National Defence / Défense nationale

Chief Review Services / Chef - Service d'examen

CRS / CS Ex

Audit of Industrial Security

May 2011

7050-51 (CRS)



Canada

Table of Contents

Acronyms and Abbreviations

CA	Contracting Authority
CF	Canadian Forces
CFPM	Canadian Forces Provost Marshal
CISD	Canadian Industrial Security Directorate
CGD	Controlled Goods Directorate
CRS	Chief Review Services
DCC	Defence Construction Canada
DND	Department of National Defence
DPM Secur	Deputy Provost Marshal Security
DSM	Defence Security Manual
DSO	Departmental Security Officer
DSP	Departmental Security Program
ISP	Industrial Security Program
PA	Project Authority
PGS	Policy on Government Security
PWGSC	Public Works and Government Services Canada
SRCL	Security Requirements Checklist
TA	Technical Authority
TBS	Treasury Board Secretariat
VCDS	Vice Chief of the Defence Staff
VCR	Visit Clearance Request

Results in Brief

Overall Assessment

[redacted]

The Government's Industrial Security Program (ISP) was established to ensure that contract-related security requirements are identified, addressed, formally documented, implemented and monitored in all phases of procurement and throughout the term of the contract. This is meant to ensure that departmental information, assets, systems and/or facilities entrusted to industry are afforded an appropriate level of protection.

Whether a contract is within or outside a department's delegated contracting authority, the department is responsible for identifying sensitive information and assets requiring additional safeguards and ensuring that these safeguards continue to be in place for the term of the contract. Individuals granting access to these sensitive assets and/or information must confirm that the personnel to whom they are providing this access are cleared to the appropriate level and have the capability to properly safeguard the information/assets that have been entrusted to them.

Finding and Recommendation

Departmental ISP. [redacted]

It is recommended that the Vice Chief of the Defence Staff (VCDS), in collaboration with the appropriate Level 1 organizations, review and revise the objectives and practices of the departmental ISP in order to ensure they address the PGS, controlled goods commitments, as well as any unique requirements of the DND/CF. This includes ensuring the following:

- Industrial security policies are comprehensive and complete, covering all phases of the procurement and contracting process where security must be considered and managed. The policies should be well communicated and clearly define roles, responsibilities and accountabilities related to all phases of the industrial security process, beginning with the identification of a requirement through to contract closure;
- There are risk management processes in place to monitor adherence to identified security requirements or where no security requirement exists, there are mechanisms in place to ensure the determination of the "non-requirement" is accurate and supported; and

- A robust training and awareness plan is developed to ensure that the appropriate personnel are aware of all industrial security requirements, associated responsibilities and sources of expertise within the Department.

Note: Please refer to Annex A—Management Action Plan for the management response to the Chief Review Services (CRS) recommendation.

Introduction

Background

The PGS states that "Deputy Heads are responsible to ensure that all individuals who will have access to government information and assets are security screened at the appropriate level before the commencement of their duties."[1] This requirement is further supported by the Treasury Board Secretariat (TBS) Directive on Departmental Security Management which states that "the Departmental Security Officer (DSO) is responsible to ensure that security requirements are identified, addressed, formally documented, implemented and monitored in all phases of procurement and through the term of the contract. The DSO must also ensure that information, assets, systems and facilities entrusted to industry meet the industrial security requirements and are afforded an appropriate level of protection through their life cycle."[2]

Ultimately departments are responsible for protecting sensitive information and assets under their control. Whether a contract is within or outside a department's delegated contracting authority, the department is responsible for identifying sensitive information and assets warranting additional safeguards and ensuring that these safeguards continue to be in place for the term of the contract.

Industrial Security Program

Public Works and Government Services Canada (PWGSC) is responsible for providing leadership and for coordination of activities to help ensure the application of security safeguards through all phases of the contracting process within the scope of the industrial security program.[3] The Canadian Industrial Security Directorate (CISD), within PWGSC, is responsible for the ISP for the Government of Canada. The security requirements checklist (SRCL) is used by CISD and client departments to define security requirements applicable to a particular contract. According to the PGS, some of PWGSC/CISD's key activities include the following:

- Performing security screening of private sector individuals and organizations that have access to departmental protected and classified information and assets;
- Ensuring compliance in those security contracts that afford industry access to government information and assets; and
- Processing requests for visits when security cleared individuals must visit government or commercial organizations in Canada or abroad.

[1] TBS Policy on Government Security (2009).
[2] TBS Directive on Departmental Security Management (2009).
[3] Public Works and Government Services Canada, Industrial Security Manual (2009).

Within DND, industrial security is the responsibility of the Deputy Provost Marshal Security (DPM Secur),[4] specifically DPM Secur 3 corporate security. This responsibility includes the following:

- Providing advice and guidance on the use of SRCLs;
- Serving as the departmental signing authority for SRCLs; and
- Coordinating the visit clearance request (VCR) program.

Any organization entering into a contract must consider security requirements related to the specific contract. An SRCL must be completed for all requisitions or requisition amendments, standing offers or supply arrangements that contain a requirement for physical security, information security, information technology security, or personnel security screening. When there are no contract-related security requirements, an attestation must be completed by the technical authority or someone in the organization with appropriate knowledge, certifying that no requirement exists.

The contracting authority (CA) is responsible to ensure that the appropriate security clauses are included in the solicitation documents and that the contractor's security clearance is verified through CISD prior to contract award.

Objective

The objective of the audit was to assess whether there are adequate processes in place to ensure contract-related security requirements are identified, validated, implemented and monitored. Audit criteria are outlined in Annex B.

Scope

The scope of this audit included contracts over $5,000 awarded between 1 January 2009 and 31 December 2009. This included new contracts, standing offers and supply arrangements for goods, service and construction procured/contracted by DND, PWGSC and Defence Construction Canada (DCC). This audit did not include a review of PWGSC/CISD processes and procedures.

Methodology

- Reviewed TBS, PWGSC and DND/CF policies, guidelines and directives associated with contract security.
- Interviewed staff from DPM Secur, Assistant Deputy Minister (Materiel), Assistant Deputy Minister (Infrastructure and Environment), DCC and various Level 1 technical/project, procurement and contracting authorities.
- Reviewed a judgmental sample of 106 contract files and nine construction project files (two site visits).

[4] DPM Secur has since been re-organized and re-named. As a result, industrial security is now the responsibility of Director Military Police Operations.

- Analyzed contract description information from three contracting databases as well as information contained in the DPM Secur SRCL/VCR database.
- The sample was selected from the various databases—the Contracting Data Management System (contracts awarded by DND), PWGSC database (contracts awarded by PWGSC on behalf of DND) and DCC database (construction projects awarded by DCC on behalf of DND).
- An original sample of 96 contracts was selected. Ten additional contracts were subsequently added to provide further information with regards to contracts awarded by DND.

Finding and Recommendation

Industrial Security Program

[redacted]

Governance

Security program governance as a whole, and not just as it relates to the ISP, may be a serious impediment to meaningful change. While the recently created DSO position is responsible for the development, implementation, maintenance, coordination and monitoring of a departmental security program (DSP) consistent with security policy and associated standards,[5] this responsibility is not accompanied by any authority over the organizations involved in delivering the various elements of the security program. In the case of industrial security, this is exemplified by the fact that DPM Secur reports to the Canadian Forces Provost Marshal (CFPM) and not to the DSO. The ability of the DSO to implement a sufficiently rigorous ISP that meets the requirements of both the PGS and the Department may be impaired by the lack of direct authority over those responsible for performing day-to-day activities.

In addition to the overarching organizational reporting and authority issues, the mandate and objectives of the departmental ISP, [redacted] there is no documented objective statement for the ISP. The only place where high-level responsibilities are detailed is on the CFPM website where it is stated that DPM Secur is responsible for three activities: providing advice and guidance on the use of SRCLs; serving as the departmental signing authority for the SRCLs; and coordinating the VCR program. Departmental policies [redacted]

[redacted]

[5] TBS Directive on Departmental Security Management (2009).

According to the PGS, PWGSC is responsible for "ensuring compliance in those security contracts that afford industry access to government information and assets."[6]

[7]

[8]

[6] TBS Policy on Government Security (2009).
[7] Note: other responsibilities are defined in the PGS for the ISP; however, these are the ones that have direct impact on DND.
[8] DND/DCC, An integrated framework for managing industrial security on defence projects (2008).

Furthermore, the framework agreement states that "Director General Military Engineering is the central focal point within DND for managing industrial security on defence projects, and is responsible for communicating industrial security processes to all DND personnel involved in the management of realty assets."[9] This appears to be in conflict with DPM Secur's responsibilities with regards to industrial security. Currently available departmental guidance has proven to be of little assistance in this matter. [redacted]

Identification of Security Requirements

[redacted] TA/PAs are aware that they are required to identify contract-related security requirements, [redacted]

[redacted]

In order to assess the process controls, a judgmental sample of 96 contracts was reviewed, 30 of which identified security requirements while 66 stated that no security requirement existed. After assessing the statement of work for each contract, [redacted]

---

[9] Ibid.

Reviewed by CRS in accordance with the *Access to Information Act* (AIA). Information UNCLASSIFIED.

- [redacted]
- [redacted]
- [redacted][10]

[redacted]

Validation and Implementation

Current policy and guidance documents [redacted] the Procurement Administration Manual states that the "CA's security authority is responsible for ensuring that the suppliers are compliant with the security requirements identified in the SRCL."[11] Moreover, the TBS Directive on Departmental Security Management states that PWGSC is "responsible to ensure compliance in contracts with security requirements"[12] [redacted]

The PWGSC Supply Manual requires that CAs sign the SRCL once they have confirmed with CISD that the contractor has the appropriate clearance. TA/PAs interviewed [redacted] The 30 sampled contracts with an SRCL were reviewed to determine how contractor clearance confirmation was being performed. Of the 30 contracts reviewed, 26 were awarded by PWGSC; the remaining four were awarded by DND or DCC.

- [redacted]
- [redacted]
- [redacted]
- [redacted]

---

[10] [redacted]

[11] DND, Procurement Administration Manual (April 2011).

[12] TBS Directive on Departmental Security Management (2009).

Based on the interviews and file review conducted, [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]

In addition to the sign-off requirements on the SRCL, for contracts where DND or DCC is the CA, part II of the SRCL must be completed by the CA, submitted to CISD, who are to confirm clearances, and then returned to the CA as confirmation that the winning contractor has the appropriate clearance. [redacted]

- [redacted]
- [redacted]
- [redacted]

Access to DND Facilities or Assets

In instances where a contractor requires access to a DND/CF facility, the TA/PA is required to submit a VCR to DPM Secur 3 so that the contractor's clearance level can be confirmed. [redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted] The statements of work for these contracts had identified a need for security; [redacted]

Controlled Goods

In addition to confirming contractor clearances, contractors requiring access to controlled goods must be registered with PWGSC's Controlled Goods Directorate (CGD) prior to contract award. The requirement to access or be in possession of controlled goods must be identified as part of the SRCL process, and the procurement authority is responsible for ensuring that the contractor has a valid registration certificate. Nineteen of the 96 contracts reviewed identified a controlled goods component to the contract. [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted][13][redacted]

In order to afford the highest level of protection, to be in compliance with the *Defence Production Act* and uphold commitments to the allies, the Department must have processes and controls in place to ensure these commitments and requirements are implemented.

[13] DWAN website reference: "Contractors who perform the totality of their contracted work within a DND establishment (a facility under the control of DND and where DND has authority and responsibility for security), whether on a full-time or part-time basis (i.e., no work is performed off-site)."

Monitoring and Oversight

To determine whether security requirements were being monitored, nine construction projects were selected from two CF locations. [14]

Finally, at the locations visited, the practice was to rely on DCC to notify the project manager of security-related issues that might arise. Therefore, the responsibility for the project's security requirements appears to reside with DCC,

[14] For construction projects, the term "project manager" is used instead of "technical authority."

Recommendation

It is recommended that the VCDS in collaboration with other Level 1 organizations review and revise the objectives and practices of the ISP in order to ensure they address the PGS, controlled goods commitments, as well as the unique requirements of the DND/CF. This includes ensuring that:

- Industrial security policies are comprehensive and complete, covering all phases of the procurement and contracting process where security must be considered and managed. The policies should be well communicated and clearly define roles, responsibilities and accountabilities related to all phases of the industrial security process beginning with the identification of a requirement through to contract closure;
- There are risk management processes in place to monitor adherence to identified security requirements or where no security requirement exists; there are mechanisms in place to ensure the determination of the "non-requirement" is accurate and supported; and
- A robust training and awareness plan is developed to ensure that the appropriate personnel are aware of all industrial security requirements, associated responsibilities and departmental subject matter experts.

OPI: VCDS with affected Level 1 organizations

Annex A—Management Action Plan

CRS Recommendation

It is recommended that the VCDS in collaboration with other Level 1 organizations review and revise the objectives and practices of the ISP in order to ensure they address the PGS, controlled goods commitments, as well as the unique requirements of the DND/CF. This includes ensuring that:

1. Industrial security policies are comprehensive and complete, covering all phases of the procurement and contracting process where security must be considered and managed. The policies should be well communicated and clearly define roles, responsibilities and accountabilities related to all phases of the industrial security process beginning with the identification of a requirement through to contract closure;

2. There are risk management processes in place to monitor adherence to identified security requirements or where no security requirement exists; there are mechanisms in place to ensure the determination of the "non-requirement" is accurate and supported; and

3. A robust training and awareness plan is developed to ensure that the appropriate personnel are aware of all industrial security requirements, associated responsibilities and departmental subject matter experts.

Management Action

1. VCDS concurs completely with the audit recommendations. The Security Renewal Campaign Plan, currently ongoing under the leadership of the DSO, will address all of the specific recommendations. The Defence Security Plan and DSM, currently under development, will provide the comprehensive security policies identified as being required. The oversight and governance construct, both within the DSO/Director Defence Security organization and that provided by the Senior Security Advisory Committee reporting to the Defence Management Committee, will ensure compliance with the risk management processes to be laid out in the Defence Security Plan and DSM, and the ISP will be included in the Department-wide rejuvenation of security education, training and awareness, which is already under way. In addition, the DSO is currently studying, in collaboration with PWGSC and other subject matter experts at TBS, how to enhance the efficiency and effectiveness of DND's application of the ISP now and in the future. A gap analysis and a detailed work plan for both the Defence Security Plan and DSM will be completed no later than 1 October 2011. At that point, the contract to complete the security plan and DSM can be competed with a completion date forecasted for 1 April 2012.

OPI: VCDS with affected L1 organizations
Target Date: April 2012

Annex B—Audit Criteria

Objective

The objective of the audit was to assess whether there are adequate processes in place to ensure contract-related security requirements are identified, validated, implemented and monitored.

Criteria

1. Governance structures are in place with clear objectives, roles and responsibilities to ensure the effective operation of the DND ISP.

2. Documented risk management strategy exists that addresses known and potential security risks related to the achievement of program objectives.

3. Departmental security policies clearly detail responsibilities for the ISP and have been communicated and implemented throughout the Department.

4. Industrial security procedures and processes have been developed, are monitored and support the achievement of program objectives.