contractor (screening, education, and sanctions of contractors) to safeguard government information and assets. Should a private sector firm retain information at its work site, departments also rely on the inspection of the physical security of the firm's facilities (location and design of facilities and physical measures to prevent, detect, and respond to unauthorized access at the contractor's place of business).

Our 2007 audit included five entities—The Treasury Board of Canada Secretariat, PWGSC, National Defence, Defence Construction Canada, and the Royal Canadian Mounted Police. We examined how these entities were implementing the Government Security Policy (2002) and its related operational and technical standards. We found that weaknesses in the Policy led to uncertainty about responsibilities and accountability for security in contracting and about the effectiveness of the security in contracting processes. We concluded that the roles and responsibilities for security in the federal government's contracting were unclear and that accountability was lacking.

In this audit, we followed up with the same entities to determine whether they have made satisfactory progress in addressing the issues we reported in 2007. We focused on the policies and processes in place to safeguard classified information and assets in these entities as well as two other security agencies that were not included in our 2007 audit—the Canadian Security Intelligence Service and Communications Security Establishment Canada.

Audit work for this chapter was completed on 3 December 2012. Details on the conduct of the audit are provided in **About the Audit** at the end of the chapter.

Why it's important

The Treasury Board Policy on Government Security (2009) outlines the government's roles and responsibilities for protecting information, assets, and individuals. This assists in ensuring the government's ability to achieve its objectives related to security and to safeguard the health, safety, security, and economic well-being of Canadians.

Given the potentially significant consequences that could arise if protected or classified information or assets were to be compromised, the government must manage sensitive assets and information held within its own departments and entrusted to external parties to ensure that they are protected from unauthorized access, disclosure, removal, modification, use, or interruption.

What we found

- Overall, progress has been unsatisfactory in implementing the commitments made in response to our 2007 recommendations. Although the government has made a number of improvements, including providing clearer requirements for departments to monitor and report on their security programs, in our opinion significant weaknesses remain. There is a gap in the 2009 Policy on Government Security as well as the Security and Contracting Management Standard, as they do not explicitly address the clearance of private sector firms with access to protected and classified information. In addition, departments use a variety of practices to identify whether a contract security requirement exists or not. As a result, contracts are sometimes awarded to those who lack the appropriate security clearance.
- PWGSC has implemented standard operating procedures. It does not award a contract on behalf of client departments until it receives a completed Security Requirement Check List or an attestation that no security requirement exists. Funding for the Industrial Security Program has been provided through cost recovery from client departments. PWGSC has not been able to demonstrate whether

the charging methodology is appropriate for the services being provided. Further, more than 1,400 security clearances at the secret level have been in process for almost eight months.

- The Canadian Security Intelligence Service (CSIS), Communications Security Establishment Canada (CSEC), and the Royal Canadian Mounted Police's policies and procedures provide assurance beyond the level required by the Policy on Government Security. CSIS, CSEC, Defence Construction Canada, and Public Works and Government Services Canada comply with the Policy on Government Security and have put in place security policies, a departmental security plan, and a Departmental Security Officer or Corporate Security Officer. However, the departmental security plan for the RCMP has not yet been approved and National Defence has not yet developed its plan. In the contract files we examined, CSIS consistently included security requirements in contracts, while National Defence and the RCMP did not. Defence Construction Canada included requirements to the extent that they had been communicated by National Defence. CSEC included security requirements in contracts, but requirements for clearances of firms were not met at the time the contract was awarded.

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

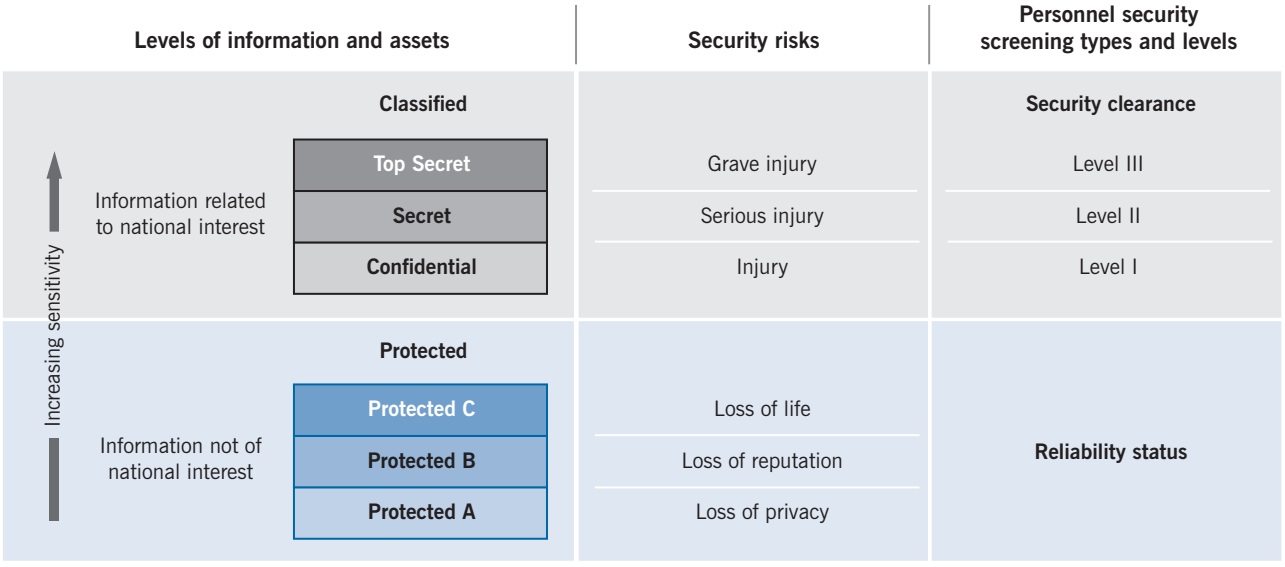
Introduction

2.1 Government information and assets can be accessed not only by federal employees but also by contracted private sector individuals and firms that provide services to the government. The security of government information and assets entrusted to private sector contractors (also known as industrial security) must therefore be managed to ensure protection against unauthorized access, disclosure, removal, modification, use, or interruption.

Sensitive government information and assets—Information and assets that are either protected or classified. The disclosure of protected information and assets could harm personal or commercial interests. The disclosure of classified information and assets could harm the national interest.

2.2 The government first needs to determine whether prospective contractors who will have access to **sensitive government information and assets** are trustworthy, reliable, and loyal. This is determined through security screening, which helps to ensure that the government's information and assets will be kept secure when entrusted to a contractor, whether an individual or a firm. The level of security required for access depends on the severity of the consequences that might reasonably be expected if the information were compromised (Exhibit 2.1).

Exhibit 2.1 Types of information and personnel screening



Source: Adapted from the Policy on Government Security (Treasury Board, 2009)

Roles and responsibilities for government security

2.3 The 2009 Policy on Government Security is supported by directives, standards, and guidelines. The Security and Contracting Management Standard is the operational standard for identifying security requirements in the contracting process.

2.4 The Policy's objectives are to ensure that deputy heads effectively manage security activities within their departments and contribute to effective government-wide security management. The Policy outlines key responsibilities for deputy heads and also identifies lead security agencies and their roles.

2.5 Lead security agencies provide advice, guidance, and services to support the day-to-day security operations of departments. They enable government as a whole to effectively manage security activities, coordinate a response to security incidents, and achieve and maintain an acceptable state of security readiness. The Policy describes the responsibilities of lead security agencies in relation to their areas of expertise. Exhibit 2.2 summarizes the roles and responsibilities regarding security in contracting.

Key elements of security in contracting

2.6 Each federal department is responsible for protecting sensitive information and assets under its control—not only in its own operations but also through all phases of the contracting process and while in the possession of contractors. It is also responsible for identifying any security requirements that must be included in its contracts.

2.7 **Industrial Security Program.** Public Works and Government Services Canada (PWGSC) is responsible for providing leadership and for coordinating activities that help ensure the application of security safeguards in the contracting process within the scope of the Industrial Security Program when the Department is the contracting authority or upon client request.

2.8 **Contract security requirements.** According to the Security and Contracting Management Standard, a department has two options to ensure security in contracts that involve access to sensitive government information and assets and are within the department's approved contracting authority. The department either uses its own internal processes to conduct the security screening to ensure that the contractor meets the appropriate security requirements or requests that PWGSC perform this task through the Industrial Security Program.

2.9 When contracts involving access to sensitive information and assets are above a department's approved contracting authority, PWGSC is responsible for ensuring that the contractor meets the appropriate security requirements.

2.10 The key processes for security in contracting include personnel security screening of the contractor and screening of the contractor's firm (called **facility security clearance**). Each of the entities we audited also conducts additional activities to reflect their particular security requirements, including background checks on individuals, criminal record checks, interviews, and monitoring after the contract is awarded, as required.

Facility security clearance—Approval granted to a private sector firm to access classified information and assets at the level of confidential, secret, or top secret, depending on the level of the information and assets to be accessed. The clearance grants access to certain individuals—key senior officials—in addition to those who will be working on the contract. Where applicable, clearance may also include an assessment of the firm's physical security and its information systems.

Exhibit 2.2 Key roles and responsibilities for security in contracting

Who	Key roles and responsibilities
Deputy heads	• Establish a security program • Appoint a departmental security officer • Approve the departmental security plan • Ensure that all individuals with access to government information and assets are security screened at the appropriate level before starting their duties • Ensure security incidents are investigated • Ensure periodic reviews are conducted to assess whether the departmental security program is effective, objectives outlined in the departmental security plan were achieved, and the departmental security plan remains appropriate to the needs of the department and government as a whole • Report periodically to the Treasury Board of Canada Secretariat on the status and progress of the Policy's implementation and on results of ongoing performance measurement
Treasury Board of Canada Secretariat	• Monitor compliance with the Policy and the achievement of expected results • Review and report to Treasury Board on the effectiveness and implementation of the Policy and its directives and standards five years from its effective date
Deputy heads of lead security agencies	• Provide departments with advice, guidance, and services related to government security, consistent with their mandated responsibilities • Appoint an executive to coordinate and oversee provision of support services to departments and represent the deputy head to the Treasury Board of Canada Secretariat in this regard • Ensure that the security support services provided help government departments achieve and maintain an acceptable state of security and readiness and that those services remain aligned with government-wide policies related to government security • Ensure that periodic reviews are conducted to assess the effectiveness of their security support services • Report on their activities under the Policy through current government reporting mechanisms

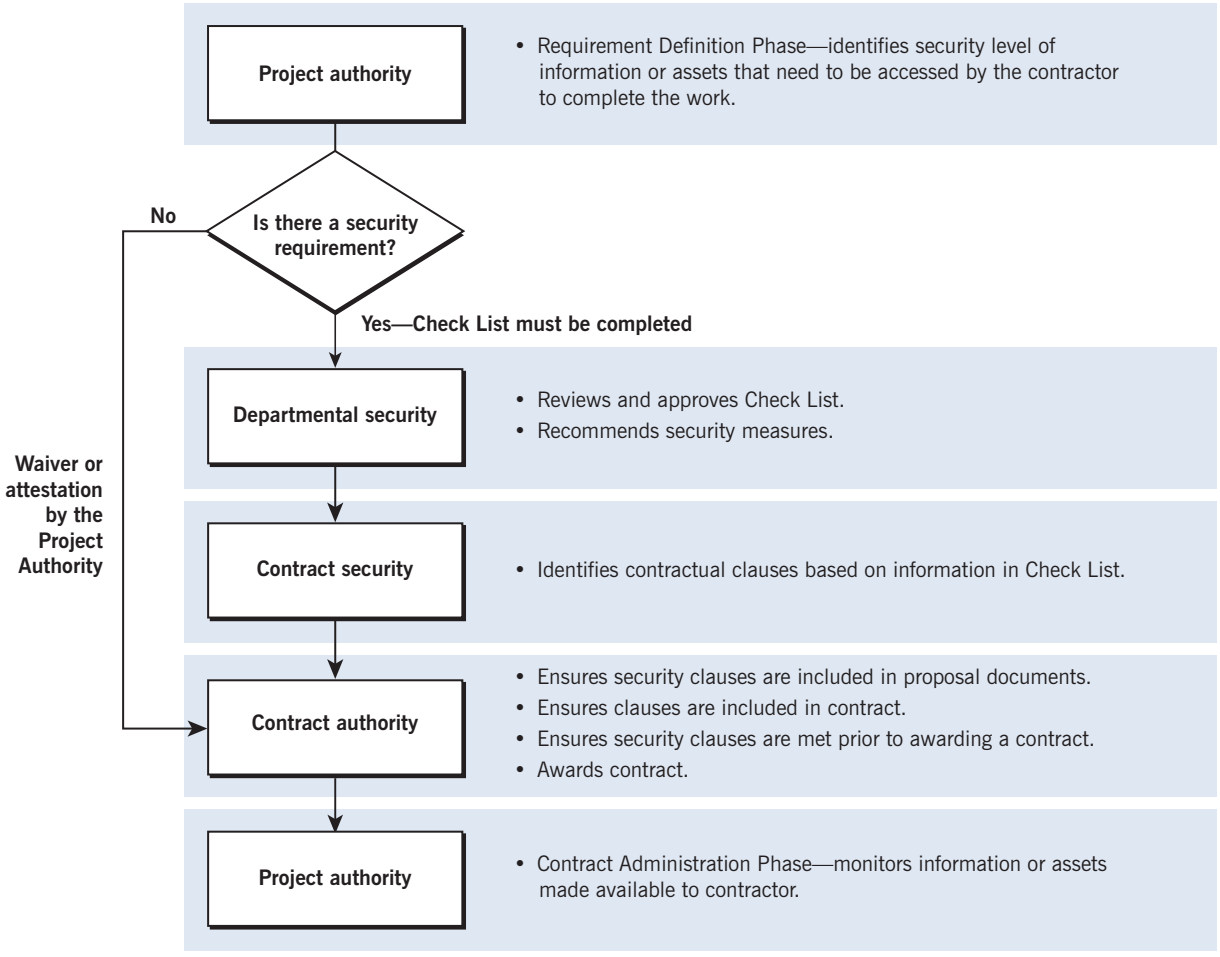
Source: Adapted from the Policy on Government Security (Treasury Board, 2009)

2.11 **Security Requirements Check List.** Each department is responsible for assessing and identifying any security requirements in its contracts. A Security Requirements Check List must be used when PWGSC is the contracting authority for a department. The Security and Contracting Management Standard also recommends that a department use the Check List when it retains contracting authority. This process to complete the Security Requirements Check List is shown in Exhibit 2.3.

What we found in 2007

2.12 Our 2007 audit examined whether government departments had taken the measures necessary to protect sensitive information and assets that it makes available to industry in the course of contracting. Federal entities selected for audit included the Treasury Board of

Exhibit 2.3 **Process to complete the Security Requirements Check List**



Source: Adapted from the Public Works and Government Services Canada Supply Manual and Treasury Board of Canada Secretariat Instructions for Completion of a Security Requirements Check List

Canada Secretariat, Public Works and Government Services Canada, National Defence, Defence Construction Canada, and the Royal Canadian Mounted Police.

2.13 We reported that weaknesses in the framework that supports the Government Security Policy led to uncertainty about responsibilities and accountability for security in contracting and the effectiveness of the process. As a result, many federal contracts that provided access to sensitive government information and assets had been awarded to firms and their personnel without the appropriate security clearance. In addition, we found that some contracts with clearly identified security requirements had been completed before the security requirements were met.

2.14 We also reported serious security concerns at an above-ground NORAD complex designed to handle highly classified information. These deficiencies included inadequate security for physical access to the complex and access by contractors without a security clearance.

2.15 Stable funding for the Industrial Security Program was not in place; PWGSC relied on temporary funding from the Deputy Minister's reserve for close to one third of the Industrial Security Program's permanent workforce.

Events since 2007

2.16 **Revised policy.** Effective 1 July 2009, Treasury Board replaced the Government Security Policy (2002) with the Policy on Government Security, which outlines the government's roles and responsibilities for protecting information, assets, and individuals.

2.17 **Task force recommendations.** Shortly after the publication of our 2007 audit report, the interdepartmental Deputy Minister Committee on National Security commissioned a task force to review the federal government's security screening process.

2.18 The task force issued its report and recommendations in 2009. The Committee endorsed the report and requested that the Treasury Board of Canada Secretariat implement the recommendations. The Secretariat drafted a proposal but determined in 2009 that funding was not available in the 2010–11 fiscal year to address the recommendations. As a result, work on the proposal was halted.

2.19 **PWGSC funding solution.** Over the past five years, Public Works and Government Services Canada has sought the needed funding for the Industrial Security Program. In 2010, Treasury Board

approved a cost recovery initiative beginning in the 2011–12 fiscal year and for subsequent years, enabling PWGSC to recover costs from client departments and agencies for services provided by the Industrial Security Program.

Focus of the audit

2.20 The audit work for this status report looked at what the government has done to address the issues that gave rise to our 2007 recommendations. Our objective was to determine whether the Treasury Board of Canada Secretariat, Public Works and Government Services Canada (PWGSC), and selected departments and agencies have made satisfactory progress in addressing issues we raised in the Auditor General's October 2007 Report, Chapter 1, Safeguarding Government Information and Assets in Contracting.

2.21 The current audit included all of the entities covered in our 2007 audit. In addition, we included Communications Security Establishment Canada and the Canadian Security Intelligence Service, given their responsibilities as lead security agencies, their focus on security, and the nature of the information they need to conduct their work.

2.22 The audit focused on the policies and processes related to safeguarding classified information and assets. We examined

- the requirements of the Policy on Government Security and its associated directives and standards, and the entities' level of compliance;
- PWGSC's policies and procedures related to the Industrial Security Program; and
- compliance by the selected lead security agencies with their internal policies and processes related to security in contracting.

2.23 The audit covered the security screening process for contracts issued in the 2011–12 fiscal year. We also looked at earlier actions taken by the government in response to our 2007 audit, including the development and implementation of the 2009 Policy on Government Security.

2.24 As part of our audit, we relied on PWGSC's internal audit of the Industrial Security Program undertaken to determine PWGSC's progress on implementing our 2007 recommendations. Where its scope and the period covered coincided with those of our follow-up audit, we have included the internal audit's results in this chapter.

2.25 More details about the audit objectives, scope, approach, and criteria are in **About the Audit** at the end of this chapter.

Observations and Recommendations

Policy on Government Security

2.26 In 2007, we found that the Security and Contracting Management Standard, which outlines how departments were to implement the Government Security Policy in contracting, was ambiguous, contributing to confusion about responsibilities under the Policy. We recommended that the Treasury Board of Canada Secretariat ensure consistency among the Government Security Policy and its associated directives, standards, and guidelines.

2.27 We also found in 2007 that the use of the Security Requirements Check List across departments was inconsistent, and there was little assurance that contractors had been cleared to the appropriate security levels. We recommended that the Secretariat revise the Security and Contracting Management Standard to require that, before awarding a contract, departments identify security requirements either by completing the Check List or by certifying that there are no security requirements.

The Security and Contracting Management Standard has not been revised, and policy changes leave clearances of firms unaddressed

2.28 In our follow-up audit, we examined the changes incorporated in the 2009 Policy on Government Security and supporting directives, standards, and guidelines. We found that the Policy now includes expectations for deputy heads, as well as clearer requirements for departments to monitor their security programs and their implementation of the Policy. The Policy also requires lead security agencies to report on the effectiveness of their security support services.

2.29 We found that some of the directives, standards, and guidelines supporting the 2009 Policy have also been updated. However, the Security and Contracting Management Standard was not revised and has not been updated since 1996. In 2008, the Treasury Board of Canada Secretariat provided some additional guidance to departmental security officers on the application of the policy. Unlike the previous version of the Policy, the 2009 Policy does not state whether contracted firms with access to protected and classified information are required to hold a security clearance. In our opinion, this is an important gap that could result in inconsistent application of the Policy and thus introduce additional security risk.

2.30 Since the Policy was implemented, some of the entities in our audit have developed their own systems and procedures for implementing security in contracting. This has led to inconsistent practices for security in contracting. The Secretariat is in the process of revising the Standard. For example, we found that the RCMP and National Defence were not always completing the Security Requirements Check List to identify a security requirement. Instead, while recognizing that a security requirement existed, they were using other methods to avoid the lengthy security clearance process and mitigate the risks. In some cases, departments arranged for an uncleared contractor to be escorted by an individual with a security clearance, thereby allowing the uncleared contractor to perform work on a site that requires a specific level of security clearance. For certain National Defence projects where Defence Construction Canada was the contract authority, the area where the contractor was required to complete work was declassified. While meeting operational requirements, this practice introduces additional security risks.

2.31 In summary, the changes to the Government Security Policy fall short of addressing our 2007 recommendations (Exhibit 2.4). The concerns outlined in our 2007 audit remain. We encourage the Treasury Board of Canada Secretariat to complete and issue the revised Security and Contracting Management Standard on a timely basis and provide clarification on clearances of firms.

Exhibit 2.4 Unsatisfactory progress in addressing recommendations on the policy framework for security in contracting

Recommendation from 2007 audit	Progress
1.21 The Treasury Board of Canada Secretariat should ensure consistency among the Government Security Policy and the associated directives, standards, and guidelines.	**Unsatisfactory**
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.	**Unsatisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

2.32 **Recommendation.** The Treasury Board of Canada Secretariat, in consultation with Public Works and Government Services Canada and the lead security agencies, should address the security risks related to the absence of a specific requirement to security screen private sector firms and ensure consistency among the Policy on Government Security and associated directives, standards, and guidance.

The Secretariat's response. Agreed. Deputy heads are responsible for the management of security within their organizations, and the Treasury Board of Canada's current policy instruments already require that all individuals (which includes contractors) with access to government information and assets be security screened. With this understanding, the Treasury Board of Canada Secretariat, in consultation with Public Works and Government Services Canada and the lead security agencies, will address the security risks, as identified in this report, which may arise as the result of the absence of a specific requirement to security screen private sector firms. The Treasury Board of Canada Secretariat will also ensure consistency across the Policy on Government Security, including its related directives, standards, and guidelines. This will be accomplished as part of the current security policy suite renewal activities and the update to the Security and Contracting Management Standard, which is planned for summer 2013.

Requirements have been established to improve oversight of security in contracting

2.33 In 2007, we found that some of the audited entities lacked an adequate process for managing their oversight of security in contracting. We recommended that the Treasury Board of Canada Secretariat require departments and agencies to implement a quality assurance program, including the review of contract files to verify that they meet security in contracting requirements.

2.34 We also found in 2007 that the Treasury Board of Canada Secretariat's practices were not sufficient to provide assurance that federal objectives for security in contracting were being met across the government. We recommended that the Secretariat ensure that it obtains timely and sufficient information from deputy heads of federal departments to determine that they are fulfilling their obligations under the Policy.

2.35 Our follow-up audit examined actions taken since 2007 to respond to these two recommendations. We found that the 2009 Policy on Government Security incorporates a requirement for departments and agencies to implement a quality assurance program that includes reviewing contract files to verify that they meet security in contracting requirements. Treasury Board's Directive on Departmental Security Management identifies this requirement as part of the departmental security officer's responsibilities. We found that the entities audited have implemented this requirement. This is discussed in more detail in the following sections, beginning in the section entitled "Other progress since our 2007 audit" and continuing in the individual sections for each entity.

2.36 We also found that the Treasury Board of Canada Secretariat monitors compliance with the Policy in a variety of ways. For example, it conducted a survey that required feedback on key issues and challenges facing departments and on the effectiveness of lead security agencies in supporting the security community. In addition, it obtained feedback on the usefulness of existing Secretariat guidance and tools related to the development of the departmental security plan through a questionnaire. Both identified several key focus areas for the Secretariat, including the lack of up-to-date standards and guidance and lack of funding for activities regarding security in contracting.

2.37 In the 2011–12 fiscal year, the Secretariat also conducted a review of departments' internal audit findings related to security. In addition, the Secretariat, as part of its review of departments' submissions under the Management Accountability Framework (a tool to evaluate departmental performance against the Secretariat's expectations for good management), assessed departmental security management practices. These practices included governance, planning, training, awareness, and incident management. It also assessed compliance with two security standards—the Management of Information Technology Security and Business Continuity Planning—as outlined in the departments' Management Accountability Framework submissions. However, these management practices and standards do not specifically address security in contracting. The Secretariat has noted that it expects to expand the monitoring of compliance in future years.

2.38 In summary, the Treasury Board of Canada Secretariat has improved its oversight of security in contracting. Exhibit 2.5 shows our assessment of progress in addressing our 2007 recommendations.

Exhibit 2.5 Satisfactory progress in addressing our recommendations on oversight of security in contracting

Recommendation from 2007 audit	Progress
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.	**Satisfactory**
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.	**Satisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Industrial Security Program

2.39 We examined actions taken by Public Works and Government Services Canada (PWGSC) on our 2007 recommendations to improve certain aspects of the Industrial Security Program and its process, policies, and procedures for security in contracting. Our assessment of PWGSC's progress in meeting our recommendations can be found in Exhibit 2.6 on page 65.

Departmental processes related to security have been implemented

2.40 In 2007, we noted that PWGSC relied on project managers within its client departments to identify any security requirements related to their contracts and to forward this information to the Industrial Security Program for processing. At that time, there was no means of identifying all contracts awarded by PWGSC that contained security requirements.

2.41 In our current audit, we found that when PWGSC is the contracting authority, a client department is now required to formally identify whether there is a security requirement or not on the Requisition for Goods and Services. If there is a security requirement, the client completes the Security Requirements Check List.

2.42 We found that PWGSC complies with the Policy on Government Security, including the requirement to have a departmental security plan. Since 2007, PWGSC has implemented standard operating procedures for security in contracting and has reduced the number of procedures to focus on key areas. In addition, it has implemented a quality assurance program to ensure consistency in the processes for security in contracting. PWGSC has also provided training to its employees and those of other government departments on topics such as security in contracting and the use of the Security Requirements Check List.

2.43 We conducted a review of the Industrial Security Program's files for contractors who had been cleared at the classified level, with document safeguarding capability, and who had been awarded a contract during the 2011–12 fiscal year. We reviewed 10 contracting files with security requirements and 20 files identified as having no security requirements.

2.44 Our review included some files that Internal Audit had also reviewed. In all files reviewed, security requirements were correctly identified in the contract. In contracts where there was a security requirement, we found that the Check List had been completed, and that security clearances had been granted to contractors and their firms before they were awarded contracts.

The Industrial Security Program's charging methodology needs improvement

2.45 In 2007, we found that PWGSC had not allocated sufficient funding to the Industrial Security Program. The Department's annual funding covered only about 70 percent of the full-time equivalent positions, with funding for the remaining 30 percent coming from a departmental reserve on a year-to-year basis. We recommended that PWGSC ensure that the Industrial Security Program has adequate resources to meet the program's objectives.

2.46 In our current audit, we found that the level of funding provided for PWGSC's Industrial Security Program has increased since 2007. PWGSC had received authority from Treasury Board to recover costs from client departments for the Industrial Security Program's services related to security in contracting. A cost recovery initiative was approved for the 2011–12 fiscal year and subsequent fiscal years. Costs are recovered from entities based on the entity's proportion of all contracts with security provisions averaged over a two-year period,

adjusted for contract complexity. The costs to be recovered in the 2011–12 fiscal year were calculated at $18.2 million; of 53 departments, 47 signed memoranda of understanding with PWGSC and paid their share of the costs, representing 97 percent of the total recovery. This addresses the recommendation from the 2007 audit.

2.47 However, some entities have expressed concerns with the cost recovery initiative. They have urged PWGSC to find another solution, because they question whether the services they are receiving are commensurate with the fees paid. PWGSC has not been able to demonstrate whether the charging methodology is appropriate for the services being provided. We were advised that PWGSC is reviewing options for additional improvements to the Industrial Security Program's charging methodology.

2.48 **Recommendation.** Public Works and Government Services Canada should improve its charging methodology to meet the needs of client departments and agencies.

The Department's response. Public Works and Government Services Canada accepts the recommendation and will continue to work with client departments and agencies to improve its charging methodology.

The Industrial Security Program needs to better manage its pending personnel clearances

2.49 As part of our audit work, we examined whether the Industrial Security Program had personnel clearances that had not been completed and remained in process at the end of the audit. We found that of the approximately 27,000 secret clearance requests received during the 2011–12 fiscal year, approximately 1,400 requests had been in process for almost eight months, well beyond Public Works and Government Services Canada's service standard of 75 days. Further, approximately 1,100 requests remained pending from previous years, some of which were pending for more than five years. While delays are often due to waiting for additional information from the applicant or other government departments, these delays may impede the government from completing its projects in a timely manner. At the time of the audit, PWGSC could not provide us with evidence that demonstrated whether the pending clearances were being managed or whether any of these requests had been subsequently cancelled.

2.50 **Recommendation.** Public Works and Government Services Canada should improve its processes to manage pending personnel screening requests and follow up on all valid clearance requests, eliminating those that have been cancelled.

The Department's response. Public Works and Government Services Canada accepts the recommendation and has already undertaken an administrative review of the pending clearance requests, which has resulted in the elimination of requests that are no longer valid. The administrative review will be completed by 31 March 2013. A new standard operating procedure for the management of pending clearances will be developed and fully implemented by 30 April 2013.

Progress has been made in the Industrial Security Program's information technology security

2.51 In 2007, we found that the Department was unable to provide evidence that the Industrial Security Program's information systems had been certified as meeting the Treasury Board's Standard on Management of Information Technology Security. We recommended that Public Works and Government Services Canada (PWGSC) ensure that its secure information technology environment for the operations of the Industrial Security Program be certified.

2.52 We also found that PWGSC did not have a comprehensive disaster recovery plan for the information technology systems of the Industrial Security Program. We recommended that it review its departmental business continuity plan to determine whether it had made adequate provisions for the Program.

2.53 In this audit, we found that the Industrial Security Program's information systems have been certified on an interim basis since 2007, continuing until mid-2013. The Industrial Security Program's systems will not achieve full certification due, in part, to the age of the business systems applications. However, PWGSC believes that this is not a significant risk. We have been advised that PWGSC is exploring options to replace its aging business systems.

2.54 In our current audit, we also found that PWGSC updated its business continuity plan in 2012 and included provisions for the Industrial Security Program's information systems.

Exhibit 2.6 Satisfactory progress in addressing our recommendations on the Industrial Security Program

Recommendations from 2007 audit	Progress
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.	**Satisfactory**
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.	**Satisfactory**
1.59 Public Works and Government Services Canada should ensure that the Industrial Security Program has adequate resources to meet its program objectives.	**Satisfactory**
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.	**Satisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Other progress since our 2007 audit

2.55 We examined actions taken by National Defence, Defence Construction Canada, and the RCMP on our 2007 recommendations to improve their policies and procedures for security in contracting.

Progress has been made on recommendations to the RCMP and Defence Construction Canada, while progress at National Defence has been varied

2.56 In 2007, we noted that National Defence's policies on security in contracting were outdated and incomplete, and that the RCMP had limited policies and procedures in place that were not followed consistently. We recommended that each entity ensure that its policies and procedures were up to date and accurately reflected the entity's roles and responsibilities under the Government Security Policy. We also recommended that their policies and procedures be well communicated to staff and followed consistently.

2.57 We also reported that in 99 percent of contracts managed on its behalf by Defence Construction Canada, National Defence had not provided a Security Requirements Check List. As a result, neither entity had any assurance that the contractors had been cleared to the appropriate level. We recommended that the two entities establish an integrated framework for managing industrial security on defence projects.

2.58 In our current audit, we examined whether National Defence, the RCMP, and Defence Construction Canada had made changes in their policies and procedures for security in contracting to respond to issues we identified in 2007. We found mixed results.

2.59 In 2008, National Defence established an integrated framework with Defence Construction Canada for managing industrial security on defence projects. We found that the framework identifies the roles and responsibilities of both parties and requires either a Security Requirements Check List or written attestation that no security requirement exists. However, the framework was not reviewed within two years, as required.

2.60 We found that while Defence Construction Canada complies with the Policy on Government Security and has communicated this to its staff, National Defence complies with only portions of the Policy. We found that National Defence has policies in place that cover security in contracting, but they are inconsistent and dispersed among several manuals and policy documents that are not linked. For example, the manuals and policy documents have different criteria identifying what does and does not constitute a security requirement. This is further complicated by differences we found in how various departmental units apply the documented procedures.

2.61 We found that the RCMP now has policies in place for the significant processes related to security in contracting as communicated to staff, and is mostly compliant with the Policy on Government Security. It requires the use of either the Check List to identify security requirements or another form indicating that no security requirements exist, and includes guidance with clear examples.

2.62 Both National Defence and the RCMP have implemented a quality assurance program. However, we found that National Defence has yet to develop a departmental security plan. The RCMP's plan has been drafted but has not yet been approved.

2.63 In summary, while the RCMP and Defence Construction Canada have made satisfactory progress, National Defence has not, as noted in Exhibit 2.7.

Exhibit 2.7 Progress in addressing our recommendations related to other government entities

Recommendations from 2007 audit	Progress
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.	**National Defence—Unsatisfactory** **RCMP—Satisfactory**
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.	**Defence Construction Canada—Satisfactory** **National Defence—Satisfactory**

Satisfactory—Progress is satisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

Unsatisfactory—Progress is unsatisfactory, given the significance and complexity of the issue, and the time that has elapsed since the recommendation was made.

2.64 Recommendation. National Defence should integrate its policies and procedures and ensure they are aligned with the Policy on Government Security. It should also develop its departmental security plan.

The Department's response. Agreed. All of National Defence's security policies are currently being updated, with expected completion by the end of the 2013–14 fiscal year. National Defence has put in place a Security Reform Team to establish a defence security model that uses the Treasury Board of Canada Secretariat's mandated security objectives and implements security best practices throughout the Canadian Forces and National Defence in order to enhance its operational effectiveness. One of the end results of this initiative will be the development of a current and relevant departmental security plan for National Defence. Target date for the departmental security plan is the end of the 2014–15 fiscal year.

Current issues in security practices

2.65 In addition to the entities included in our 2007 audit, we expanded the scope of this audit to look at current policies, procedures, and overall processes for security in contracting at the Canadian Security Intelligence Service and Communications Security Establishment Canada. We included these two entities because of their responsibilities as lead agencies, their focus on security, and the nature of the information they need to do their work.

Entities' adherence to the Policy on Government Security has been mixed

2.66 We examined how well policies and procedures are followed in the five entities and to what extent they align with the Policy on Government Security. To determine this, we reviewed a sample of each entity's contracting files, with and without security requirements, and related personnel security files of contractors cleared at the classified level who had been awarded a contract during the 2011–12 fiscal year.

2.67 We found mixed results in our examination of contracts with identified security requirements and those with none. The Canadian Security Intelligence Service consistently identified when security requirements were to be included in contracts, while National Defence and RCMP continue to be challenged in identifying security requirements. Communications Security Establishment Canada included security requirements for firms in each of the contracts reviewed, but these requirements were not met in all of these contracts at the time the contract was awarded.

2.68 Exhibit 2.8 shows the number of files we reviewed for each entity. The last column indicates the number of contracts with incomplete or absent security documentation or improper allocation of controls. The main issues we identified included

- the lack of signatures,
- no evidence that firms were cleared, and
- clearances that were not completed prior to contract award.

Exhibit 2.8 Several reviewed contracts had incomplete or absent security documentation, or improper application of controls

Entity	Number of contracts with security requirements	Number of contracts without a security requirement	Total contracts reviewed	Number of contracts with incomplete or absent security documentation or improper application of controls
Canadian Security Intelligence Service	44	42	86	0
Communications Security Establishment Canada	18	42	60	14
Defence Construction Canada	36	25	61	28
National Defence	25	23	48	32
RCMP	14	28	42	11

2.69 We also observed files with no identified security requirement when, based on departmental policy and procedures, they should have had one. The majority of files did not present significant security risks, but they demonstrated a lack of proper application of controls. These issues are discussed in more detail in the individual sections for each entity that follow.

The Canadian Security Intelligence Service complies with the Policy

2.70 We found that the Canadian Security Intelligence Service's (CSIS's) policy and procedures are consistent with the Policy on Government Security. Its departmental security plan has been approved, a quality assurance program has been implemented, and processes are in place to provide assurance that contracts are issued only after personnel security clearances have been granted. Our file review found that security clearances were granted before contracts were awarded, and all contractors were cleared appropriately. In every case where no security requirement existed, the contract was managed appropriately.

2.71 CSIS uses a variety of good practices, including deactivating contractors' security clearances when the contract is completed, and it has several internal performance measures geared toward continuous improvements. As a lead security agency, CSIS has also conducted a survey of its clients on requirements for security screenings based on the services provided and has developed an action plan to address several of the key issues identified.

2.72 CSIS does not use the Security Requirements Check List for contracts within its delegated contracting authority; however, it does use the Check List for contracts outside its delegated authority. In consultation with CSIS's departmental security officer, the project manager must identify any security requirements of a contract. According to CSIS management, it has assurance that contracts are awarded only after security clearances have been granted, but it has also recognized that it can improve controls so that all security requirements in contracts have been appropriately assessed and identified. CSIS is currently working on revising its policy and processes to include the use of such a control.

2.73 CSIS reviews private sector firms to provide assurance that no links exist to organizations of concern, as identified by CSIS. However, CSIS does not conduct a complete security screening of the firm. We encourage CSIS to strengthen its controls for clearances of firms to the appropriate extent to ensure that firms that will have

access to protected and classified information and assets are cleared before a contract is awarded.

Communications Security Establishment Canada complies with the Policy

2.74 We found that Communications Security Establishment Canada (CSEC) is consistent with the Policy on Government Security. It uses the Security Requirements Check List to identify security requirements, has implemented a quality assurance program, and has approved its departmental security plan. CSEC's requirement for clearances of firms went beyond the requirements in the Policy on Government Security. CSEC recently approved a policy on key activities related to security in contracting, which will help ensure that the process is carried out uniformly.

2.75 From our interviews and file review, we found that individual contractors had been granted security clearances at the appropriate levels before contracts began. We also reviewed the security in place for CSEC's Long-Term Accommodation Project (Exhibit 2.9).

Exhibit 2.9 Security has been well considered in Communications Security Establishment Canada's Long-Term Accommodation Project

We looked at a major project currently under construction to replace Communications Security Establishment Canada's (CSEC's) facilities and consolidate its workforce. For this project, Defence Construction Canada is the contracting authority. We found that security had been well considered and integrated into project planning and delivery. The projected cost of this Long-Term Accommodation Project is $880 million, with completion planned for 2014. Given the highly classified nature of CSEC's business, the design and construction of the new facility took security considerations into account with a view to enhancing monitoring and eliminating the need for costly retrofits.

CSEC conducted the personnel screening and provided the results to the Industrial Security Program for inclusion in the Program's database. It also signed a service-level agreement with Public Works and Government Services Canada (PWGSC) to conduct the facility security clearances. At the same time, CSEC conducted contractor clearances and requested clearances of firms from PWGSC. Until a firm was cleared, there was no access to the site and no work was permitted. Together, these procedures ensured that both firms and contractors would be appropriately cleared. CSEC cleared or provided site access clearance to more than 6,000 individuals, from truck drivers to consultants—no individual was allowed on site without first being cleared.

CSEC also took additional precautions, such as the following:

- It ensured that firms providing construction materials and equipment were granted access only to specific sections of the work site as necessary.
- It restricted access to drawings of the building and the building site.
- It established verification procedures to ensure that there were no unobserved breaches of security.

While the cost of these additional procedures was considerable, in CSEC's opinion they provided the assurance that its Chief needed—that risks had been mitigated appropriately.

2.76 We also reviewed 18 CSEC contracts unrelated to the Long-Term Accommodation Project. We found that for 14 contracts entered into with six firms, the firm had not been cleared when the contract was awarded. While CSEC had a security clause in these contracts for firms to be cleared, clearance was obtained only after the work had started.

2.77 **Recommendation.** Communications Security Establishment Canada should ensure that all contract security requirements related to firm clearances are met prior to awarding the contract.

The Agency's response. Agreed. Communications Security Establishment Canada acknowledges the audit's finding that CSEC met all requirements of government policy. With respect to the additional requirements that CSEC put in place over and above the policy, CSEC accepts the findings of the Auditor General, although additional risk mitigation measures were put in place. CSEC's guidelines have been amended accordingly.

National Defence falls short of the Policy's requirements

2.78 For National Defence projects, where either National Defence or Defence Construction Canada (DCC) is the contracting authority and National Defence is the project authority, National Defence has developed procedures to address key activities related to security in contracting. For those projects where DCC is the contracting authority, National Defence is responsible for defining the security requirements that DCC will implement during construction.

2.79 We examined National Defence and DCC files to determine whether all firms were cleared before being awarded contracts. Both National Defence and DCC use the Industrial Security Program to clear firms. Our audit work on the Program confirmed that in the files we reviewed, firms had been appropriately cleared by the Program.

2.80 We found that for projects in which DCC is the contracting authority, the two entities have implemented a joint quality assurance program for compliance with National Defence procedures. We also found that while DCC complied with the Policy on Government Security, National Defence was partially compliant, as indicated by our observations in the section of this chapter outlining progress on our 2007 recommendations. (See paragraphs 2.56 to 2.64.)

2.81 We found a lack of consistency in National Defence's procedures for contracts in which a security requirement has been identified, such as whether to use the Security Requirements Check List or not. Several files we reviewed also had incomplete or missing

documentation. Examples included the absence of key signatures from the Security Requirements Check List, or the lack of evidence that the firm had been cleared.

2.82 National Defence's criteria for identifying the absence of security requirements were also inconsistent. Certification that there were no security requirements was missing in some cases. In other cases, where access to a sensitive site was required or heavy machinery and ammunition was to be moved, the contracts failed to identify a security requirement.

2.83 In 25 DCC files that we reviewed there was a security requirement, but no Check List was used. In those files, we found that DCC accepted the mitigation of security through other measures identified by National Defence. These included 14 cases of escorting uncleared contractors while on the project site and 3 cases of removing all classified material while the work was being done. This practice fails to address identified security requirements and may result in inadequate security for projects.

2.84 We also found that National Defence's departmental security officer is not always consulted on the need for a security requirement by a branch of National Defence before contracts are awarded.

2.85 As part of the current audit, we also followed up on the NORAD project, as discussed in our 2007 audit (Exhibit 2.10).

Exhibit 2.10 Additional costs were required for the security of a NORAD 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. Given the intended purpose of the building, and as required by the Government Security Policy (2002), a Security Requirements Check List should have been completed to identify security requirements. In 2007, we found 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.

The facility is now operational and handles classified information. To rectify the original security concerns, a portion of the building was demolished and a smaller secure area was rebuilt. There were also additional costs for monitoring whether the new structure would be electronically secure. Costs to mitigate the original security concerns are about $2.3 million to date.

This case demonstrates that unclear direction in identifying security requirements or lapses in security during contract delivery can result in additional expense. For example, a building may not be fully used for its intended purpose, or may need a retrofit. In addition, credibility with other countries' security units could be affected. Ongoing monitoring may also be needed to ensure security has not been compromised.

2.86 A more recent project included plans for a secure communications area within a helicopter support facility at CFB Petawawa. The procurement strategy called for the design and construction of a secure area to be excluded from the original contract, with the intention of including it in subsequent contracts. However, security measures were deemed necessary, and provisions were made for security personnel, fences, site access controls, and passes for site workers. It is unclear the extent to which these resources were to address normal construction needs or the eventual use of the building. According to the departmental policy for construction projects, there was no need to complete a Security Requirements Check List, although security precautions had been put in place.

2.87 As contracting authority for the CFB Petawawa project, Defence Construction Canada was responsible for the implementation of security measures as identified by National Defence. A site inspection by DCC early in 2012 identified that the security measures were in fact not in place. After discussion, National Defence decided they were no longer required. At the time of the audit, National Defence had not completed the project.

2.88 National Defence procedures recognize that its process for identifying security requirements for construction projects may not provide clear direction for facilities that raise security concerns, but the Department has not documented how this assessment is to be made. This demonstrates the need to consider the eventual use of a facility when defining security requirements.

2.89 **Recommendation.** National Defence should ensure that construction projects consider the eventual use of the facility when defining the security requirements. National Defence should involve Defence Construction Canada earlier in the assessment of planned security requirements to ensure that they will be implemented appropriately.

The Department's response. Agreed. National Defence will update its policies to clearly reflect that the eventual use of a facility will be considered when defining the security requirements of all construction phases. National Defence will assess whether sufficient direction is being provided with respect to accurately and clearly defining and communicating our industrial security needs to Defence Construction Canada in a timely manner to ensure appropriate implementation. This is expected to be completed by the end of the 2013–14 fiscal year.

2.90 **Recommendation.** Defence Construction Canada should be involved earlier in the assessment of planned security requirements to ensure that these requirements are consistent with the eventual use of the facility and can be implemented appropriately.

The Corporation's response. Agreed. Defence Construction Canada will continue to act in a proactive manner when dealing with security in contracting. Defence Construction Canada will work closely with National Defence to ensure that security requirements are clearly defined and subsequently implemented appropriately.

The Royal Canadian Mounted Police is mostly compliant with the Policy

2.91 Overall, we found that the RCMP's departmental policies and processes are mostly compliant with the Policy on Government Security, as indicated by our observations in the section of this chapter outlining progress on our 2007 recommendations. (See paragraphs 2.61 to 2.63.) The RCMP uses good practices, including the deactivation of contractors' security clearances at the end of the contract and real-time fingerprinting. It also uses the Check List to identify security requirements, or a waiver to indicate that none exist.

2.92 We found that in all cases we reviewed with an identified security requirement, the RCMP did not award any contracts before personnel security clearances had been granted, and all of the contractors were cleared appropriately. However, in 11 of the 42 files we reviewed, we found that the Security Requirements Check List was incomplete or missing. Examples included the absence of key signatures and files that should have had identified security requirements, based on departmental policy and procedures, but did not. Although the RCMP uses the Industrial Security Program for contracts above its authority, we found that the RCMP does not undertake security clearances of private sector firms for contracts within its delegated contracting authority.

2.93 **Recommendation.** The RCMP should assess security risks for firms that will have access to its protected and classified information and assets and complete any additional security checks or clearances to respond to these risks before a contract is awarded.

The RCMP's response. Agreed. The RCMP will review its departmental security risks for contracting, which involves private sector firms having access to its protected and classified government information and assets, and carry out additional security screening of individuals as required to mitigate those risks before such contracts are awarded.

Conclusion

2.94 Overall, progress has been unsatisfactory in implementing the commitments made in response to our 2007 recommendations regarding security in contracting. Although the government has made a number of improvements, including providing clearer requirements for departments to monitor and report on their security programs, in our opinion, significant weaknesses remain. Successful projects integrate security into all phases of the development and management of contracts. However, risks increase when entities modify their security requirements to meet cost or scheduling constraints.

2.95 The Treasury Board Policy on Government Security has been revised. It clarifies roles and responsibilities for Public Works and Government Services Canada (PWGSC), departments, and lead security agencies. Further, it requires deputy heads to report on the implementation of the Policy. However, the Policy on Government Security falls short of addressing our 2007 recommendations. The Policy, as well as the Security and Contracting Management Standard, does not explicitly address the clearance of private sector firms with access to protected and classified information.

2.96 PWGSC has made satisfactory progress since our 2007 audit. It complies with the Policy and requires the Security Requirements Check List to be completed before contracts are awarded and it has defined and implemented standard operating procedures. Additional funding has been provided through a cost recovery model that PWGSC uses to charge departments for the services it offers, including services related to security in contracting. However, its charging methodology does not demonstrate that it is meeting clients' needs. PWGSC also needs to improve its management of pending personnel screening requests.

2.97 In most cases, lead security agencies' policies and procedures are designed to provide assurance beyond the level required by the Policy on Government Security and other federal departments. The entities we audited had policies and processes that were aligned with the Policy on Government Security. However, a departmental security plan has not been implemented in National Defence, and the RCMP's has yet to be approved. As well, there were inconsistent approaches among the entities, including the processes they used to clear private sector firms. The RCMP and Defence Construction Canada have made satisfactory progress since our 2007 audit and, along with the Canadian Security

Intelligence Service and Communications Security Establishment Canada, comply with the Policy on Government Security. National Defence's progress is unsatisfactory.

2.98 In our examination of contracts with identified security requirements and those with none, we found mixed results. Canadian Security Intelligence Service consistently identified when security requirements were to be included in contracts, while National Defence and RCMP continue to be challenged in the identification of security requirements for the contracts they tender. Communications Security Establishment Canada included security requirements for firms in contracts, which were not met at the time the contract was awarded.

About the Audit

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

Objectives

The overall objective of the audit was to determine whether the Treasury Board of Canada Secretariat, Public Works and Government Services Canada (PWGSC), and selected departments and agencies have made satisfactory progress in addressing issues reported in the October 2007 Report, Chapter 1, Safeguarding Government Information and Assets in Contracting.

Scope and approach

Our work focused on the security screening process for assessing the loyalty (including reliability) of external contractors and their firms; the granting of access to classified information and assets; and other related contract security activities. We examined the key clauses in contracts to ensure security provisions were addressed, but we did not conduct reviews of site security management.

Areas that we determined were outside the audit's scope (which were also not part of the 2007 audit) include

- PWGSC's International Industrial Security Directorate. This Directorate manages industrial security arrangements with foreign countries.
- PWGSC's Controlled Goods Directorate. This Directorate is responsible for the prevention and detection of the unlawful examination, possession, or transfer of controlled goods in Canada through its mandatory registration and regulation of Registered Persons (registered businesses and individuals).

The following entities were included in the audit: Treasury Board of Canada Secretariat, Public Works and Government Services Canada, Royal Canadian Mounted Police, National Defence, Defence Construction Canada, Communications Security Establishment Canada (CSEC), and Canadian Security Intelligence Service (CSIS). CSIS and CSEC were included due to their responsibilities as lead agencies, their focus on security, and the nature of the information they need to do their work.

PWGSC's internal audit function conducted a follow-up audit of the Industrial Security Program. Our work determined that the Office of the Auditor General of Canada was able to rely on the work of the internal audit function within PWGSC.

Criteria

Criteria	Sources
To determine whether the Policy on Government Security has addressed weaknesses previously identified, including the roles and responsibilities of selected lead security agencies, and to determine whether the Treasury Board of Canada Secretariat has reasonable assurance that departments have complied with the Policy on Government Security, we used the following criteria:	
Treasury Board of Canada Secretariat, through the Policy on Government Security, has addressed weaknesses previously identified.	• Foundation Framework for Treasury Board Policies, Treasury Board, 2008 • Policy on Government Security, including associated directives and standards, Treasury Board, 2009
Treasury Board of Canada Secretariat has monitored compliance with the Policy on Government Security.	
To determine whether Public Works and Government Services Canada's (PWGSC's) Industrial Security Program is aligned with the Policy on Government Security and whether PWGSC has complied with its own program requirements, and to determine whether Public Works and Government Services Canada has assigned the resources and capacity necessary to administer the Industrial Security Program, we used the following criteria:	
PWGSC has policies in place for industrial security that are consistent with the Policy on Government Security.	• Foundation Framework for Treasury Board Policies, Treasury Board, 2008 • Policy on Government Security, including associated directives and standards, Treasury Board, 2009 • Contracting Policy, Treasury Board, 2008 • PWGSC's Departmental Policy 54: Industrial Security Program, Public Works and Government Services Canada, 2007 • Expenditure Management System of the Government of Canada, Treasury Board, 1995
PWGSC's procedures for the Industrial Security Program ensure completeness and accuracy of information required to fulfill its mandate.	
PWGSC has measures in place to determine if it has adequate resources and capacity necessary to administer the Industrial Security Program.	
To determine whether selected lead security agencies' departmental security policy and process requirements are aligned with the Policy on Government Security, and to determine whether selected lead security agencies comply with their own departmental security policy and process requirements, we used the following criteria:	
Selected lead security agencies and Defence Construction Canada have policies in place for industrial security that are consistent with the Policy on Government Security.	• Foundation Framework for Treasury Board Policies, Treasury Board, 2008 • Policy on Government Security, including associated directives and standards, Treasury Board, 2009 • Departmental procedures and standards for industrial security
Departmental procedures are designed to provide assurance that the requirements of the Policy on Government Security and departmental policies have been met.	
Departments have implemented procedures for industrial security to ensure access to classified government information has only been given to individuals and firms with appropriate clearance.	

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

Period covered by the audit

The period under examination was the 2011–12 fiscal year for screening levels granted and contracts issued. We extended this period to cover actions taken in earlier years to respond to issues reported in our 2007 audit, including the development and implementation of the Policy on Government Security. Audit work for this chapter was completed on 3 December 2012.

Audit team

Assistant Auditor General: Nancy Cheng
Principal: Gordon Stock
Lead Director: Marianne Avarello
IT Director: Bernard Battistin

John McGrath
Toby Climie

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 2. 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
Policy on Government Security	
2.32 The Treasury Board of Canada Secretariat, in consultation with Public Works and Government Services Canada and the lead security agencies, should address the security risks related to the absence of a specific requirement to security screen private sector firms and ensure consistency among the Policy on Government Security and associated directives, standards, and guidance. **(2.26–2.31)**	Agreed. Deputy heads are responsible for the management of security within their organizations, and the Treasury Board of Canada's current policy instruments already require that all individuals (which includes contractors) with access to government information and assets be security screened. With this understanding, the Treasury Board of Canada Secretariat, in consultation with Public Works and Government Services Canada and the lead security agencies, will address the security risks, as identified in this report, which may arise as the result of the absence of a specific requirement to security screen private sector firms. The Treasury Board of Canada Secretariat will also ensure consistency across the Policy on Government Security, including its related directives, standards, and guidelines. This will be accomplished as part of the current security policy suite renewal activities and the update to the Security and Contracting Management Standard, which is planned for summer 2013.
Industrial Security Program	
2.48 Public Works and Government Services Canada should improve its charging methodology to meet the needs of client departments and agencies. **(2.45–2.47)**	Public Works and Government Services Canada accepts the recommendation and will continue to work with client departments and agencies to improve its charging methodology.
2.50 Public Works and Government Services Canada should improve its processes to manage pending personnel screening requests and follow up on all valid clearance requests, eliminating those that have been cancelled. **(2.49)**	Public Works and Government Services Canada accepts the recommendation and has already undertaken an administrative review of the pending clearance requests, which has resulted in the elimination of requests that are no longer valid. The administrative review will be completed by 31 March 2013. A new standard operating procedure for the management of pending clearances will be developed and fully implemented by 30 April 2013.

Recommendation	Response
Other progress since our 2007 audit	
2.64 National Defence should integrate its policies and procedures and ensure they are aligned with the Policy on Government Security. It should also develop its departmental security plan. **(2.55–2.63)**	Agreed. All of National Defence's security policies are currently being updated, with expected completion by the end of the 2013–14 fiscal year. National Defence has put in place a Security Reform Team to establish a defence security model that uses the Treasury Board of Canada Secretariat's mandated security objectives and implements security best practices throughout the Canadian Forces and National Defence in order to enhance its operational effectiveness. One of the end results of this initiative will be the development of a current and relevant departmental security plan for National Defence. Target date for the departmental security plan is the end of the 2014–15 fiscal year.
Current issues in security practices	
2.77 Communications Security Establishment Canada should ensure that all contract security requirements related to firm clearances are met prior to awarding the contract. **(2.74–2.76)**	Agreed. Communications Security Establishment Canada acknowledges the audit's finding that CSEC met all requirements of government policy. With respect to the additional requirements that CSEC put in place over and above the policy, CSEC accepts the findings of the Auditor General, although additional risk mitigation measures were put in place. CSEC's guidelines have been amended accordingly.
2.89 National Defence should ensure that construction projects consider the eventual use of the facility when defining the security requirements. National Defence should involve Defence Construction Canada earlier in the assessment of planned security requirements to ensure that they will be implemented appropriately. **(2.78–2.88)**	Agreed. National Defence will update its policies to clearly reflect that the eventual use of a facility will be considered when defining the security requirements of all construction phases. National Defence will assess whether sufficient direction is being provided with respect to accurately and clearly defining and communicating our industrial security needs to Defence Construction Canada in a timely manner to ensure appropriate implementation. This is expected to be completed by the end of the 2013–14 fiscal year.
2.90 Defence Construction Canada should be involved earlier in the assessment of planned security requirements to ensure that these requirements are consistent with the eventual use of the facility and can be implemented appropriately. **(2.78–2.88)**	Agreed. Defence Construction Canada will continue to act in a proactive manner when dealing with security in contracting. Defence Construction Canada will work closely with National Defence to ensure that security requirements are clearly defined and subsequently implemented appropriately.

Recommendation	Response
2.93 The RCMP should assess security risks for firms that will have access to its protected and classified information and assets and complete any additional security checks or clearances to respond to these risks before a contract is awarded. **(2.91–2.92)**	Agreed. The RCMP will review its departmental security risks for contracting, which involves private sector firms having access to its protected and classified government information and assets, and carry out additional security screening of individuals as required to mitigate those risks before such contracts are awarded.