National Defence / Défense nationale

Chief Review Services / Chef - Service d'examen

CRS / CS Ex

Audit Follow-up on Departmental Security Program Implementation and Security-Related Audits

June 2012

7050-33-7 (CRS)



Canada

Caveat

The results of this work do not constitute an audit. Rather, this report provides an update on the progress made regarding the management action plans (MAP) of the security-related audits. This information was obtained through documentation review and interviews.

Table of Contents

Acronyms and Abbreviations

A&A	Assessment and Authorization
ADM(IM)	Assistant Deputy Minister (Information Management)
ANST	Active Network Security Testing
ARA	Aggregated Risk Assessment
C&A	Certification and Accreditation
CF	Canadian Forces
CF MP Gp HQ	Canadian Forces Military Police Group Headquarters
CRS	Chief Review Services
CSEC	Communications Security Establishment Canada
CSIS	Canadian Security Intelligence Service
CSNI	Consolidated Secret Network Infrastructure
DDS	Director Defence Security
Dir IM Secur	Director Information Management Security
DND	Department of National Defence
DPM Secur	Deputy Provost Marshal (Security)
DSM	Defence Security Manual
DSO	Departmental Security Officer
DSP	Departmental Security Plan
DWAN	Defence Wide Area Network
ISP	Industrial Security Program
IT	Information Technology
L1	Level One
MAP	Management Action Plan
NDSI	National Defence Security Instruction
OPI	Office of Primary Interest
PGS	Policy on Government Security
SSAC	Senior Security Advisory Committee
TBS	Treasury Board of Canada Secretariat
TRA	Threat and Risk Assessment
VCDS	Vice Chief of the Defence Staff

Introduction

Chief Review Services (CRS) first began reporting on the Department of National Defence's (DND) security program with the release of the May 2004 report on the Audit of Security for Sensitive Inventories. CRS now has two audit teams dedicated to the conduct of security-related audits [redacted] a Memorandum of Understanding with Communications Security Establishment Canada (CSEC) through which active network security testing services (ANST) were provided to the Department.

Since the conduct of the sensitive inventories audit, CRS has performed audits of the Department's security clearance process, the process used to certify and accredit information systems and networks, the security incident management process and the contracting security process. Additionally, with the assistance of the CSEC ANST team, security assessments of both the Defence Wide Area Network (DWAN) and the Consolidated Secret Network Infrastructure (CSNI) were performed.

Three common issues have emerged from each of the security-related audits. The first being the [redacted]

The second issue is the [redacted] security policy and guidance. Departmental security-related policy documents are significantly outdated and require a complete rewrite to take into account significant changes in departmental organizational structure, operational procedures and authorities. The current security policy suite consists of a mix of outdated National Defence Security Policy, National Defence Security Instruction (NDSI) and Defence Security Manual (DSM) documents; [redacted]

The final issue, but one that is just as important as the others and possibly a direct result of the first two issues, [redacted]

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

Annex A provides an update on the MAPs for key findings associated with each of the previously conducted security-related audits and assessments. The information was provided by the organizations responsible for implementation of the action plans. With few exceptions, the three key issues—[redacted] policy [redacted] In the case of the Information Technology (IT-)related issues, there has been more progress, [redacted]

Progress against Action Plans

While both the Vice Chief of the Defence Staff (VCDS) and the Assistant Deputy Minister (Information Management) (ADM(IM)) have acknowledged the identified deficiencies, the implementation of management action plans has been slow; [redacted] Aside from the completion of the DWAN MAP [redacted] developed to address the findings detailed in the CSEC assessments, [redacted]

Director Information Management Security (Dir IM Secur) staff have made significant progress towards developing a more rigorous approach to accrediting the Department's numerous information systems and networks; [redacted] Due to a dependency on system owners providing the required documentation, expected completion dates cannot be provided. [redacted] Department cannot be definitively quantified; regardless, [redacted] As an example, a recently completed accreditation of a portion of the [redacted]

[redacted]

Contributing Factors

While the creation of the Director Defence Security (DDS) organization has been a positive step, [redacted] the development of a truly functional security program. Recent events, both actual and simulated, have [redacted]

[redacted]

Overall Assessment

Notwithstanding the creation of the DDS organization and current initiatives to address the misalignment of accountability and authority, [redacted] before any process changes are made, a [redacted]

Annex A—Key Security Audit Observations, Recommendations and Management Action Plans

1. Physical Security of Sensitive Inventories (OPI: VCDS) May 2004

Key Observation: [redacted]

Impact/Risk: [redacted]

Audit Follow-Up, August 2008

Key Observation: [redacted]

Impact/Risk: [redacted]

[redacted] [1] [redacted]

Audit Follow-Up, May 2012

Key Observation: [redacted]

[1] At the time of original audit, the organization responsible for sensitive inventories was the Deputy Provost Marshal (Security) (DPM Secur). This responsibility now falls under the CF MP Gp HQ.

Annex A

1. Physical Security of Sensitive Inventories (OPI: VCDS) May 2004 (cont'd)

Key Recommendations	Key Management Action Plans	CRS Audit Follow-Up, May 2012

Table 1. Physical Security of Sensitive Inventories, May 2004. The results of a CRS follow-up in 2012

Annex A

2. Security Clearance Process (OPI: VCDS) September 2006

Key Observation: [redacted] Policy on Government Security (PGS) required characteristics and attributes (identity, trustworthiness, honesty, financial responsibility, habits, stability, loyalty, associations, values and beliefs) [redacted]

Impact/Risk: Reliability status serves as the foundation for security clearances. The CF MP Gp HQ[2] (specifically, the Directorate of Police and Security) provides the hiring organization with automated credit and criminal name check results. [redacted]

Secret clearances are granted based on information obtained by repeating previously performed credit and criminal name checks and getting CSIS to perform various checks [redacted]

There is minimal opportunity to identify [redacted]

The Department [redacted]

Audit Follow-Up, August 2008

Key Observation: The security clearance process [redacted]

Impact/Risk: Effective April 1, 2008, [redacted]

[2] At the time of original audit, the organization responsible for security clearances was DPM Secur. This responsibility now falls under the CF MP Gp HQ.

Annex A

2. Security Clearance Process (OPI: VCDS) September 2006 (cont'd)

Audit Follow-Up, May 2012

Key Observation: [redacted] addressing key recommendations from the original audit. [redacted] of the security clearance process.

Impact/Risk: [redacted]

Key Recommendations	Key Management Action Plans	CRS Audit Follow Up, May 2012
Initiate a full review and revision of the security clearance program that addresses identified shortcomings in the current reliability/clearance process.	Initiate review addressing security clearance process issues identified to ensure all PGS guidelines and treaty obligations are met, options/feasibility of checks that provide higher levels of assurance are considered, [redacted] and supporting documentation is appropriately retained and stored. **Initial Target Date: December 2006**	[redacted] The Personnel Security Working Group is working to define DND requirements for security screening and examine options to improve the security clearance process. [redacted] TBS is currently studying the [redacted] [redacted] **Time Lapse: 5.5 years**

Annex A

2. Security Clearance Process (OPI: VCDS) September 2006 (cont'd)

Key Recommendations	Key Management Action Plans	CRS Audit Follow Up, May 2012
Before making changes, conduct a risk management assessment of the clearance process addressing each of the risk-related issues and identified process deficiencies.	As part of the security clearance process review, conduct a risk management assessment that addresses the identified issues and deficiencies. **Initial Target Date: November 2006**	Risk assessment completed as part of an ARA in December 2011. [redacted] [redacted] **Time Lapse: 5.5 years**

Table 2. Security Clearance Process, September 2006. A 2012 audit follow-up [redacted]

Annex A

3. Certification and Accreditation (C&A) Process (OPI: ADM(IM)) September 2007

Key Observations: The process [redacted] determined, documented or communicated.

Impact/Risk: [redacted]

Audit Follow-Up, July 2009

Key Observations: Progress has been slow in [redacted] original CRS report.

Senior management's [redacted] and the associated authorities and accountabilities for the [redacted] been determined, documented or communicated.

Audit Follow-Up, May 2012

Key Observation: Work is under way to transition from the C&A process to the assessment and authorization (A&A) process outlined by CSEC. [redacted]

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

Annex A

3. Certification and Accreditation (C&A) Process (OPI: ADM(IM)) September 2007 (cont'd)

Key Recommendations	Key Management Action Plans	CRS Audit Follow-Up, May 2012
		C&A Information Technology security policy authorities and responsibilities have been articulated through Defence Administrative Order and Directive 1000-1, 6003-0 and 6003-1. **Time Lapse: 2.5 years**
		C&A status [3]

[3] Numbers do not include systems certified and accredited for operations and exercises.

Annex A

3. Certification and Accreditation (C&A) Process (OPI: ADM(IM)) September 2007 (cont'd)

Key Recommendations	Key Management Action Plans	CRS Audit Follow-Up, May 2012
Elicit senior executive management [redacted] and then develop and seek endorsement for [redacted] and accountabilities, documentation and communication requirements. **(OPI: VCDS)**	Quantify and develop recommendations for [redacted] management. **Initial Target Date: March 2008**	Senior management [redacted] **Time lapse: 4 years**

Table 3. Certification and Accreditation Process, September 2007. [redacted]

Annex A

4. Security Posture Assessment—Defence Wide Area Network (DWAN) & Consolidated Secret Network Infrastructure (CSNI) (OPI: ADM(IM)) May 2009

Key Observations:

Impact/Risk:

Audit Follow-Up, May 2012

Key Observation: The implementation of enhanced security measures can only be confirmed by conducting a follow-up security posture assessment.

Key Recommendation	Summary of Management Action Plans	CRS Audit Follow-Up, May 2012
Within the context of a TRA for each system consider implementation of enhanced security measures in areas such as: • • • • • • • • •	Recommendations were assessed/prioritized based on Technical management action plans were developed for each of the identified areas in order to enhance the security posture of the DWAN and CSNI. **Initial Target Date: March 2010**	[4]

Table 4. Security Posture Assessment—DWAN and CSNI, May 2009.

[4]

Annex A

5. Security Incident Management (OPI: VCDS) June 2010

Key Observation: [illegible]

Impact/Risk: [illegible]

Audit Follow-Up, May 2012

Key Observation: [illegible]

Key Recommendations	Key Management Action Plans	CRS Audit Follow-Up, May 2012
[illegible]	[illegible]	[illegible]
Revise security policies to reflect appropriate roles, responsibilities and authorities, and to ensure requirements are clear and consistent within the Department and aligned with the PGS.	Revise and update the departmental security policies as well as administrative directives related to the governance of security matters. Promulgate clear guidance in the Department's core security policy (in draft) and subsequent security standards, in order to ensure the proper management of security incidents, mitigating strategies, and compliance with the PGS. **Initial Target Date: December 2010**	Draft security incident management procedures have been developed. **Time lapse: 1.5 years**

Annex A

5. Security Incident Management (OPI: VCDS) June 2010 (cont'd)

Key Recommendations	Key Management Action Plans	CRS Audit Follow-Up, May 2012
Develop and implement strategies to ensure that the appropriate organizations receive relevant security incident information, such as damage assessments and security investigation reports, to make certain policy requirements are met and appropriate action is taken to minimize damage and prevent recurrence.	Engage key stakeholders to develop proper reporting procedures and oversight mechanisms regarding the actions to be taken following an investigation. [redacted] **Initial Target Date: January 2011**	[redacted] Strategies in place to ensure appropriate organizations receive relevant security incident information (i.e., damage assessments, security investigation reports) to minimize damage and prevent recurrence. No supporting documentation provided. **Time lapse: 1.5 years**
Forum/mechanism to be established to periodically communicate security incident information to senior management.	This recommendation has also been noted in past reports. Consequently, the VCDS has re-established the Senior Security Advisory Committee (SSAC) to ensure that such communication takes place.	Completed. The SSAC has been officially stood up through the renewal of the security campaign plan and meets quarterly. **Note:** SSAC membership has been downgraded from L1s to working level.

Table 5. Security Incident Management, June 2010. [redacted]

Annex A

6. Industrial Security (OPI: VCDS) May 2011

Key Observations: The Department's Industrial Security Program (ISP) [redacted] the PGS and its associated directives.

Impact/Risk: The CF MP Gp HQ[5] [redacted]

Audit Follow-Up, May 2012

Key Observation: [redacted] key recommendations from the original audit. [redacted] indicates a review of the departmental ISP has taken place. The industrial security process [redacted]

Key Recommendation	Key Management Action Plans	CRS Audit Follow-Up, May 2012
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 the following: • Clear, comprehensive, complete and well-communicated industrial security policies.	The Security Renewal Campaign Plan, currently ongoing under the leadership of the DSO, will address all of the specific recommendations. • The DSP and DSM will provide the required comprehensive security policies. [redacted]	[redacted] development of an updated DSP/DSM. Draft version of DSM from 2008 [redacted] [redacted] [redacted]

[5] At the time of original audit, the organization responsible for industrial security was DPM Secur. This responsibility now falls under the CF MP Gp HQ.

Annex A

6. Industrial Security (OPI: VCDS) May 2011 (cont'd)

Key Recommendation	Key Management Action Plans	CRS Audit Follow-Up, May 2012
• Risk management processes to monitor adherence to identified security requirements or where no security requirement exists, mechanisms to ensure the determination of the "non-requirement" is accurate and supported. • A robust training and awareness plan to ensure that the appropriate personnel are aware of all industrial security requirements, associated responsibilities and sources of expertise within the Department.	• The oversight and governance construct (DSO/DDS organization and the SSAC reporting to the Defence Management Committee) will ensure compliance with the risk management processes. • The ISP will be included in the Department-wide rejuvenation of security education, training and awareness. **Initial Target Date: April 2012**	

Table 6. Industrial Security, May 2011. According to the CRS audit follow-up in 2012, | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |