National Defence Défense nationale

Chief Review Services Chef - Service d'examen

CRS CS Ex

Reviewed by CRS in accordance with the *Access to Information Act* (AIA). Information withheld in accordance with the AIA under section 15(1)(c) International affairs and defence of the AIA. Information UNCLASSIFIED.

Audit of Information Technology Security: Certification and Accreditation

September 2007

7050-33 (CRS)

Canada

TABLE OF CONTENTS

LIST OF ACRONYMS

ADM(IM)	Assistant Deputy Minister (Information Management)
C&A	Certification and Accreditation
CDS	Chief of the Defence Staff
CF	Canadian Forces
CFNOC	Canadian Forces Network Operations Centre
CFSS	Canadian Forces Supply System
CNet	Classified Network
COMSEC	Communications Security
COS(IM)	Chief of Staff (Information Management)
CRS	Chief Review Services
CSE	Communications Security Establishment
Dir IM Secur	Director Information Management Security
DM	Deputy Minister
DND	Department of National Defence
DSO	Departmental Security Officer
DVCN	Defence Video Conference Network
DWAN	Defence Wide Area Network
EMSEC	Emissions Security
FMAS	Financial Managerial Accounting System
GSP	Government Security Policy
HRMS	Human Resources Management System
IAP	Interim Authority to Process
IS	Information system
IT	Information technology
MASIS	Materiel Acquisition and Support Information System
MITS	Management of Information Technology Security
NDSI	National Defence Security Instruction
OA	Operational Authority
RPSR	Revised Pay System for the Reserves
TAV	Technical assistance visit
TB	Treasury Board
TRA	Threat and Risk Assessment
TRAP	Tracking Application
V&O	Verification and Oversight
VCDS	Vice Chief of the Defence Staff

RESULTS IN BRIEF

Overall Assessment

The DND/CF C&A process ……………....
……………………….…
……………………….…
……………………….…
……………………….…
……………………….…
……………………….…
……………………….…

The Government Security Policy (GSP) states that "departments must apply baseline security controls, continuously monitor service delivery levels, track and analyse threats to departmental IT systems, and establish effective incident response and IT continuity mechanisms."[1] The Certification and Accreditation (C&A) process is the primary mechanism to ensure that baseline security controls are applied and additional controls are implemented to prevent compromise of the confidentiality, integrity and availability of Department of National Defence and Canadian Forces (DND/CF) information from internal and external threats. Director Information Management Security (Dir IM Secur) is the DND/CF information technology (IT) security coordinator and is responsible for ensuring that DND/CF IT systems have been properly certified and accredited prior to operating.

The Department's ability to maintain public and international confidence, to comply with government statutes such as the *Security of Information Act* and the *Privacy Act*, and to support the successful completion of military operations and government initiatives such as audited financial statements, relies heavily on the confidentiality, integrity and availability of numerous information systems. …………………………..……… the Department's current C&A program ………………………………………………….

Findings and Recommendations

Certification and Accreditation. The DND/CF C&A process ………………………..
…………………. to ensure systems are certified and accredited in accordance with the GSP.
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………………………………
……………………………………………………………………

Recommendations. Chief of Staff (Information Management) (COS(IM)) should …………
……….. the C&A process ……………………………. the GSP and associated standards and guidelines. In addition, a plan of action should be developed and implemented to …………..
…………………………………………….

Residual Risk. …………………………………………………………………………………
…………………………………………………………………………………………..
……………….

[1] *Government Security Policy*, S10.12, February 2002.

Recommendation. The Vice Chief of the Defence Staff (VCDS), in conjunction with COS(IM), ……………………………………………………………………………………………… ………………………………………

- ……………………………………………………………………………………………… …………
- ……………………………………………………………………………………………… ………………..
- ………………………………………………………………………………………………

Contributing Factors. The C&A program requires a clear, concise and consistent direction that articulates current roles, responsibilities, levels of authority, and policy requirements. ……………………………………………………………………………………………… ……………………………………………

Recommendations. Dir IM Secur needs to update departmental C&A policy to clearly reflect roles, responsibilities, authorities and accountabilities and to ensure the compliance with the GSP C&A requirements and senior executive management direction regarding the documentation and acceptance of residual risk.

It is recommended that COS(IM) …………………………………………………………..… ……………………………………………………………………………………………… ……………………………………

Note: For a more detailed list of Chief of Review Services (CRS) recommendations and management response please refer to Annex A—Management Action Plan.

INTRODUCTION

Background

DND/CF relies heavily on information and supporting systems for the success of both day-to-day administrative and military activities. The sensitivity of information in DND/CF is wide-ranging—public and commercial information, personal data, military operations, and national and international intelligence—and its confidentiality, integrity, availability and value to the department needs to be preserved. Therefore, to protect the health, safety, security and economic well-being of Canadians, and to ensure compliance with government statutes, it is critical that DND/CF apply baseline security controls and any additional controls deemed necessary based on a comprehensive assessment of internal and external threats, risks and vulnerabilities of a system and its information.

Dir IM Secur is responsible for the departmental IT security program. This responsibility includes the GSP requirement that IT systems be properly certified and accredited prior to operation and that these systems be subjected to sound configuration management practices.[2] Dir IM Secur 2 is responsible for the C&A program—certifying and accrediting information systems (IS) and performing verification and oversight.

Objective

The objective of this audit is to assess the management control framework with respect to IT security activities undertaken to ensure the confidentiality, integrity and availability of IT systems, assets, data and services.

Scope

Due to the complexity of the subject matter and varied elements of the IT security program, this audit is being conducted in phases. As such, this report is limited to the C&A program managed by Dir IM Secur. The audit focused on the information and processes used to grant a system accreditation and to monitor the C&A program. It did not include testing of security controls for specific systems nor did it include an assessment of C&A activities performed at the Base/Wing level.

Certification and Accreditation

According to Treasury Board’s (TB) operational security standard—Management of Information Technology Security (MITS)—“the purpose of certification is to verify that the security requirements established for a particular system or service are met and that the controls and safeguards work as intended. The purpose of accreditation is to signify that management has authorized the system or service to operate and has accepted the residual risk of operating the

[2] *Government Security Policy*, S10.12.1a, February 2002.

system or service, based on the certification evidence."[3] Therefore, a system must be certified before it can be accredited, and must be accredited prior to operating. Figure 1 depicts the C&A process according to Communications Security Establishment (CSE) guidelines.

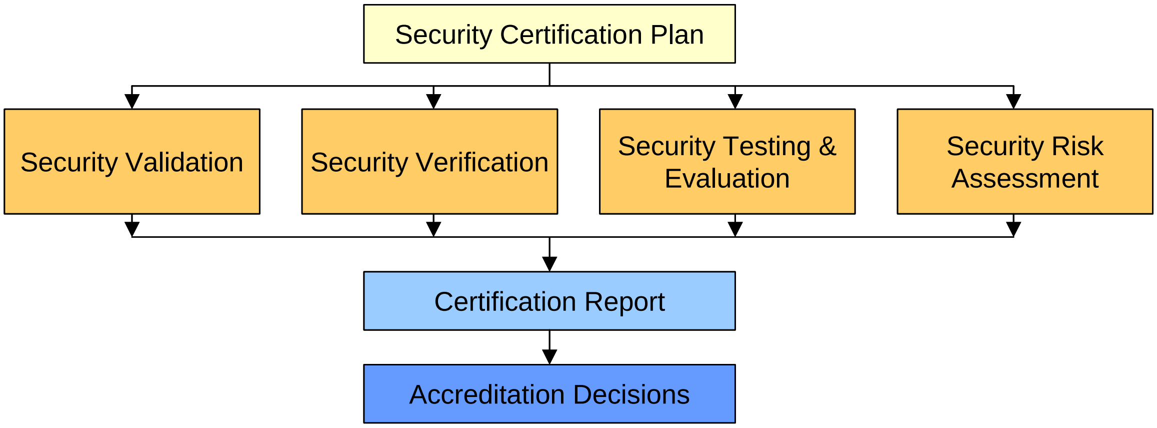

Figure 1. C&A Process. *According to the CSE C&A guideline, accreditation decisions are based on a comprehensive certification process, including validation, verification, testing and evaluation, and a risk assessment of security controls.*[4]

The National Defence Security Instruction (NDSI) 70: IS Security, defines a system as "hardware and software that processes, stores, transfers or otherwise communicates data or electronic information." It includes, but is not limited to, "single or interconnected (networked) computers of any sort that can intercommunicate."

DND/CF policies and guidelines describe three types of accreditations:

- **Formal Accreditation—**formal approval for a system to operate for a specified period of time (maximum five years) at an identified sensitivity level, in a particular configuration, at an identified environment/location, in a specified mode of operation, and under any other conditions prescribed by the Accreditor.
- **Interim Authority to Process (IAP)—**temporary approval for a system to operate for a specified period of time (maximum two years) due to extenuating circumstances. This allows a system to operate while security deficiencies are corrected, formal accreditation documentation is completed or where operations require the system to operate.
- **Security Waiver—**used when the system is required to operate and one or more security deficiencies will not be corrected during the life of the IS.

[3] *TBS Operational Security Standard: Management of Information Technology Security*, Section 12.3.3 Certification and Accreditation.

[4] *A Guide to Certification and Accreditation for Information Technology Systems (MG-4)*, CSE, January 1996.

Methodology

- Reviewed relevant policies and guidelines, including the GSP and related standards, CSE Guide to C&A for IT Systems, NDSI /Policies for chapters 70 (IS Security), 34 (IS Security: C&A (draft)) and 4 (Threat and Risk Assessment (TRA)), and the DND/CF C&A Guideline (2005).
- Selected and reviewed the C&A files for 20 national systems, relative to NDSI 70 documentation requirements. Although the sample is not statistically representative, it included significant systems from the designated and classified domains (list of systems in Annex B).
- Reviewed 16 technical assistance visits (TAV) reports resulting from site visits performed by Dir IM Secur 2 Verification and Oversight (V&O) sub-section since January 2005.
- Interviewed the Departmental Security Officer (DSO) and Dir IM Secur staff, including the section heads, Dir IM Secur 2 C&A analysts, and V&O staff.

FINDINGS AND RECOMMENDATIONS

Certification and Accreditation

……
……
……………………………………………………………

DND/CF C&A Process

For a system to be properly certified, there should be activities that validate, verify, test and evaluate, and assess the risk of system security controls. Certification activities are supposed to provide assurance that the controls are implemented, sufficient and functioning as intended to mitigate risk to an acceptable level.

- **Validation—**confirms, through mapping, that the security features meet policy requirements (physical, personnel, administrative, computer and communication).
- **Verification—**confirms that technical and non-technical controls were implemented correctly to work as intended, and meet the assurance requirements.
- **Testing and Evaluation—**demonstrates that security features work correctly and determine whether vulnerabilities exist.
- **Risk Assessment—**evaluation of residual risk based on the effectiveness of safeguards, the likelihood of vulnerabilities being exploited and the consequence if compromised.

The residual risk and accreditation decisions should be based on the outcome of the certification activities. By signing the accreditation letter, the Operational Authority (OA) agrees to implement the conditions to operate set out by the accreditor, and accepts and commits to maintaining the stated residual risk. Without a robust and integrated certification process, there would be little value in accrediting systems.

Currently, Dir IM Secur—the accreditor—assesses residual risk and grants the accreditation
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
…………………………………………………………………………………………………
………………..

- Dir IM Secur 2 ……………………………………………………………………………… accordance with the NDSI 70 (see detailed results of the C&A file review in Annex C). ……………………………………………………………………………………… ………………………………………………………………………..

  - …………………………………………………………………………………………
  - Although the minimum documentation for a formal accreditation is more stringent than for an IAP, formal accreditations have been granted …………………………. ……………………………………
  - ………………………………………………………………………………………… ……………………………………………………
- ………………………………………………………………………
  - Information sensitivity impacts the minimum standard of security controls required for a given system.
  - Access to the vast majority of DND/CF systems is provided via the Defence Wide Area Network (DWAN), which is only accredited to process information up to Protected A. Given that the requirements for security controls for information designated/classified at Protected B and above ……………………….………… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ……………………………………………………[5] ……..…………………………………… ……………………………………………………………[6] ………………...……… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ……………………………………………………………………
- Contractors often conduct TRA. ……………………………………………...… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………

………………………………………………………………………………………………… ……………………………………………………………………………For example, Canadian Forces Network Operations Centre (CFNOC) has a mandate to perform vulnerability assessments. ………………………………………………………………………….………… ………………………………………………………………………………………………… ………………………

[5] ……… ……..

[6] ………

Accreditation Status and Types

………………………………….. GSP requirement that systems be accredited prior to implementation and continued use. According to Dir IM Secur 2 records, ……..

Status	Number of Systems	Percentage
Accredited/IAP	…..	…..
Expired	…..	…..
Unknown/Pending	…..	…..
New	…..	…..
As Required	…..	…..
Dormant	…..	…..
Total	…..	…..

Table 1. Accreditation Status for National Systems. [7] ………………………………….………

- There are at least three tracking tools being used to track accreditation status in DND/CF, …………………………………………………………
  - **C&A Tracking Application (TRAP)**—this tool was developed to track C&A status for national and local system accreditations. ………
  - **Task list for national systems**—this Excel spreadsheet was not intended to be used to track accreditation status. It was designed to task C&A analysts at the national level. ……
  - **Task list for operations and exercises**—this Excel spreadsheet was developed to track accreditations granted for military operations and exercises. …………………………………………………………………………………………
- The NDSI 70 states that the departmental C&A Authority (i.e., Dir IM Secur) is responsible to maintain a database of departmental IS and the corresponding C&A status. The MITS states that "departments need to continually be aware of the assets they hold, and their associated sensitivity and criticality."[8] In 2005 and 2006,[9] CRS made

[7] Source: ……………………………………………………………………..

[8] *Operational Security Standard: Management of Information Technology Security*, Section 4: Principles—Decision making requires continuous risk management.

[9] *Review of Management of Non-Classified Information Technology Hardware*, September 2006. *Internal Audit of Software Acquisition and Maintenance*, September 2005.

recommendations to establish and maintain a department-wide inventory of IT assets. ……………………………………………………………………………………… ……………………………………………………………………

Dir IM Secur 2 staff indicated that an IAP, ……………………………………………………….. ………………………………………………………………………..

- Of the most recent accreditations for 20 sample files, ………………………………….. …………………….. (Annex B).
- CSE C&A guidelines state that the maximum length for interim approvals (i.e., IAP) is one year; DND policy indicates that they can be granted for periods of up to two years.
  - o ………………………………………………………………………………………… ……..
  - o ………………………………………………………………………………………… ……………………………………………………………………
- ……………………………………………………………………………………………… …………………………………………………………………………………… ………………………………………………………………………………………………
  - o …………………………………………………………… …………………………………………………………… …………………………………………………………… …………………………………………………………… …………………………………………………………… …………………………………………………………… …………………………………………………………… ……..
  - o Dir IM Secur staff indicated that once a system is ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ………………………………………………………………………………………… ………..

…………………………………
…………………………………
…………………………………
…………………………………
…………………………………
…………………………………
…………………………………
………………..

- Dir IM Secur staff indicated that ……………………………………………………… ……………………………………………………………………………………………. …………………………………………..

………………………………………………………………………………………………… ………………………………………………………………………………………………… ………………………………………………………………………………………………… ………………………………………………………………………………………………… ………………………………………………………………………………………………… ………………………………………………………………………………………………… …………………………………………………………

Recommendations

OPI	RECOMMENDATIONS
ADM(IM)/COS(IM)	**DND/CF C&A Process.** .... to ensure compliance with the GSP and associated standards and guidelines.
ADM(IM)/COS(IM)	**Accreditation Status and Type.** Develop and implement a plan of action to ....

Residual Risk

……………………………………………………………………………………………………
…………………………………………………………………………………….

Acceptance and Accountability for Residual Risk

As was highlighted in the CRS *Audit of the Security Clearance Process* (September 2006), there is …………………………………………………………………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… ………………… The issue is further complicated when it comes to determining who can accept risk, and how they ……………………………………………………………………….. …………………………………

- The NDSI 70 states that "by virtue of accrediting an IS, the Department assumes the residual risk to the IS. With the assumption of risk comes the stipulation that the IS OA will continue to manage the residual risk at a level acceptable to the accreditor." It also states that "only when needed, as an immediate operational requirement, shall IS of moderate or high operating risk be accredited."[10] In these cases, the DSO must also be apprised of and give approval for the system to operate. ………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… ………………
- …………………………………………………………………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… ………………… Additionally, while the level of residual risk associated with a particular system is documented, ……………………………………………………….. …………………………………………………………………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… …………………………………………………………………………………………… ………..
  - Dir IM Secur, who is responsible for the DND/CF IT security program (including the C&A process), ………………………………… An assessment of residual risk is performed ……………………………………………………………………… ……………………………………………………………………………….. ……………………………………………………………………………… ……………

[10] NDSI 70—Information System Security, S70.23, June 1999.

- o ……………………………………………………………………………………… ……………………………………………………………………………………… …………………………………………

Security Risks and Impacts

In order to maintain the confidentiality, integrity and availability of DND/CF information, mitigating measures in each of the four security pillars—personnel, physical, procedural, and technical—must be maintained. In the current C&A process, ………………………………… ……………………………………………………………………………………………… ……………………………………………………………… [11] ……………………………………… security at specific DND/CF facilities.[12]

- When accrediting information systems, …………………………………………………… ……………………………………………………………………………………………… ……………………………………………………………………………………………… ………….
- ……………………………………………………………………………………………… ……………………………………………………

These results highlight …………………………………………………………………………….. ……………………………………………………………….

Recommendation

OPI	RECOMMENDATION
VCDS ADM(IM)/COS(IM)	**Residual Risk.** ……………………………………………………… ……………………………………………………………………… ……….. • …………………………………………………………………… ………………………… • …………………………………………………………………… …………………………………. • …………………………………………………………………… ………………………..

[11] CRS *Audit of the Security Clearance Process*, September 2006.
[12] CRS *Audit of Security for Sensitive Inventories*, May 2004.

Contributing Factors

> *The C&A program ……………………………………………………………………………… roles, responsibilities, levels of authority, and policy requirements.* …………………………… ……………………………………………………………………………………………… ………

DND/CF Policy

DND/CF IT security policies and guidelines are …………………………

- ………………………………………………………………………………. ……………………… For example, the NDSI 70:
  - ……………………………………………………………………….. the GSP dictates that departments establish IT continuity mechanisms. This is only reflected in the DND/CF C&A Guideline as a requirement for formal accreditation. ………… ………………………………………………………………………………… ………………………………………………………………………………… ………………………………………
  - Specifies that the DSO must approve systems with moderate or high risk. ………… ……………………………………………………………
  - ………………………………………………………………………………… ……………………………………………………
- ………………………………………………………………………………… ………………………
  - ………………………………………………………………………………… ………………………………………………………………………………… ……………………………………While the MITS is a guidance document in this ………………………………………………………………………………… ………………………………………………
  - ………………………………………………………………………………… ……………………………………………………………………
  - ………………………………………………………………………………… ………………………………………………………………………
  - ……………………………………………………………………………. ……………...
- Documentation requirements for C&A ………………………………………………

Resources

At the time of audit, ……………………………………………………………………….. systems at the national level. These systems are also required to be re-accredited or the original accreditation must be re-considered when:

- The current IAP or formal accreditation expires;
- The risk changes due to new threats, risks and vulnerabilities to the system/information;

- There are changes to the accredited configuration or security architecture; and/or
- There are changes in policy, standards and procedures.

The NDSI 70 indicates that the extent to which the system is re-accredited or the accreditation is reconsidered is at the discretion of the accreditor—Dir IM Secur. …………………………..
…………………………………………………………………………………………………
……………………………………………………………………………………

Additionally, Dir IM Secur ………………………………….
……………………………………………………………
……………………………………………………………
……………………………………………………………
……………………………………………………………
……………………………………………………………
……………………………………………………………
……………………………………………………………
……………………………………………………………
……………………………………………………………
……..

Dir IM Secur ………………
……………………………..
……………………………..
……………………………..
……………………………..
……………………………..
……………………………..
……………………………..
……………………………..
………………….

Dir IM Secur 2 has ……………………………………………….. Staffing these positions would help to alleviate some of the issues addressed in this report; …………………………
…………………………………………………………………………………………
…………………………………………… Other areas to consider when identifying resource requirements would be training for C&A Analysts; tracking tools; ………. roles, responsibilities, policies, procedures; the impact of deployments; and ……… handover procedures to ensure continuity in system knowledge and status.

Recommendations

OPI	RECOMMENDATIONS
ADM(IM)/COS(IM)/ Dir IM Secur	**DND/CF Policy.** Departmental C&A policy needs to be updated to clearly reflect roles, responsibilities, authorities and accountabilities and to ensure the compliance with the GSP C&A requirements and senior executive management direction regarding the documentation and acceptance of residual risk.
ADM(IM)/COS(IM)	**Resources.** Determine, fund and acquire the necessary resources and tools to conduct and administer a C&A program …………….. ………………………………………………………………………..

ANNEX A—MANAGEMENT ACTION PLAN

Ser	CRS Recommendation	OPI	Management Action	Target Completion Date
Certification and Accreditation				
1.	**DND/CF C&A Process.** ………… …………………………………….. to ensure compliance with the GSP and associated standards and guidelines.	ADM(IM)/ COS(IM)	It is agreed that the Department has not always been successful ………………. ……………….. and that there are measures that can be taken to give a ………..………..……………….. ………..………..……………….. ………….. should additional resources be dedicated to this activity. It is possible to provide greater assurance that the ……………………. ………..………..……………….. ………..………..……………….. ………..………..……………….. ………..………..……………….. ………..………..……………….. ………..………..……………….. ………… The detailed plan will be produced by the end of Oct 07.	31 Oct 07
2.	**Accreditation Status and Type.** Develop and implement a plan of action to …………………………… …………………………………..	ADM(IM)/ COS(IM)	ADM(IM)/COS(IM) agrees that the current situation needs more attention and will develop a plan ……………. ………..………..……………….. ……………	31 Oct 07
Residual Risk				
3.	……………………………………… ……………………………………… ……………………………………… ………… • ………………………………… ………………………………… …………………………………	VCDS		

Residual Risk (cont'd)				
	• …………………………………… …………………………………… …………………………………… • …………………………………… …………………………………… ……………………………………	 ADM(IM)/ COS(IM)	VCDS agrees and it is anticipated that initial actions to quantify and develop recommendations for ……………….. ………………………………………. ……………..will be completed by the end of Mar 08. ADM(IM)/COS(IM) agrees and indicates that this activity is properly led by the VCDS and his staff. IM Group staff will assist as required in this effort.	Mar 08
Contributing Factors				
4.	**DND/CF Policy.** Departmental C&A policy needs to be updated to clearly reflect roles, responsibilities, authorities and accountabilities and to ensure the compliance with the GSP C&A requirements and senior executive management direction regarding the documentation and acceptance of residual risk.	ADM(IM)/ COS(IM)/ Dir IM Secur	ADM(IM)/COS(IM)/Dir IM Secur agree. The IT Security policy is in the process of being rewritten as part of the DSO's move from National Defence Security Policy and National Defence Security Instructions to the Defence Security Manual. The first IT Security policy document (DSM 700 Chapter 1), which describes the IT Security portion of the Departmental Security Program and its underlying risk management philosophy, has been released for coordination across the Department and should be ready for submission to the DSO this fall. Chapter 2, on C&A, will follow.	Fall 07
5.	**Resources.** ………………………… ……………………………………… ……………………………………… ……………………………………… ……………………………………… ………………………………………	ADM(IM)/ COS(IM)	ADM(IM)/COS(IM) ……………… ………………………………………… ………………………………………… ………………………………………… ………………………………………… ………………………………………… ………………………………………… ………………………………………… ………………………………………… …………………… Resource requirements will be identified in the proposed plan.	31 Oct 07

ANNEX B—SAMPLE SYSTEMS FOR C&A FILE REVIEW

System Name	Accreditation Type	Status (23 April 2007)	Expired for more than one year?
Systems accredited with the capability to process classified information			
Classified Network (CNet)	…….	…….	…….
TITAN	…….	…….	…….
SPARTAN	…….	…….	…….
Defence Video Conference Network (DVCN)	…….	…….	…….
STONEGHOST	…….	…….	…….
GRIFFIN	…….	…….	…….
Canadian Forces Network Operations Centre (CFNOC) Facility	…….	…….	…….
Canadian Forces Experimental Network (CFXNet)	…….	…….	…….
Synthetic Environment Research Facility Local Area Network (SERF LAN)	…….	…….	…….
Systems accredited that do not have capabilities to process classified information			
BlackBerry System	…….	…….	…….
Canadian Forces Health Information System (CFHIS)	…….	…….	…….
Canadian Forces Supply System (CFSS)	…….	…….	…….
Revised Pay System for the Reserves (RPSR)	…….	…….	…….
Claims-X (web application)	…….	…….	…….
Defence Wide Area Network (DWAN)	…….	…….	…….
Financial Managerial Accounting System (FMAS)	…….	…….	…….
Materiel Acquisition and Support Information System (MASIS)	…….	…….	…….
e-Recruiting	…….	…….	…….
General Purpose Network (GPNet)	…….	…….	…….
Human Resources Management System (HRMS)	…….	…….	…….

ANNEX C—C&A FILE REVIEW RESULTS

Systems Operating with a Formal Accreditation														
System	Concept of Operations	Statement of Sensitivity	System Description	Block Diagram	Threat and Risk Assessment	EMSEC Zoning*	Tempest Testing*	Technical COMSEC Inspection Report*	IS Security Survey/ Checklist	System-specific Security Policy & Orders	C&A Plan	Communications Requirement Request	Material Authorization Change Request	System-specific Security Requirements Statement
Synthetic Environment Research Facility Local Area Network	……..	……..	……..	……..… …..	……..	……..	……..	……..	……..	……..	…….	……..	……..	……..
Canadian Forces Experimental Network	……..	……..	……..	……..	……..	……..	……..	……..	……..	……..	…….	……..	……..,	……..
Canadian Forces Network Operations Centre Facility	……..	……..	……..	……..	……..	……..	……..	……..	……..	……..	…….	……..	……..	……..
Human Resources Management System	……..	……..	……..	……..	……..	……..	……..	……..	……..	……..	…….	……..	……..	……..
General Purpose Network	……..	……..	……..	……..	……..	……..	……..	……..	……..	……..	…….	……..	……..	……..

Legend
***** – Required for systems capable of processing classified information
Red – documentation not on file
Yellow – documentation on file was considered to be too old relative to accreditation date (≥ 1 year) or were draft versions
Green – documentation on file and relevant
NR – not required according to NDSI 70

ANNEX C

Systems Operating with an IAP								
System	Concept of Operations	Statement of Sensitivity	System Description	Block Diagram	Threat and Risk Assessment	EMSEC Zoning*	Tempest Testing*	Technical COMSEC Inspection Report*
Canadian Forces Health Information System	.....	.....	.....	.....	.....	.....	.....	.....
BlackBerry System	.....	.....	.....	.....	.....	.....	.....	.....
GRIFFIN	.....	.....	.....	.....	.....	.....	.....	.....
SPARTAN	.....	.....	.....	.....	.....	.....	.....	.....
Revised Pay System for the Reserves	.....	.....	.....	.....	.....	.....	.....	.....
Claims-X	.....	.....	.....	.....	.....	.....	.....	.....
Defence Video Conferencing Network	.....	.....	.....	.....	.....	.....	.....	.....
Defence Wide Area Network	.....	.....	.....	.....	.....	.....	.....	.....
STONEGHOST	.....	.....	.....	.....	.....	.....	.....	.....
Materiel Acquisition and Support Information System	.....	.....	.....	.....	.....	.....	.....	.....
Classified Network	.....	.....	.....	.....	.....	.....	.....	.....
TITAN	.....	.....	.....	.....	.....	.....	.....	.....
Canadian Forces Supply System	.....	.....	.....	.....	.....	.....	.....	.....
e-Recruiting	.....	.....	.....	.....	.....	.....	.....	.....
Financial Managerial Accounting System	.....	.....	.....	.....	.....	.....	.....	.....

Legend
***** – Required for systems capable of processing classified information
Red – documentation not on file
Yellow – documentation on file was considered to be too old relative to accreditation date (≥ 1 year) or were draft versions
Green – documentation on file and relevant
NR – not required according to NDSI 70