Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

HIGH ASSURANCE PRODUCTS AND SERVICES PROGRAM EVALUATION (PAA 2.1.1)

Final Report

DGAEE

2011/12

CERRID 868791

Canada

Evaluation in Brief

Introduction

s.15(1)

This report provides the results of an evaluation that was conducted between July 2011 and January 2012 using DGAEE internal resources. The report consists of two parts:

- This section, the 'Evaluation in Brief' summarizes the evaluation's objectives, methodology, context and results. It also offers recommendations that stem from the evaluation findings. The ensuing Management Action Plan will be tabled in the Final Report, pending the Audit and Evaluation Committee's review.

- The second section offers a more detailed description of the methodology used during the evaluation, the results that ensued and the analysis that led the Evaluation Team to their conclusions.

Objectives

The objective of this evaluation was to ensure that CSEC's High Assurance Products and Services Program (HA Program) remains relevant, efficient and effective, and is achieving expected outcomes.

Methodology

This evaluation used the following data collection methods:

- review of relevant CSEC documentation including COMSEC doctrine, policies, guidelines, web-sites, PeopleSoft data and financial data;
- interviews with seven HA program managers, as well as the supervisor in ATA Director Director ATA and the DG Cyber Protection; and
- interviews with key contacts from the following Internal Services (as per the Program Activity Architecture (PAA)):
  - → 3.2.3 Translation and Printing
  - → 3.4.2 Employee Acquisition & Orientation
  - → 3.7.1 Distributed Computing
  - → 3.7.2 Application/Data Development
  - → 3.7.3 Production and Operations Computing
  - → 3.8.1 Real Property and Operations Management
  - → 3.10.1 Services Acquisitions
  - → 3.10.2 Goods Acquisitions

Context

As the National COMSEC Authority, CSEC manages the HA Program, which provides products and services for the protection of classified or very sensitive Government of Canada (GC) information. These high assurance products are referred to as Type 1 or High-Grade products and are not generally publicly available.

In order to ensure that the HA Program deliverables are widely available to CSEC clients, a variety of activities are undertaken. The following describes the HA Program's main activities which were the focus of this evaluation:

- Providing generic guidance to ensure HA specifications and standards for devices and solutions are suitable for use by the GC and Canadian Forces (CF). This guidance includes the provision of services required to acquire and manage High-Grade or Type-1 products within Canada; and, producing directives and guidance to instruct all departments on how to integrate and use high assurance products within their IT environment to protect their most sensitive information.

- Providing tailored guidance directly to specific GC departments or agencies to assist with their high assurance security needs such as architecture/design, integration of devices for very tailored use, or special projects for their business needs.

- Providing cryptographic key material and COMSEC support services to GC departments to ensure the proper encryption and interoperability of high assurance devices.

- Evaluating and approving High Assurance cryptographic products and key management systems.

Evaluation Results

Overview:

The HA Program spans four CSEC directorates (Crypto Material Systems and Services Architecture and Technology Assurance (ATA), Crypto Modernization Program and ITS Program Management and Oversight (PMO)). Activities are spread over seven management teams.

Key Conclusions:

Relevance:

CSEC's HA Program has had a long standing presence within the information protection arena. As the sole provider of high assurance products and services to GC departments and agencies, its foundation is firmly rooted in legislation, government policy and part B of CSEC's mandate. Looking forward, this is unlikely to change. However, the focus of the HA Program will have to keep in stride with new methodologies stemming from the United States.

Performance:

The governance and coordination framework underpinning the HA Program, both internally and externally, demonstrates a solid oversight and communications capability. However, the Cross Domain Solutions (CDS) unit appeared orphaned from these structures as there was no active participation in the numerous internal working groups and its services were not listed within the *Cyber Protection CSEC-approved High Assurance Products, Systems and Services Product and Service Catalogue.*

There are a number of output metrics captured and reported for the HA Program; metrics that primarily measure the pulse of the operations but they are not yet advanced enough to influence more strategic decision making. There are however, plans in place to implement more strategically focused metrics that are expected to measure the impact the HA products and services are having on Canada's security posture. Of note, both the IT Learning Centre and the COMSEC have made active use of their data and they are proactively informing the policy and doctrine areas on issues that impact these operations. This is regarded as a best practice.

Group has responded to various client service concerns and implemented solutions that address issues related to centralized client assistance and the dissemination of information. Formal processes such as training, inspecting and 'Approval for Use' enable the tracking of COMSEC and High Assurance Products and Services clients. Both formal and informal processes are in place to solicit client feedback on an on-going basis.

The Business Continuity Plan (BCP) for the HA Program has evolved from a paper-based exercise to a plan that is expected to achieve an 'up and running' response time of between 24-48 hours post incident.

It was widely recognized that the health of CSEC's 5-Eyes partnerships was a key consideration in the success of the HA Program. Both formal and informal partner interaction processes are in place to help nurture these relationships. The HA Program is making use of CSEC's Integree program.

The CDS is unique as it straddles both the High Assurance and COTs solutions within the Cyber Protection Directorate. As such, it deserves attention to ensure that it receives appropriate governance.

The financial model that the HA Program follows makes maximum use of high assurance cryptographic, key management and CDS products from the United States Government (USG), resulting in significant cost savings. The number of resources within the HA Program has remained relatively stable compared to the population of IT Security and CSEC wide. Over the last few years, budgets demonstrate consistency in spending both with respect to Capital and O&M. The HA Program Directors and Managers pointed to processes that demonstrate consideration for resource utilization, organizational restructuring efficiencies and opportunities for product and services devolution. Although collectively these do not provide for a complete review of cost effectiveness, the practices reviewed demonstrate adherence to principles related to positive stewardship and accountability.

Internal Services

The HA Program managers identified the Internal Services (IS) that were of most importance to the success of their operations. A number of those services were included as part of the evaluation. The principal concerns expressed by the managers included difficulty accessing process and procedural information related to the delivery of a service, long lead and wait times, as well as the continuous interruption of services as a result of the CIO's transition to the Mid Term Accommodations (MTA).

The evaluation examined these concerns and focused on: IS prioritization processes, the availability and accessibility of policy, process and procedural information, how metrics were used to inform decision making, key constraints in delivering client services specific to the HA Program as well as in general, and initiatives in place that address CSEC-wide client service improvements.

The IS providers were able to identify documented approaches to setting client priorities; however, the HA Program managers had concerns about client service management. Despite an established process for Business Planning, the content within these plans appeared to be insufficient to enable IS providers to plan for and support client requirements in an optimal manner. Details about roles and responsibilities regarding certain content within the *Business Plan template* also seemed lacking (e.g. who is responsible for IT maintenance, etc.).

Although there is information about IS on the web, more proactive measures to increase awareness of this material from each of the service providers would be beneficial.

Although no formal measures to obtain client feedback were in place for any of the service providers interviewed, informal practices are enabling these areas to 'keep a pulse' on their operations. Each of the service providers would benefit from more structured client feedback processes.

The IS providers who were interviewed were making use of the data available to them to help anticipate, plan and prioritize client requirements. Most of this data came from the Action Request System (ARS). Internal Service providers not using ARS should explore opportunities to do so.

IS providers pointed to a number of constraints including:

- Staff shortages interfering with many of the internal services interviewed (e.g. CIO, AMG), most as a result of the affected staff within Corporate Services and the CIO. (However, strategies are being implemented to meet current and future client requirements).

- Details in the business plan do not permit proactive planning on the part of the service providers.

- More up front quality control on the part of clients would facilitate the timely return of jobs sent to the print shop and Linguistic Services.

Although a number of initiatives are underway to improve client services, they mostly reflect plans as opposed to implementable actions. Internal service providers would benefit from metrics that measure the impact they are having on operations.

Recommendations

- Strategic Planning and Modern Management (SPMM) should:

    - identify ways to improve the Business Planning process to enable more effective and integrated use of its contents by Internal Service Providers; and,

    - lead an initiative that will enable Internal Service providers to measure the impact their services are having on operations.

Management Action Plan

During FY 2012/2013 SPMM will lead a review of the business planning process throughout CSEC with the intent of identifying gaps in planning and best practices and recommending standardized practices for business planning to integrate corporate and activity based planning.

While noted improvements can be made throughout FY 2012/2013, the most significant changes will be made in FY 2013/2014 as approved recommendations are implemented.

Through the Performance Measurement Framework Working Group, SPMM is leading the coordination of performance measures across CSEC. By providing guidance on interpreting TBS policies and managing the overall CSEC PMF, SPMM will work with the operational activity areas and internal service providers to establish performance measures that reflect horizontal impacts on each other's activities.

The initial PMF will be submitted to TBS for review and observations by 31 August 2012. Performance indicators will be reviewed in consideration of TBS comments, submitted for ExCom approval and submitted to TBS as the CSEC PMF of record by 31 December 2012.

Report Status

This report, including its Management Action Plan, was approved by the Audit and Evaluation Committee effective 6 July 2012. The evaluation is concluded.

s.15(1)

FORWARD

The evaluation work reflected in this report was conducted consistent with the policies and practices directed by the Treasury Board of Canada Secretariat for Evaluations within the Government of Canada.

DOCUMENT REVISION HISTORY

Version	CERRID	Reviewer	Changes	Date	Approval
Office Draft	868791	DAE	Editorial & Quality Review	19 Dec 11	
Clearance Draft	868791	DG Finance, DG CP.	Editorial and addition of the MAP	30 Mar 12	
Discussion Draft	868791	A&E Com	Review IT Security recommendations	19 Apr 12	DGAEE
Draft Disc V2	868791	A&E Com	Revised recommendations and MAP	11 Jun 12	DGAEE
Final Report	868791	A&E Com	Report Approved	6 Jul 12	A&E Com

For information about this report contact:
Director General, Audit, Evaluation and Ethics
Communications Security Establishment Canada
PO Box 9703, Terminal
Ottawa, Ontario K1G 3Z4

TABLE OF CONTENTS:

1.0 PROGRAM BACKGROUND

1.1 Context

Part B of CSEC's legislated mandate is to help ensure the protection of electronic information and information systems that are of importance to the Government of Canada (GC). To meet this objective, CSEC's new Program Activity Architecture (PAA), describes two programs within IT Security: Cyber Protection (PAA 2.1) and Cyber Defence (PAA 2.2). The focus of the Cyber Defence function is to identify, detect and mitigate actual and potential threats and vulnerabilities of GC communications security and its associated architecture and infrastructure. The Cyber Protection activities help protect GC information networks and systems by providing advice, guidance and support on IT security practices and techniques, and on the secure use of commercially available computer and networking products and specialised cryptographic products within the GC IT environment.

Within the Cyber Protection function, CSEC has developed two major business lines:

- CSEC-approved High Assurance Products and Services (PAA 2.1.1) (HA Program);[1] and
- CSEC Security Guidance for Commercial Products, Systems and Services (PAA 2.1.2).

This report focuses on PAA 2.1.1: HA Program business line within the Cyber Protection Branch.

As the National Communications Security (COMSEC) Authority, CSEC manages the HA Program, which provides products and services for the protection of classified or very sensitive GC information. These high assurance products are referred to as Type 1 or High-Grade and although commercially produced, are not generally publicly available.

In order to ensure that the HA Program deliverables are widely available to CSEC clients, a variety of activities are undertaken. The following describes the main activities which were the focus of this evaluation:[2]

- Providing generic guidance to ensure High Assurance (HA) specifications and standards for devices and solutions are suitable for use by the GC and Canadian Forces (CF). This guidance includes the provision of services required to acquire and manage High-Grade or Type-1 products within Canada; and, producing directives and guidance to instruct all departments on how to integrate and use high assurance products within their IT environment to protect their most sensitive information.

- Providing tailored guidance directly to specific GC departments or agencies to assist with their high assurance security needs such as architecture/design, integration of devices for very tailored use, or special projects for their business needs.

- Providing cryptographic key material and COMSEC support services to departments to ensure the proper encryption and interoperability of high assurance devices.

- Evaluating and approving HA cryptographic products and key management systems.

[1] Provides product, architectural and engineering advice, guidance and support to the GC to protect its information and communications using commercially available IT Security products, systems and services.
[2] Refer to Annex A: High Assurance Program Logic Model

2.0 ABOUT THE EVALUATION

2.1 Evaluation Objectives

Recent Treasury Board of Canada Secretariat (TBS) policy directs departments to evaluate the Value-for-Money (VFM) of all programs. The definition of VFM adopted by TBS has two components: performance of programs and relevance. The performance of a program is defined as the extent to which effectiveness, efficiency and economy are achieved, while the incorporation of relevance into the assessment of VFM allows for conclusions on performance that are better contextualized.

The objective of this evaluation was to ensure that CSEC's HA Program remains relevant, efficient and effective, and that it is achieving expected outcomes.

2.2 Lines of Inquiry

The following lines of inquiry guided the collection and analysis of evidence used during this evaluation to support conclusions regarding the relevance and performance of the HA Program:

- continued need for the program and its responsiveness to the needs of Canadians (via meeting the needs of GC Departments) *(Relevance)*;
- alignment with government priorities, and federal roles and responsibilities (including CSEC's mandate) (*Relevance)*;
- achievement of expected outcomes (*Effectiveness)*; and
- demonstration of efficiency and economy.

2.3 Scope

The evaluation focused on the primary activities undertaken by the HA Program (refer to the Logic Model in Annex A). It also examined a number of CSEC's internal services that were identified by the HA Program managers as key to the success of the HA program (refer to Section 4.0).

A substantial part of the HA program is the Canadian Cryptographic Modernization Program (CCMP). This is a Major Crown Project that has been the subject of numerous reviews, including two internal formative evaluations (2008/09), an internal financial framework audit (2008/09), and one independent (external) review (2010/11). Given this relatively extensive oversight, coverage of the CCMP in this evaluation was minimized.

2.4 Methodology (Approach, Instrumentation, Data sources)

This evaluation used the following data collection methods:

- review of relevant CSEC documentation including COMSEC doctrine, policies, guidelines, web-sites, PeopleSoft data and financial data;[3]
- structured interviews with the seven managers in the HA program, as well as the supervisor in ATA [4] Director Director ATA and the DG Cyber Protection; and

[3] Refer to Annex B for a list of references
[4] Refer to Annex F for a list of acronyms for the full titles of the HA Program directorates , management and supervisory groups.

- interviews with representatives from the following Internal Services as per the Program Activity Architecture (PAA):
  - → 3.2.3 Translation and Printing
  - → 3.4.2 Employee Acquisition & Orientation
  - → 3.7.1 Distributed Computing
  - → 3.7.2 Application/Data Development
  - → 3.7.3 Production and Operations Computing
  - → 3.8.1 Real Property and Operations Management
  - → 3.10.1 Services Acquisitions
  - → 3.10.2 Goods Acquisitions

3.0 EVALUATION FINDINGS

3.1 Relevance

Using information obtained from interviews as well as various documents, this section provides an evaluative opinion of the HA Assurance Program's relevance. The following lines of inquiry were used to develop this assessment:

- continued need for the program;
- alignment with Government Priorities; and
- alignment with Federal Roles and Responsibilities.

Continued Need for the Program

Program Origins

An early description of the COMSEC mission under the Communications Branch National Research Council captures many of the current activities of the HA program. The responsibilities described in the 1959 mission statement include:

- review and evaluate crypto principles;
- review, evaluate and formulate crypto security rules, regulations and instructions;
- review and evaluate COMSEC procedures used by any department;
- produce keying material;
- conduct COMSEC research;
- provide technical guidance and support in COMSEC matters; and
- liaise with NSA and GCHQ on technical COMSEC matters.

The capability to perform an independent,[5] in-depth evaluation of cryptographic algorithms and products was established at CSEC in 1974.

Contextual Changes since Inception

The most significant factors which have shaped the evolution of the original COMSEC program into today's High Assurance program are the technologies and environments in which the GC operates. Electronic and computer technologies have seen many-fold increases in complexity, miniaturization and speed. GC systems and networks are upgraded and replaced on a more frequent basis. At the same time, the growth of computer networks along with the growth of the GC itself has greatly increased the amount of classified and sensitive information being communicated, processed and stored. In addition, there is now a need for users to exchange information and collaborate between different security domains, (e.g., unclassified, Secret and Top Secret domains). These changes have impacted the High Assurance program in the following ways:

- the scope has broadened;
- there is a greater need for specialized staff trained in engineering, mathematics and computer science;
- there is an increased demand for HA products and services; and
- there is a greater urgency in the delivery of HA products and services.

Predicted Future Demand

The size of the public service together with the quantity of classified information being communicated, processed and stored is not expected to diminish significantly in the foreseeable future.

[5] Independent of the National Security Agency (NSA) and the Government Communications Headquarters (GCHQ)

Major crown projects requiring IT Security development can place significant demands on the HA Program, but in the past such projects have provided sufficient lead time to be manageable. Examples include the Department of National Defence's (DND) and the Canadian Space Agency's HA Program managers predict that the creation of Shared Services Canada may in the short-term, increase demand for HA Program services.

The CCMP provides a roadmap for how Type 1 products and crypto key management services are evolving. An independent review of the CCMP conducted in May 2011 found that its business case *was current and aligned with the GC and stakeholder priorities in modernizing the Type 1 devices that* protect GC classified information. This indicates that there will be a sustained need for Type 1 crypto and related support services.

Alignment with Government Priorities

CSEC is aligned with the GC Priority: "A Safe and Resilient Canada". The HA Program specifically supports this goal via the delivery of high assurance products and services for the protection of classified or very sensitive GC information.

"Securing Government Systems" is one of the three pillars within the GC's *Cyber Security Strategy for a Stronger and more Prosperous Canada.* Activities within the HA Program are directly related to the strategy's requirement to: "put in place the necessary structures, tools and personnel to meet its obligations for Cyber Security".

In February 2011, the GC unveiled the *Perimeter Security and Economic Competitiveness Action Plan*, in concert with the United States Government. One of the many core initiatives is to: "protect vital government and critical digital infrastructure of bi-national importance, and make cyberspace safer for all citizens."[6] Public Safety Canada will necessarily look to CSEC's HA Program to assist with the delivery of this objective.

Alignment with Federal Roles and Responsibilities

The National Defence Act under paragraph 273.64(1)(b) states that the Communications Security Establishment has the following mandate:

> To provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the GC.

This gives legislative authority for CSEC to provide high assurance services to protect GC classified electronic information. Moreover, CSEC is the sole provider of high assurance products and services to departments and agencies of the GC.

In addition, the *Policy on Government Security* (PGS) contains requirements to ensure that deputy heads effectively manage security activities within their departments and contribute to effective government-wide security management. The PGS states that CSEC provides leadership and coordination for departmental activities that help ensure the protection of electronic information and information systems of importance. CSEC also serves as the government's national authority for SIGINT and COMSEC. The PGS states that CSEC is responsible for the following activities all of which are relevant to the HA Program:

- Developing, based on analysis of community needs and in partnership with TBS, policy instruments related to IT security for approval by TBS.

- Developing, approving and promulgating COMSEC and SIGINT related policy instruments for classified information and developing guidelines and tools related to IT security.

[6] Found on page 28 of the publication.

- Coordinating the development and provision of training and awareness related to IT security, COMSEC and SIGINT to Departmental Security Officers (DSOs), security practitioners and, as required, other authorized individuals.

- Leading IT security-related interdepartmental committees and working groups and facilitating the sharing of information and collaboration across security communities.

- Collecting and reviewing IT security best practices and making recommendations to TBS and security governance committees to facilitate security policy improvements and collaboration among departments.

- Conducting research on IT security methods, technologies or common services and proposing solutions to TBS and governance committees to improve risk management and economies of scale in government.

- Responding to and participating in the investigation or analysis of sophisticated IT security incidents, threats and vulnerabilities and acting on information collected or received from these investigations.

- Providing advice and guidance to departments on the:
  - use and application of IT security products, COMSEC devices, cryptographic measures and key management;
  - certification of shared and common IT services, emerging IT security technologies, ITS architecture design, common ITS solutions, including secure use of commercial-off-the-shelf products, system and network security design and security posture and vulnerability assessments;
  - design and upgrade of GC IT infrastructures and their security interconnectivities;
  - application of IT access controls for confidentiality and integrity as well as threat detection and prevention; and
  - certification of GC shared, common or federated IT services.

- Providing services to departments for:
  - key management systems and related components for classified information;
  - predicting, preventing and defending against sophisticated IT security incidents, threats and vulnerabilities;
  - handling and mitigation of sophisticated IT security incidents;
  - security architecture design for GC shared, common or federated initiatives;
  - IT security product assessment and/or approval for products in use in classified domain when deemed necessary; and
  - tailored engineering and operational support for information infrastructure projects of importance to the GC.

- Gathering, analyzing and facilitating the authorized sharing of consolidated IT security threat and vulnerability information with departments and with Public Safety Canada.

- Representing the GC on national and international initiatives related to IT security and SIGINT.

The Management of Information of Information Standard (MITS) pursuant to the PGS defines baseline security requirements for departments to ensure the security of information and information technology (IT) assets under their control. The following requirements within MITS are related to the HA Program:

s.15(1)
s.16(2)(c)
s.21(1)(a)
s.21(1)(b)
s.21(1)(c)

- Departments must use encryption or other safeguards endorsed or approved by the Communications Security Establishment to protect electronic communications of classified and Protected C information.

- In Canada, departments should use Telecommunications Electronic Material Protected from Emanating Spurious Transmissions (TEMPEST) protection for Top Secret and Protected C information when justified by a Threat and Risk Assessment (TRA). At posts abroad, departments should apply TEMPEST protection to all classified information when justified by a TRA.

- Related to telecommunications cabling, departments should ensure additional protection, such as a for the transmission of Protected C and classified information. When physical security and safeguards are impractical, departments should use encryption or other methods approved by the Communications Security Establishment.

HA Program alignment with CSEC's mandate, strategic vision and IT Security vision

The HA Program directly supports Part B of CSEC's Mandate.

CSEC 2015 outlines the priorities that must be addressed by IT Security and includes the following which directly relate to the HA Program:

-
-

IT Security 2015 provides a strategic direction for the IT Security Program and was written in the context of *CSEC 2015.* The following objectives within *ITS 2015* directly relate to the HA Program:

-
-
-

Looking Forward

As noted from the interviews, the HA Program may have to strategically adjust to align within NSA's Commercial Solutions for Classified (CSFC) program.

Conclusions

CSEC's HA Program has had a long standing presence within the information protection arena. As the sole provider of high assurance products and services to GC departments and agencies, its relevance is firmly rooted in legislation, government policy and part B of CSEC's mandate. Looking forward however, the focus of the HA Program will have to keep in stride with new methodologies stemming from the United States.

[7] NSA's Management Directive No. 101 (*Certification or Approval for Use of Information Assurance Products and Solutions)*
[8] The National Information Assurance Partnership (NIAP) and the Cryptographic Module Validation Program (CMVP)

3.2 Performance

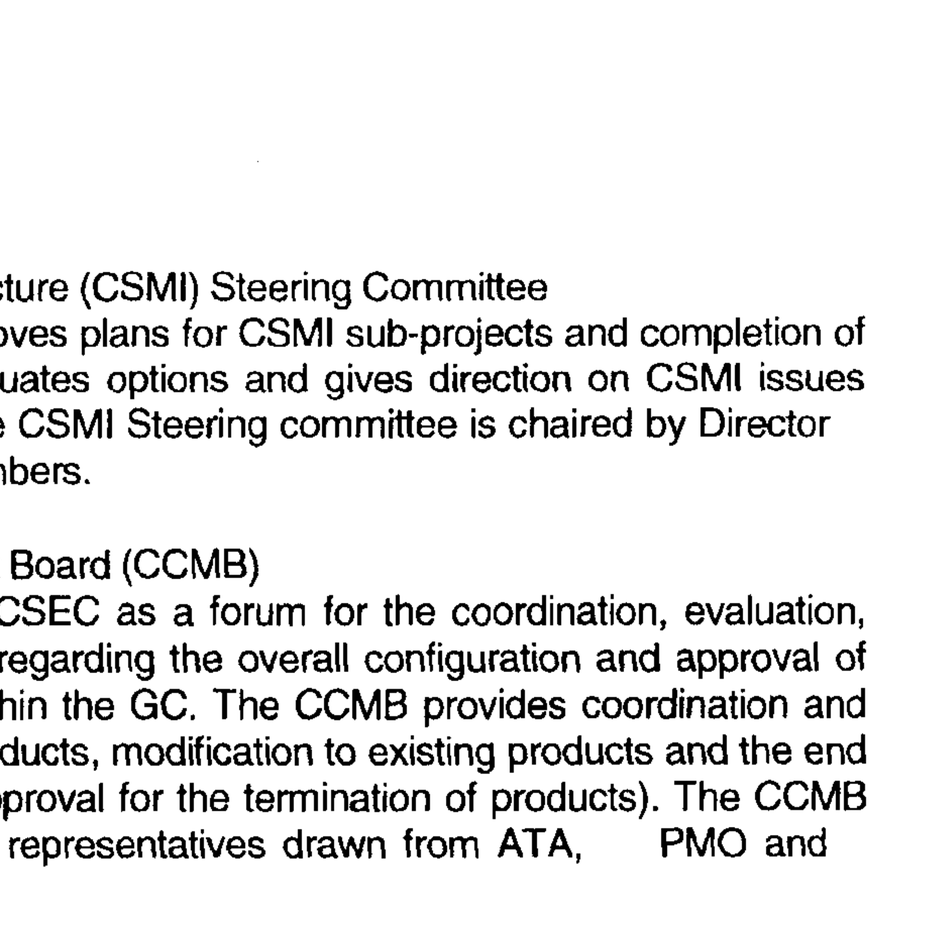
The HA Program's performance was assessed by addressing both operational and cost effectiveness.

3.2.1 Operational Effectiveness

Operational effectiveness examined:

- Governance
- Use of Metrics to Inform Decision Making
- Client Interactions
- Business Continuity Planning
- Partnerships

Figure 1: High Assurance Program: Directorates



3.2.1.1 Governance

The HA Program spans four directorates: (Crypto Material Systems and Services Architecture and Technology Assurance (ATA), Canadian Cryptographic Modernization Program and ITS Program Management and Oversight (PMO)).

Activities are spread over seven management teams. Annex C depicts the distribution of key activities within them.

The COMSEC elements of the HA Program have a Steering Committee, a Management Board and numerous working groups and processes in place to provide a governance and coordination framework.[9]

These include:

Steering Committees/Decision Boards:

- Classified Security Management Infrastructure (CSMI) Steering Committee
  - The CSMI Steering Committee approves plans for CSMI sub-projects and completion of major CSMI milestones. It also evaluates options and gives direction on CSMI issues requiring Director-level approval. The CSMI Steering committee is chaired by Director with Directors and ATA being members.

- Cryptographic Configuration Management Board (CCMB)
  - The CCMB was established within CSEC as a forum for the coordination, evaluation, discussion and resolution of issues regarding the overall configuration and approval of cryptographic products deployed within the GC. The CCMB provides coordination and guidance for the approval of new products, modification to existing products and the end of operational life (removal of the approval for the termination of products). The CCMB membership consists of permanent representatives drawn from ATA, PMO and group.

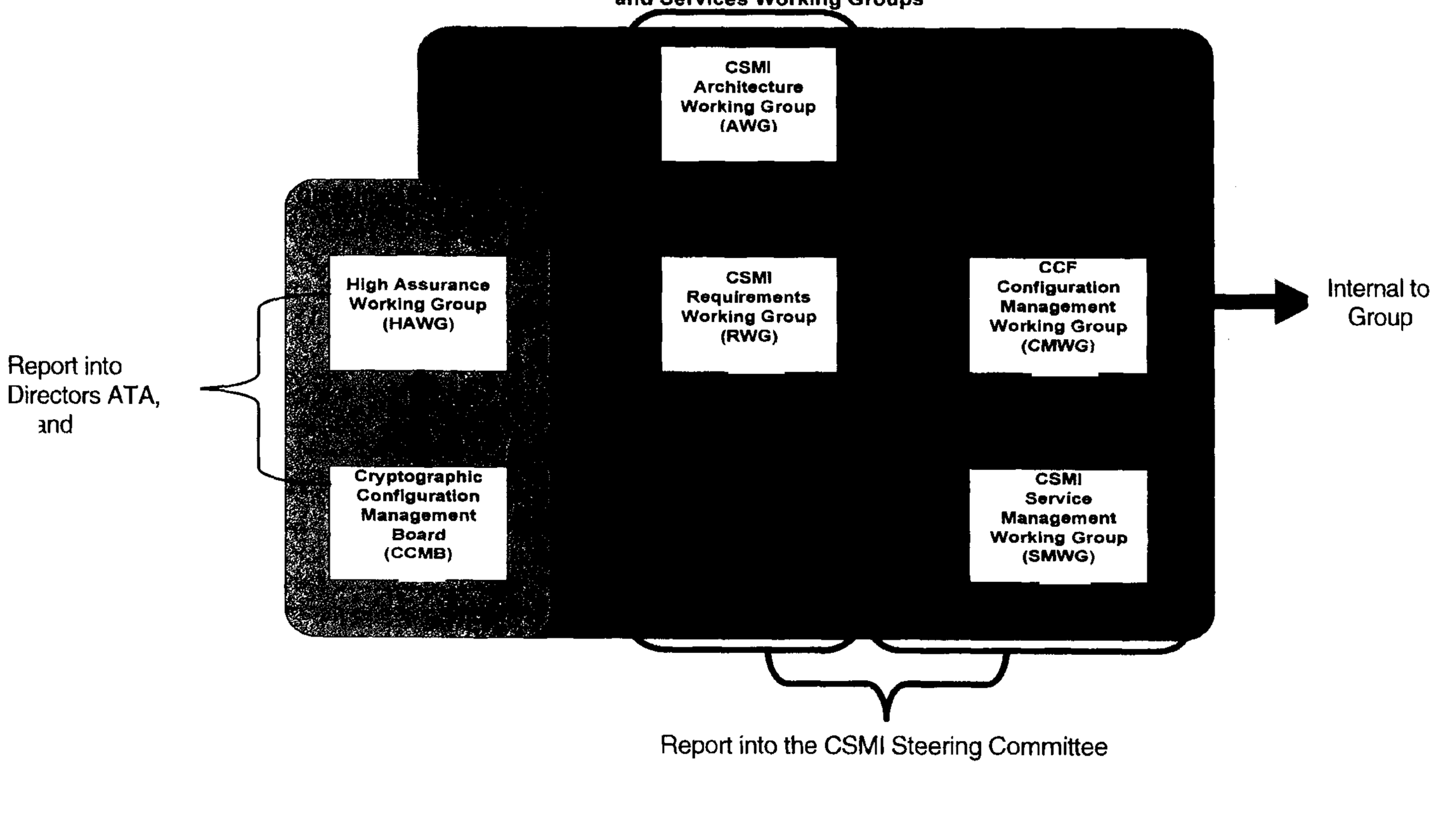
[9] Detailed descriptions can be found in Annex D

Working Groups:

- High Assurance Working Group (HAWG);
- CSMI Requirements Working Group (RWG);
- CSMI Architecture Working Group (AWG);
- Canadian Central Facility (CCF) Configuration Management Working Group (CMWG); and
- CSMI Service Management Working Group (SMWG).

Figure 2 shows interactions between the working groups and the CCMB and Table 1 provides a summary of the focus and membership within each working group:

Figure 2: CSEC Approved High Assurance Products, Systems and Services Working Groups



s.15(1)

Table 1: Summary of Internal Working Groups

Working Group	Focus	Chair	CoChair	Member Groups
CSMI RWG	Provide advice and guidance for business requirements that will continuously improve the service delivered by the CCF to CCSE's GC clients			ATA
CSMI AWG	Provide architectural advice, guidance and decisions in support of the present and future environment of the CSMI.			ATA
CCF CMWG	Provide Configuration Management advice and guidance in support of CCF Development, Test, Staging and Production environments.			ATA
HAWG	Provide advice, guidance and certification recommendations in support of CSMI and IT Security cryptographic programs	ATA-		ATA ATA ATA
CSMI SMWG	Continuously improve the service delivered by the CCF to CCSE's Government of Canada clients			ATA
CSWG	Ensure that client requirements are tracked, communicated, well understood and effectively managed across the program. Ensure that collectively the IT Security Client Service Model is able to effectively respond to client requirements in a coordinated and efficient manner	ATA	Dir	ATA CTEC

In addition to the steering committees, management board and working groups, the HA Program Directors hold weekly meetings with their managers. There is also the Business Development Review Committee (BDRC) monthly meeting within Group which includes managers and supervisors.

External Groups

From an external perspective there are a number of COMSEC forums used to ensure co-ordination of requirements, technical analysis, programmatics and solutions. These include the CCMP Senior Project Advisory Committee (SPAC), the CCMP Inter-Departmental Advisory Committee (IDAC), the CCMP Senior Decision Board (SDB), the COMSEC User's Group (CUG), DND Bilats (Director Information Management Security (Dir IM Security) & Group), IAD Senior's Bi-Lat, the 5-Eyes Key Management Strategy Group (KMSG) and a number of technology (e.g. secure voice and Internet Protocol (IP)) focussed 5-Eyes working groups.

CCMP SPAC: The CCMP SPAC was established to ensure consistent, cohesive and coordinated direction for the CCMP and to ensure that the program continues to meet GC needs. The committee provides oversight for the CCMP IDAC. It is co-chaired by DCITS and DND/ADM (IM). Members include CSEC, CSIS, DFAIT, DND, PCO, PS, PWGSC, RCMP and TBS/CIOB.

CCMP IDAC: The CCMP IDAC is the mechanism for inter-departmental planning and coordination for the CCMP. This committee is co-chaired by Director and DND/Deputy Project Director Defence CMP and its membership includes CSIS, DFAIT, PCO, PWGSC, PS, RCMP and TBS.

CCMP SDB: The CCMP SDB is a joint CSEC/DND board that provides guidance, review and oversight of the funded aspects of the CCMP, particularly with respect to financial agreements between CSEC and DND. The CCMP SDB is chaired by DG ITS Cyber Protection. Membership includes CSEC and DND.

CUG: The CUG is attended by all clients across the GC (40-45 departments that hold COMSEC accounts). The CUG is managed by Group and is a forum for providing COMSEC related information to clients and receiving their feedback. The CUG meets twice a year.

KSMG: The Key Management Strategy Group (KMSG) is a 5-Eyes forum established to ensure consistent key management policies, standards and systems. The KMSG helps ensure that key management systems and cryptography used by Combined Communications Electronics Board (CCEB) nations are interoperable as required.

Observations

The extensive and comprehensive governance and coordination framework described above provides an integrated mechanism for managing operations within the COMSEC element of the HA Program.

Within CSEC, decision-making is conducted via an active steering committee, processes are defined and documented, requirements and activities are coordinated and metrics are captured and reported.

External to CSEC, through forums such as the CUG and departmental bi-lats, GC client needs are coordinated and information on solutions is provided. The HA Program has also established both formal and informal means of coordinating requirements, specifications and solutions with CSEC's 5-Eyes partners.

A review of working group representation at the HA Program supervisory level (e.g. demonstrated good coverage and participation by most units. However, there was one group within the HA Program that remains outside of these working groups and committees: the Cross Domain Solutions (CDS) element within ATA which has only been in existence for a few years. The CDS is unique as it straddles both the High Assurance and COTs solutions within the Cyber Protection Directorate. As such, at the time of the evaluation it was not a member of any HA Program WG and did not have a governance and coordination framework consistent with other HA elements.[10] Reporting, coordination and oversight occurs through line management and requirements are gathered through direct (ad hoc) interaction with client departments. To date, CDS has established informal relationships with CSIS, DFAIT, DND and PCO. It also participates within the 5-Eyes CDS WG.

The Cross Domain Solution (CDS) activities were re-focused in FY 11/12 to support a couple of tactical high-priority GC initiatives, resulting in two solutions that will be used by TBS/Finance to interconnect their segregated and unclassified networks. These solutions are also being considered for the Information Exchange Gateway (IEG) project in SSC. In FY 12/13 the recommendation on use of these solutions will be formalised and communicated under an appropriate process. The current Approval for Use (AFU) process is strictly used for high-assurance product approvals. Because a CDS is almost always composed of one or more commercial and high-assurance products, a new approval processes to address the CDS scenario will be defined. CDS services are not being captured in the Cyber Protection CSEC-approved High Assurance Products, Systems and Services Product and Service Catalogue, therefore many GC departments and agencies may be

[10] The High Assurance working groups referred under this report are all in areas of Cryptography or Key Management and therefore not related to CDS. NSA also has working groups for CDS that are separate from those addressing Cryptography or Key Management issues.

unaware of this business line. However, once these solutions are approved, they could then be included in the High Assurance Product and Service Catalogue.

Conclusions

The governance and coordinated framework underpinning the HA Program, both internally and externally, demonstrates a solid oversight and communications capability. The CDS unit is somewhat orphaned from this framework.

3.2.1.2 Use of Metrics to Inform Decision Making

The HA Program directors and managers were asked to identify the metrics used to inform decision-making.

Within Group, a *COMSEC Operations Report* is published monthly by and is reviewed by the Deputy Chief IT Security. The content speaks to output metrics such as key production, system availability, client interactions, as well as audit and policy related activities. There are also a number of metrics related to 'incident management' which dive a bit deeper and explore service requests specific to products and services within the *Cyber Protection CSEC-approved High Assurance Products, Systems and Services Product and Service Catalogue.*

tracks operational metrics such as the number of builds, failed builds and deployments as well as systems availability and the number of architectural change requests. produces more project related metrics such as monthly status, production, and resource availability reports.

In ATA, there is a Joint Executive Team (JET) Operational Dashboard that is also used by Directors and This includes output metrics such as how many products are approved for use in Canada. Director ATA identified plans for more strategically focused metrics including a measure that will examine the impact of the HA Program on Canada's security posture. There is also discussion ongoing around how to measure the use of HA Products and Services, not just in terms of being 'distributed' but being 'deployed'.

The IT Security Learning Centre tracks multiple metrics such as those related to course registration, number of courses offered, number of courses under development as well as others related to client feedback and revenue generation. These are reported quarterly to Director Project Management Office (PMO).

Of note, 'data of interest' captured by the IT Security Learning Centre and the COMSEC such as errors in doctrine identified during training or areas of non-compliance found during COMSEC are shared with the COMSEC doctrine and policy writers. This enables an ongoing refresh of the COMSEC documents and essentially has established an 'auto correct' process.

Conclusions

There are a number of output metrics captured and reported for the HA Program but they are focused on measuring the pulse of the operation vice influencing more strategic decision-making. Both the IT Learning Centre and the COMSEC are proactively informing the policy and doctrine areas on issues that impact these operations.

3.2.1.3 Client Interactions

COMSEC Clients

The majority of CSEC's COMSEC clients represent GC departments and agencies (i.e. there are roughly GC clients holding COMSEC accounts). In addition, interacts with a small number of private industries (between accounts). The Department of National Defence is notably CSEC's largest COMSEC client followed by CSEC, CSIS, the RCMP and PWGSC.

COMSEC account holders must take the mandatory training offered exclusively through the IT Security Learning Centre and all account holders are subject to periodic verifications. Both requirements keep active clients within CSEC's 'radar'.

The 2009 *CCMP Client Satisfaction Survey*[11] identified the absence of a 'centralized source of client assistance' and the 'lack of a mechanism to formally record client interactions' as the key issues put forward by the COMSEC custodians surveyed.

Similarly, a *Strengths, Weaknesses, Opportunities and Threat Analysis* (SWOT) conducted by also recognized the lack of a 'holistic approach' to client services and the presence of client silos within CSEC. The following table highlights initiatives that have been implemented to address these concerns:

Table 2: Initiatives Implemented to Address Client Concerns

Opportunity	Initiative Undertaken
Establish service standards & corresponding metrics / reporting	2011 roll out of the *Cyber Protection CSEC-approved High Assurance Products, Systems and Services Product and Service Catalogue.*
Enhance COMSEC community support through re-establishment of regular user group meetings	The CUG is a working group attended by all clients across the GC (departments that hold COMSEC accounts). The CUG is managed by Group and is a forum for providing COMSEC related information to clients and receiving their feedback. The CUG meets twice a year. (Replaced the HUG and STUG) *Internally:* • The Service Management Working Group is in place to ensure consistency in response and service to clients (Pan HA Program) • A new COMSEC Working Group has been stood up to improve situational awareness between and
Use CSEC's web presence as an effective COMSEC information dissemination tool	The COMSEC Use Portal was made accessible to GC COMSEC personnel in the Spring of 2011.

[11] Conducted by the Directorate of Audit and Evaluation

Tailored Guidance Clients

s the primary interface for GC clients seeking guidance and advice on HA products and services. While CSEC's *Approval for Use* process helps keep track of active clients, most client interactions are via informal processes. Recently, more proactive (informal) attempts to seek client engagement have been realized, specifically through attendance at conferences such as the Government Technical Electronics Conference (GTEC) where HA Program staff maintained a booth, thus hearing first hand from some of their clients.

Conclusions

The COMSEC program has responded to various feedback and implemented solutions to address concerns around centralized client assistance and the dissemination of information (e.g. training, auditing and 'Approval for Use') Both formal and informal processes are in place to solicit client feedback on an on-going basis.

3.2.1.4 Business Continuity Planning

As the sole provider of COMSEC products to the GC, it is critical that components of the HA Program continue to function in the event of an emergency. To that end, understanding the status of the HA Program's Business Continuity Planning (BCP) was included in the evaluation.

For Group, BCP is coordinated by It was indicated that their BCP status had evolved from an 'inventory on paper' to a capability to resume services within 24-48 hours post-incident. Within Group, 'mission critical' roles have been identified and the first year of a two year test plan has been initiated. This information was validated with CSEC's Emergency Management Office.

Conclusions

The BCP for the HA Program has evolved from a paper-based exercise to a plan that is expected to resume key services within 24 to 48 hours post incident.

3.2.1.5 Partnerships

Membership within the 5-Eyes provides CSEC with access to a cryptologic infrastructure.[12] As a result, sustaining relationships with these partners is important. The evaluation sought to determine the initiatives that were in place to maintain the 'health' of these relationships.

Both HA Program Directors spoke of focussed bi-lateral exchanges with their allied counterparts. In addition, at the working level, there are numerous interactions between various 'communities of interest', for example the crypto mathematicians. The HA Program is also making use of the Integree Program and at the time of the evaluation one integree was about to be deployed to NSA.

Conclusions

It was widely recognized that the health of CSEC's 5-Eyes partnership was a key contributor to the success of the HA Program. Both formal and informal partner interaction processes are in place to help nurture these relationships.

[12] CSEC 2nd Party Strategy.

3.2.2 Cost Effectiveness

Cost effectiveness was examined by reviewing , ATA (former and PMO budgets, and and ATA demographics as well as through discussion with the two HA Program directors and managers regarding program management and utilization of resources.

3.2.2.1 Access to 5-Eyes High Assurance Products and Services

The HA Program makes maximum use of high assurance cryptographic, key management and CDS products from the United States Government (USG). Canadian-unique components are only considered when the required functionality is not available from the USG or CSEC's other 5-Eyes partners. This approach enables Canada to take advantage of the immense investment made by the USG in research and development. It is an affordable and flexible approach, and enables various strategies to be used for each HA component on a case-by-case basis. The down side is the risk resulting from the associated dependency on the USG. This model's cost effectiveness was recognized implicitly by Treasury Board in their approval of the CCMP.

3.2.2.2 Budget

Table 3 provides a snapshot of the number of Full Time Equivalents (FTE)'s within ATA, PMO and Groups as well as FY10/11 O&M and Capital expenditures. The FTE data is based on information derived from PeopleSoft as reviewed against SWE data in FAMIS.

Table 3: HA Program FTE and Budget Profile

FTE Estimates & Budget Expenditures	
ATA*	
PMO	
Totals+	

* Based on FTE
& Not exclusively HA, adjusted; does not make allowance for cost recovery
+ excludes

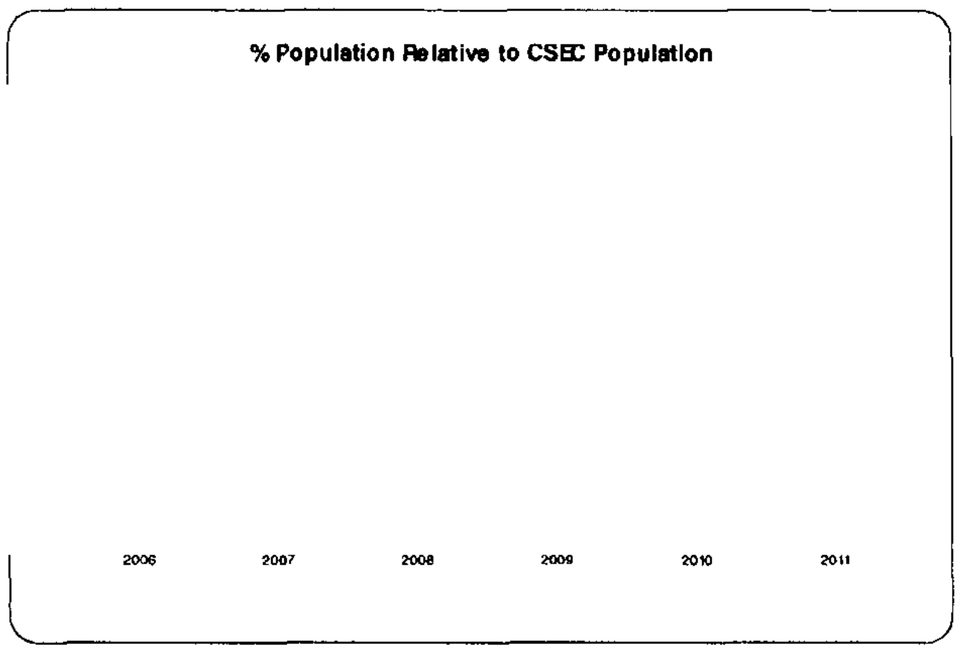
The FY10/11 capital expenditures for ATA and Group are consistent with spending patterns reviewed for FY09/10 and FY08/09. They include purchases related to lab equipment, specialized equipment, storage, network and server components.

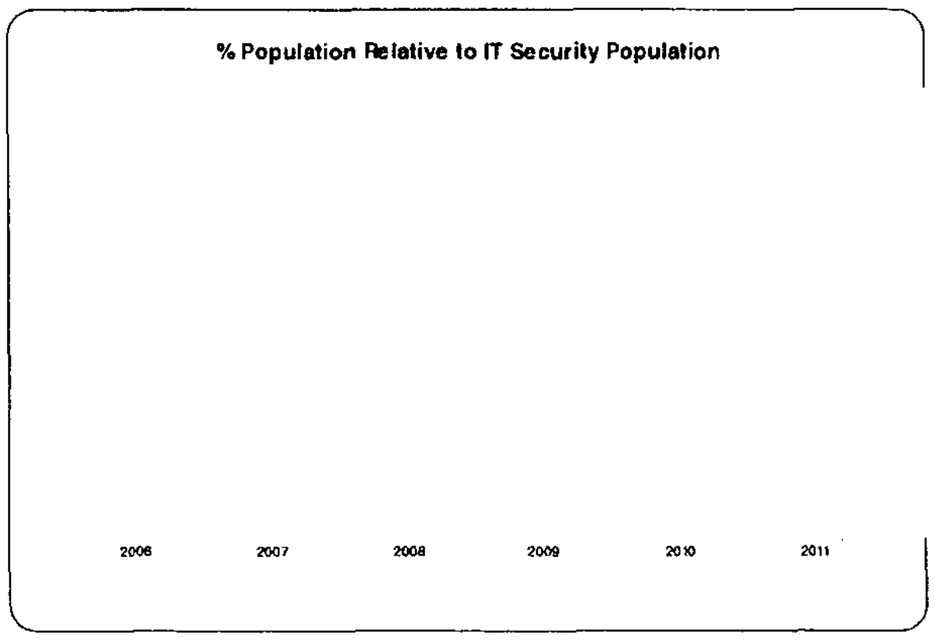
O&M expenditures were also consistent with spending patterns reviewed for the same period. Approximately 45% of the FY10/11 total was allocated to professional services. Of note, professional services account for roughly 80% of O&M expenses. Other expenses included travel, training, conference and workshops as well as software maintenance and support contracts.
is funded via and accounts for 65% of Group's O&M.

Each directorate makes use of consultants to address gaps in operations; a review of the roles and deliverables of these consultants demonstrated that some are also filling administrative gaps such as coordinating meetings and taking minutes. There are opportunities for HA Program managers to revisit how their consultants could be most effectively utilized.

3.2.2.3 Demographics

A review of ATA and Group populations over time demonstrated relative consistency in size as a percentage of IT Security and CSEC, in general.





3.2.2.4 Management and Utilization of Resources

The managers and directors were asked 'what processes had been established to ensure that the HA Program was operating within allocated resources'. Each pointed to the Business Planning process as one method used to determine the efficient use of resources. There are also mid-year resource allocation discussions between the directors and their managers. Director indicated that a bi-weekly meeting with an HR specialist occurs to ensure vacancies are addressed and to inform on the status of on-going competitions.

IT Security in general has undergone a number of reorganizations within the last few years that has resulted in a clearer separation between the Cyber Defence and Cyber Protection portfolios. Within Cyber Protection, a number of adjustments have been made to structure around specific functions such as client services, evaluations, and testing.

3.2.2.5 Outsourcing and Program Termination

Opportunities to outsource HA Program activities are generally not possible due to international agreements, such as International Traffic & Arms Regulations (ITAR), as well as other sovereign requirements.

As part of the CSMI strategy, the decommissioning of a number of products and services are being addressed including the sun-setting of the Electronic Key Management System (EKMS). This effort is also focusing on re-training requirements and HA Program managers are already undertaking a number of skills gap analysis exercises. In addition, under the auspices of the CCMP, a number of products have been discontinued including the STUIII and Key Tape 'Canister' Production.

Conclusions

The HA Program makes maximum use of high assurance cryptographic, key management and CDS products from the USG. The resources within the HA Program have remained relatively consistent over the last three fiscal years; where they have increased, the growth has mirrored the growth in IT Security and CSEC as a whole. The HA Program directors and managers can point to processes that

demonstrate consideration for resource utilization, organizational restructuring efficiencies and opportunities for product and services devolution. Although collectively these do not provide for a complete review of cost effectiveness, the practices reviewed demonstrate adherence to principles related to positive stewardship and accountability.

s.15(1)

4.0 INTERNAL SERVICES

The seven HA Program managers were asked which of CSEC's PAA Internal Services were of most importance to the success of their operations. The following chart illustrates their responses:

Internal Services Category		PMO	ATA	ATA			
3.2.2 Multi-Media Services							
3.2.3 Translation and Printing							
3.4.2 Employee Acquisition & Orientation							
3.5.1 Financial Planning and Budgeting							
3.5.2 Accounting Management							
3.5.4 Payment Services							
3.5.5 Collections and Receivables							
3.6 Information Management							
3.7.1 Distributed Computing							
3.7.3 Production and Operations Computing							
3.8.1 Real Property and Operations							
3.10.1 Service Acquisition							
3.10.2 Goods Acquisition							

Interviews were held with key representatives from most of these services.[13] Those interviews explored: client service management (including business processes, communications and feedback strategies, as well as the use of metrics), and constraints impacting their ability to deliver services and initiatives underway to improve or enhance existing processes. Where there was a particular issue or gap identified by an HA Program manager, questions specific to the issue were also addressed.

The following sections will outline the issues identified by the HA Program managers and the corresponding responses of the Internal Service Providers. The information is presented as follows:

- issues concerning client service management;
- service inhibitors; and
- continuous improvement initiatives.

4.1 Client Service Management

To understand how the selected Internal Service (IS) providers managed their client services, the evaluation focused on the following questions:

- *How are client requests prioritized?*
- *What processes and communication strategies are used to assist clients with accessing your services?*
- *What metrics are kept to inform decision making?*
- *What pressures or constraints are impacting your ability to deliver services?*
- *What, if any, process improvements are underway to address these or other concerns?*

[13] Due to recent or pending audits, the Financial and Information Management groups were not included.

4.1.1 Setting Priorities

One of the concerns most frequently cited by the HA Program managers related to a lack of understanding around how IS providers set client priorities. For the most part, the HA Program managers articulated frustration with long lead times and slow turn around.

Most of the IS reviewed had processes in place to set client priorities. These processes were documented and most were available on the web.[14] Service providers indicated that a lot of 'back door' attempts were often made to by-pass these processes. For example, rather than consult the literature available on the web, managers had a tendency to call someone they knew for information. This may be the result of there being a lot of outdated and inaccurate information published on the web.

Within the CIO, there is a Data Centre Working Group that both sets and manages client priorities. For infrastructure support, the CIO does not use a first-in/first-out method; rather, they use an incident warning system, priorities are then assigned based on the assessed severity of the problem.

None of the IS providers interviewed identified the *Business Plans* as an aid to their planning processes. For example, representatives from the CIO said that there was an inherent error in the way business lines budgeted for their IT service needs as their planning only designated the material requirements. Consequently, the services that would be required to support and maintain this equipment are not addressed. This may be indicative of a lack of understanding of who ultimately bears these related expenses.

The differing governance and oversight processes within each of the business lines appear to contribute to a variety of approaches and expectations with respect to interactions with service providers. For example, within the CIO there is a centralized unit that organizes requirements CIO-wide. In IT Security, there is a more distributed approach which some of the IS providers felt positioned different IT Security units against one another.

Conclusions

Although the IS providers were able to identify documented approaches to setting client priorities, the HA Program managers had concerns about how the IS providers manage their client services. Despite an established Business Planning process, the content within these plans appeared to be insufficient to enable service providers to plan for and support client requirements in an optimal manner. Lifecycle management is not properly considered in the business planning process, according to the IS providers.

4.1.2 Client Communication and Feedback

For the most part, the HA Program Managers indicated they felt ill informed on certain processes, particularly those pertaining to procurement. A recent joint MLN/SLN reinforced this position and noted the need for 'procurement 101' as a top priority. The procurement officer interviewed acknowledged that there is a shortfall in both information/guidance and training in procurement.
As mentioned in section 4.1.1, most information pertaining to CSEC's various internal services is available on the web. However, none of the service providers interviewed identified a *proactive* approach to ensuring that these services and processes are readily available and sufficient to meet the client's needs.

None of the service providers interviewed identified any formal methods of obtaining client feedback. However, a number of informal methods were mentioned including reviewing data stored in the Action

[14] Refer to Annex E for more details.

Request System (ARS), the use of Client Service Representatives and information gathered from day to day interactions with clients.

For the most part, the IS representatives interviewed indicated that they did not have the resources required to implement any formal methodology; as most felt they were stretched delivering on routine client requests.

Conclusions

Although there is information on internal services published on the web, more proactive measures to increase awareness of this material from each of the service providers would be beneficial to ensure it is helpful to their clients.
There are no formal measures in place to obtain client feedback by any of the service providers interviewed, however, informal practices are enabling these areas to 'keep a pulse' on their own operations.

4.1.3 Use of Metrics to inform Decision Making

Most of the service providers interviewed identified operational metrics that were used to inform decision making. For example, those using ARS (CIO, Procurement, Real Property, Translations, and Print Shop) had access to information through that system to track such things as the frequency of a problem and client usage of certain services.

The print shop occasionally outsources some of their work which provides them with benchmark data. This information has been used to inform management on how well the print shop is doing relative to industry and to provide evidence that that they provide good value for money. They are currently planning to use this data to support a business case for another resource

A number of operational metrics are kept by the CIO including readings on power, storage and cooling. Others include number of dropped calls, queue sizes, server utilization, and network lag time.

Conclusions

Those interviewed were making use of the data available to them to help anticipate, plan and prioritize client requirements. Most of this data came from ARS. Internal Service providers not using ARS should explore opportunities to do so.
The Internal Service providers are not able to use their clients' business plans to prioritize and plan work expected of them to effectively support operations.

Recommendation:
Strategic Planning and Modern Management should identify ways to improve the Business Planning process to enable more effective and integrated use of its contents by Internal Service Providers.

4.2 Service Inhibitors

Most of the IS providers interviewed were well aware of the client service concerns articulated by the HA Program managers. To help understand what was impeding their performance, those interviewed were asked to characterize their constraints.

For Real Property, the CIO and Staffing, the most common inhibitor to better services was staff shortages. For Real Property and the CIO this was further complicated by the LTA-affected staff. Many of those employees had already left to secure positions elsewhere at CSEC. Given the terminable nature of these positions, finding staff to replace those leaving was proving difficult.

To address staff shortages, Real Property implemented a new prioritization process using specific criteria. This has reduced the number of projects in queue from roughly 100 to 30. (Of note, the CSMI is one of the remaining priorities); undoubtedly, this may have adverse affects on those removed from the list.

A problem specific to the Print Shop and Translators was the lack of quality control conducted by the client prior to the receipt of a request. For example, much of the material used by the Learning Centre is contracted out; those interviewed indicated that upon receipt of this material, they sometimes delay production as they note mistakes, inaccurate dates, irregular page numbering, and problems with formatting. At the time of the evaluation, discussions between the Print Shop and IT Security Learning Centre were underway to address these concerns. More up front quality control on the part of clients would facilitate the timely return of jobs sent to the print shop and Linguistic Services.

Generally, within the IT Security Learning Centre, there seemed to be little coordination and interaction between the Subject Matter Experts (SME) and the document authors. This was attributed to some of the confusion in version control and modified content experienced by the translators. Small alterations, such as the title of a document changing, can impact turn around and delivery and can cause issues between the SME and author.

It was recommended that the IT Security Learning Centre look at new ways of delivering courses (such as e-learning and providing course material via CD). Other efficiencies were identified such as removing the name of the course instructor to permit re-use of un-used course material. Using a black and white plus 1 colour option instead of full colour would produce huge savings (the difference in cost is 7 cents a copy for full colour versus under a penny for black and white plus one colour.)

Conclusions

Staff shortages may be impeding the abilities of some of the internal services interviewed. To address this, Real Property in particular has implemented a criteria based system that has reduced the number of requests in queue from over 100 to 30. This, approach however, may have adverse affects on those removed from this list. As previously mentioned, the detail in the business plan and the limited fashion in which these plans are integrated, does not permit proactive planning on the part of the service providers.

4.3 Continuous Improvement Initiatives

To understand how service gaps were being addressed, each of the service providers interviewed were asked to identify current and future client service improvement initiatives. Below is a list of initiatives by Internal Service.

CIO:
The CIO is implementing a 'Capability Maturity Assessment Program' (being led by CIO- . This program is intended to improve service delivery capability.

The CIO is also focusing on aligning their IT Infrastructure Library (ITIL) business processes with those of HP to facilitate transition into the Long Term Accommodation (LTA).

Real Property:
Assets Management Group (AMG) recently put in place a *Facilities Management Procedures* document as well as new parking procedures. There is ongoing work focused on the help' function and a concept of operations for the LTA is being documented.

An AMG retreat to define 'essential services' is being planned to help address staffing shortages.

Procurement:
As of December 2011, clients can access ARS by calling up 'Contracting and Procurement requests' under Financial Services.

The Client Guide is under review and is projected to be finalized during FY 2012-13. There is also a course on procurement, which is being updated.

CIO is presently building a new internal procurement data base. Phase 1, which was completed in December 2011, does not include access to the managers; read only access will come in Phase 2, which is estimated for completion in FY 12-13. This web based application will allow managers to log in and check the status of their procurement initiatives. This should offset the number of calls received by Finance staff and will be an improvement over the current Excel spreadsheet used internally to track contracts.

Print Shop:
The Print Shop is examining options to position an IT Security representative who will act as a liaison between the two groups and do the associated QA and formatting.

The Print Shop is also developing a portal which should reduce the amount of printing and encourage use of multi media methods to access and review information.

Linguistic Services:
Using Cyber Security funding, the Translation unit expects to hire an 'editor' to perform quality control, and ensure consistency with the language rules implemented by the GC. CSEC's new place in government has also provided an opportunity to hire an additional translator. Both additions are expected to improve quality and turn around cycles.

Staffing:
The staffing team is about half way through reviewing HR guidelines for staffing and recruitment. That document outlines the roles and responsibilities for managers and is expected to improve manager and supervisory understanding of staffing processes. There was no mention of developing and/or automating tools to further assist managers with staffing processes.

Conclusions

Internal Service providers would benefit from metrics that measure the impact they are having on operations and, although a number of initiatives are underway to help drive improvements to client services, they mostly reflect plans as opposed to actions that are underway.

Recommendation:
Strategic Planning and Modern Management (SPMM) should lead an initiative that will enable Internal Service providers to measure the impact their services are having on operations.

5.0 SUMMARY OF RECOMMENDATIONS

#	Recommendation	Management Action Plan (MAP)
1	*SPMM should identify ways to improve the Business Planning process to enable more effective and integrated use of its contents by Internal Service Providers.*	During FY 2012/2013 SPMM will lead a review of the business planning process throughout CSEC with the intent of identifying gaps in planning and best practices and recommending standardized practices for business planning to integrate corporate and activity based planning. While noted improvements can be made throughout FY 2012/2013, the most significant changes will be made in FY 2013/2014 as approved recommendations are implemented.
2	*SPMM should lead an initiative that will enable Internal Service providers to measure the impact their services are having on operations.*	Through the Performance Measurement Framework Working Group, SPMM is leading the coordination of performance measures across CSEC. By providing guidance on interpreting TBS policies and managing the overall CSEC PMF, SPMM will work with the operational activity areas and internal service providers to establish performance measures that reflect horizontal impacts on each other's activities. The initial PMF will be submitted to TBS for review and observations by 31 August 2012. Performance indicators will be reviewed in consideration of TBS comments, submitted for ExCom approval and submitted to TBS as the CSEC PMF of record by 31 December 2012.

6.0 ABOUT THE EVALUATION

Reporting
This report reflects the evaluation results. The report including the Management Action Plan was approved secretarially by the Audit & Evaluation Committee members effective 6 July 2012.

Primary Stakeholders

- Director General Cyber Protection
- Director Architecture and Technology Assurance
- Director Crypto Material Systems and Services
- Director Canadian Cryptographic Modernization Program
- Director General Human Resources
- Director General Finance
- Director General Policy and Communications
- Director IT Operations (CIO)
- Director Information Technology Operations (CIO)

Timelines and Resources
This evaluation was conducted using DGAEE internal resources[15] between July 2011 and January 2012.

• July - September 2011	Planning
• September –December 2011	Data collection and analysis
• February 2012	Reporting
• April 2012	CSEC A&E Committee(A&E Com)
• June 2012	Revisions requested by A&E Com

[15] Internal resources include various IT Security Subject Matter Experts (SME's) on a term assignment with DGAEE

ANNEX A: LOGIC MODEL

High Assurance Program Logic Model

Inputs

- Staff/budget Infra-structure
- Legislation And Policies
- ITS Strategies, business plans, threat/industry/ 5-Eyes Info, Industry Products and Services
- Client and partner requirements and plans
- Internal Services

Activities

- Providing Generic HA Guidance
- Providing Tailored HA Guidance
- Providing Cryptographic Key Material
- Providing COMSEC Support Services
- Evaluating and Approving HA Cryptographic Products and KMS

Outputs

- ITSA, ITSB, ITSD, ITSO, HA demos and client comms, HA training
- ITS solutions, crypto Security implementation, HA advice and guidance
- Crypt material Project/Product Management and systems architecture, development and service management
- AFU support, COMSEC & Incident Mgt, TEMPEST Tests/inspections COMSEC special events
- HA Evaluation services, Crypto Algorithm research

Short Term Outcomes

- IT Security guidance is available to GC Clients
- Classified government systems are acceptably secure
- The GC is able to deploy and securely operate fully supported Type 1 crypto

Mid Term Outcomes

- The Government of Canada's IT Security is enhanced

Canada's vital interests are advanced and protected through technical and information superiority

ANNEX B: BIBLIOGRAPHY

Internal Documents

CSE: *Classified Security Management Infrastructure (CSMI) Service Management Working Group (CSMI SMWG). Terms of Reference.* V.4 November 2010. (CERRID 249232)

CSE: *CCF Configuration Management Working Group (CCF-CMWG). Terms of Reference.* December 2010. (CERRID 318406)

CSE: *History of CBNRC.* Volumes IV and V.

CSE: *Inter-Departmental Advisory Committee (IDAC) Terms of Reference. Canadian Cryptographic Modernization Program (CCMP).* Version 2.0. July 2007.

CSE: *IT Security Client Service Working Group (IT Security CSWG).* Terms of Reference. V0.3 (CERRID 648433)

CSE: *Senior Project Advisory Committee (SPAC) Terms of Reference. Canadian Cryptographic Modernization Program (CCMP).* Version 2.0. July 2007.

CSEC: *CCMB_AFU Tracking Spreadsheet.* (CERRID 848364).

CSEC: *ATA Project and Service PRC Overview FY11/12.* July 2011. (CERRID 783240)

CSEC: *CCMP Funding Pie Chart.* August 2011. (CERRID 807083).

CSEC: *CCMP Senior Decision Board Terms of Reference Canadian Cryptographic Modernization Program (CCMP).* Version 1.2. April 2010. (CERRID 837528).

CSEC: *Classified Security Management Infrastructure Architecture Working Group (CSMI AWG) Terms of Reference.* February 2011. (CERRID 222570)

CSEC: *Classified Security Management Infrastructure (CSMI) Requirements Working Group (CSMI – RWG). Terms of Reference.* February 2011. (CERRID 322746)

CSEC: *CSMI Action Item Log.* (CERRID 237319).

CSEC: *Cryptographic Configuration Management Board (CCMB):* Terms of Reference. September 2011. (CERRID 446018)

CSEC: *Cryptographic Product Approval for Use Process Overview.* August 2011. (CERRID 642905)

CSEC: *Cyber Protection CSEC-approved High Assurance Products, Systems and Services Product and Service Catalogue.* February 2011. (CERRID 606376)

CSEC: *Cyber Protection Branch Roles and Responsibilities High Assurance Program.* (CERRID 807387)

CSEC: *Directive for the Control of COMSEC Material in the Government of Canada ITSD-03).* October 2011.

CSEC: Government of Canada (GC) Commercial Product Assurance. June 2010. (CERRID 764822)

CSEC: *High Assurance Working Group Evaluation Review Gates.* Version 6. August 2011. (CERRID 695009).

CSEC: *High Assurance Working Group (HAWG) Terms of Reference.* October 2011. (CERRID 119833).

CSEC: *IT Security 2010.*

CSEC: *ITS 2015.*

CSEC: IT Security Bulletin Bulletin de sécurité TI. *Guidance for the Communications Security of Secret Information.* ITSB-79. July 2011.

CSEC: *IT Security Education Services: Enhancing the Security Posture of the Government of Canada.* Course Catalogue and Calendar. April 1, 2011 – March 31, 2012.

CSEC: *National COMSEC* Info Presentation. 2011

CSEC: *Group Monthly COMSEC Operations Report.* October 2011. (CERRID 845803)

Other Government Documents

CSEC and DND: *6th Annual Report to Treasury Board of Canada Secretariat: Canadian Cryptographic Modernization Program Omnibus Project.* April 2010- June 2011.

GC: *Canada's Cyber Security Strategy for a Stronger and more Prosperous Canada.* (2010)

GC: *Perimeter Security and Economic Competitiveness Action Plan.* (2011)

Treasury Board of Canada Secretariat: *Operations Security Standard: Management of Information Technology Security (MITS).* April 2004.

Treasury Board of Canada Secretariat: *Policy on Government Security.* July 2009.

External Documents

Henderson, Brian. *The Evolving COTS Strategy for Information Assurance and the Commercial Solutions Partnership Program.* NSA Commercial Solutions Centre. September 2010.

Plunkett, Debora A.: *(U) Certification or Approval for Use of Information Assurance Products and Solutions. Information Assurance Directorate.* NSA. IAD Management Directive No. 101. Revised July 2011.

ANNEX C: KEY ACTIVITIES BY MANAGEMENT GROUP

Key Activity		PMO	ATA	ATA			
Providing Generic HA Guidance							
Providing Tailored HA Guidance							
COMSEC Support Services							
Evaluating and Approving HA Cryptographic Products and Key Management Systems							
Providing Cryptographic Key Material							
Facilitating Crypto Modernization							

ANNEX D: WORKING GROUP DECISIONS

INTERNAL

Classified Security Management Infrastructure (CSMI) Steering Committee

The CSMI Steering Committee approves plans for CSMI sub-projects and completion of major CSMI milestones. It also evaluates options and gives direction on CSMI issues requiring Director-level approval. The CSMI Steering committee is chaired by Director with Directors and ATA being members.

Cryptographic Configuration Management Board (CCMB)

The Cryptographic Configuration Management Board (CCMB) was established within CSEC as a forum for the coordination, evaluation, discussion and resolution of issues regarding the overall configuration and approval of cryptographic products deployed within the GC. The CCMB provides coordination and guidance for the approval of new products, modification to existing products and the end of operational life removal of the approval for the termination of products.

The CCMB membership consists of permanent representatives drawn from ATA, PMO and Groups incorporating the following cryptographic expertise:

- Programmatic and Crypto modernization;
- Policy;
- Algorithms;
- Technology;
- Client requirements;
- Doctrine;
- Training; and
- Key management.

A primary role of the CCMB is to provide Approval For Use (AFU) coordination between the affected CSEC groups. The CCMB which is co-chaired by ATA and reports through senior management to DCITS for approvals. By its nature, the CCMB also provides a discussion forum to ensure and promote ongoing internal communications and to help resolve cryptographic product approval issues and concerns as, and when, they arise. The consensus developed by the representative members within the CCMB provides guidance to the board members on the initiation, recommended restrictions, termination and overall document content and prioritization of all products undergoing each stage of the AFU process. The Cryptographic Approval for Use Overview document captures in detail each Unit's roles and responsibilities. The status of all AFU's is tracked and updated regularly using an Excel spreadsheet.

High Assurance Working Group (HAWG)

The goal of the HAWG is to provide advice, guidance and certification recommendations in support of CSMI and IT Security cryptographic programs. This goal is achieved by bringing together IT Security stakeholders to address concerns and exchange points of view on High Assurance evaluations by CSEC (e.g., ATA related to the CCF/CSMI and cryptographic equipment for classified use (e.g.,

The objectives of the HAWG in support of this goal are to:

- Provide guidance on the application of High Assurance standards, specifications and evaluation methodologies

- Facilitate communication within IT Security on High Assurance topics
- Provide High Assurance certification recommendations to Security Accreditation and Authorization (SA&A) authorities and/or to CSEC IT Security executive management.

To meet the objectives, the HAWG has the following responsibilities:

1. Provide guidance and direction on the application of High Assurance standards, specifications; and evaluation methodologies:

   - Approve the High Assurance evaluation requirements and processes on a project basis;
   - Approve the selection of cryptographic algorithms for the protection of classified information. All cryptographic products and programs developed within the GC must register and gain approval by the HAWG prior to production certification.
   - Initiate the activities and processes that will impact HAWG decisions;
   - Track, coordinate the progression of, and approve High Assurance evaluation activities; and
   - Ensure that a database of High Assurance evaluation requirements and "lessons learned" is maintained.

2. Facilitate communications within IT Security on High Assurance topics:

   - Communicate decisions and approvals made by the HAWG to the appropriate IT Security Directors, other CSMI Working Groups, and CSEC staff.

3. Provide High Assurance certification recommendations:

   - For CCF/CSMI products and systems, to Security Accreditation and Authorization (SA&A) authorities (e.g., CIO- ;
   - For evaluated cryptographic equipment, to IT Security executive management (e.g., DGCP or DCITS);
   - Communicate decisions and approvals made by the HAWG to the appropriate stakeholders;
   - Provide oversight to high assurance evaluation projects by providing a High Assurance review gating process (Annex A); and
   - Advise Directors ATA, and of any issues that could impact the security of GC information and systems, or impact the IT Security program.

The HAWG is chaired by ATA and has members from Group, ATA ATA and ATA

CSMI Requirements Working Group (RWG)

The primary goal of the CSMI RWG is to provide advice and guidance for business requirements that will continuously improve the service delivered by the CCF to our GC clients. It will do this by:

- Facilitating business requests/requirement communications within Group, and between and ATA, Groups;
- Coordinate business request/requirement activities and decisions for current and future CSMI capabilities within their authority;
- Producing recommendations to ATA, Management Teams to allow them to make informed decisions where this exceeds the authority of the CSMI RWG to decide; and
- Providing requirements guidance to various CSMI projects.

The RWG is chaired by and meets monthly. It is attended by ATA, and Group staff.

CSMI Architecture Working Group (AWG)

The goal of the CSMI AWG is to provide architectural advice, guidance and decisions in support of the present and future environment of the CSMI.

The principal objectives of the CSMI AWG, in support of the above-stated goal are to:

- Facilitate CSMI specific architecture-centric communications between IT Security elements that support the CSMI (and Groups);
- Coordinate CSMI Architectural activities and decisions for current and future CSMI capabilities;
- Provide CSMI-specific architectural recommendations to IT Security management to allow them to make informed decisions; and
- Provide CSMI-specific architectural recommendations to 5-Eyes to influence decisions that affect the Communications Security Establishment Canada (CSEC).

The AWG is co-chaired by and and meets monthly. It is attended by HA engineers, evaluators and architects from ATA, and Groups.

CCF Configuration Management Working Group (CMWG)

The goal of the CMWG is to provide Configuration Management advice and guidance in support of CCF Development, Test, Staging and Production environments. It will do this by:

- Facilitating configuration management-centric communications within Group;
- Providing recommendations on Configuration Management to TMT to allow them to make informed decisions;
- Providing configuration management and change management guidance to Group projects;
- Providing IT Service Guidance;
- Approving and enforcing standardized methods and procedures are used to provide a logical model of the CCF infrastructure by identifying, controlling, maintaining, and verifying Configuration Items in existence; and
- Approving and enforcing standardized methods and procedures are for efficient and prompt handling of all CCF Changes, in order to minimize the impact of Change-related incidents on service quality.

The primary objectives of the CMWG are in support of the goals stated above. They are to:

- Approve changes to CCF operational environment.
- Approve incident management procedures and best practices.
- Approve configuration management procedures and best practices.
- Approve change management procedures and best practices.

The CMWG is chaired by and meets bi-weekly. It is attended by and ATA (optional) staff.

CSMI Service Management Working Group (SMWG)

The primary goal of the CSMI SMWG is to continuously improve the service delivered by the CCF to our Government of Canada clients. It will do this by:

- Facilitating service management-centric communications within Group, and between and Groups, including reporting on Service Management Metrics and Outstanding Client Requests;
- Making decisions on SM related issues that are within their authority;
- Approving Service Management processes that are deemed to fall within their domain including, but not limited to Incident Management, Problem Management, Availability Management, Service Catalogue Management, Service Level Management, Service Measurement, Service Reporting;
- Producing Service Management recommendations to Management Teams to allow

them to make informed decisions where this exceeds the authority of the CSMI SMWG to decide; and
- Providing service management guidance to various CSMI/ITS projects.

The principle objectives of the CSMI SMWG in support of the above-stated goal are to:
- Facilitate service management-centric communications within the ITS domain (primarily and Groups);
- Coordinate service management activities and decisions for current and future capabilities;
- Provide recommendations (service management-focused) to TMT and LMT to allow them to make informed decisions;
- Optimize visibility of outstanding client service management issues to all stakeholders; and
- Implement and maintain Service Management processes across the Crypto Material Service Management domain.

The CSMI SMWG meets monthly and is attended by PMO- ATA and Group staff.

Client Service Working Group (CSWG)

The primary goal of the IT Security CSWG is to ensure that client requirements are tracked, communicated, well understood and effectively managed across the program. As well, it is to ensure that collectively the IT Security Client Service Model is able to effectively respond to client requirements in a coordinated and efficient manner. It will do this by:
- Facilitating client service-centric communications between the three client service teams making up the IT Security Client Service Model:
  - Cyber Defence Pillar – CTEC
  - CSEC Approved High Assurance Products, Systems and Services –
  - CSEC Security Assurance for Commercial Products, Systems and Services – ATA Group;
- Reviewing all new client requirements to ensure all Client Service units are aware of these requirements and can identify any possible need for service delivery unit involvement from their pillar;
- Making decisions as to which client service unit will take the lead role on a multi-pillar service delivery;
- Coordinating multi-pillar client briefings, presentations, user groups, sessions and other client service activities requiring multi-pillar client service support;
- Reviewing and recommending IT Security client service management processes, tools and deliverables that are deemed to span the client service program; and
- Producing client service recommendations to IT Security management teams to allow them to make informed decisions.

The principle objectives of the IT Security CSWG in support of the above-stated goal are to:
- Facilitate client services communications within the IT Security domain;
- Coordinate client service management activities and decisions for current and future capabilities;
- Provide recommendations (client service management-focused) to IT Security Management to allow them to make informed decisions;
- Optimize visibility/transparency of client service requirements across the IT Security Program to ensure all required resources are aware of and can contribute to the successful delivery of services that add value to our clients/external stakeholders; and
- Implement and maintain Client Service Management processes across the IT Security program that both streamline service delivery and optimize the delivery of quality services to our clients/stakeholders.

The IT Security CSWG meets bi-weekly and is attended by ATA (client service and TAG staff), (client service staff) and CTEC (clients service staff).

EXTERNAL

CCMP Senior Project Advisory Committee (SPAC)

The CCMP SPAC was established to ensure consistent, cohesive and coordinated direction for the CCMP and to ensure that the program continues to meet GC needs. The committee provides oversight for the CCMP IDAC. It is co-chaired by DCITS and DND/ADM(IM).

CCMP Inter-Departmental Advisory Committee (IDAC)

The CCMP IDAC is the mechanism for inter-departmental planning and coordination for the CCMP. This committee is co-chaired by Director and DND/Deputy Project Director Defence CMP and its membership includes CSIS, DFAIT, PCO, PWGSC, PS, RCMP and TBS.

CCMP Senior Decision Board (SDB)

The CCMP SDB is a joint CSEC/DND board that provides guidance, review and oversight of the funded aspects of the CCMP, particularly with respect to financial agreements between CSEC and DND. The CCMP SDB is chaired by DG ITS Cyber Protection.

COMSEC User Group (CUG)

The CUG is attended by all clients across the GC departments that hold COMSEC accounts). The CUG is managed by Group and is a forum for providing COMSEC related information to clients and receiving their feedback. The CUG meets twice a year.

Key Management Strategy Group (KSMG)

KMSG is a 5-eyes forum established to ensure consistent key management policies, standards and systems. The KMSG helps ensure that key management systems and cryptography used by CCEB nations are interoperable as required.

ANNEX E: INTERNAL SERVICES

This annex captures the information provided by the representatives interviewed in response to the following questions:

- *How are client requests prioritized?*
- *What processes and communication strategies are used to assist clients with accessing your services?*
- *What metrics are kept to inform decision making?*
- *What pressures or constraints are impacting your ability to deliver services?*
- *What, if any, process improvements are underway to address these or other concerns?*

Responses are depicted in the same order as the questions and organized chronologically by PAA number. ***These responses reflect the experience and opinions of the respondents and do not indicate an evaluative opinion.***

Translation and Printing (PAA 3.2.3)

Printing:

Client Service Management & Business Processes:
Clients' deadlines determine priorities. Most clients are given a 2 week turnaround time.

The print shop has its own internal database to keep track of client requests. They do not use Remedy because there are too many variables; the system can not drill down to a sufficient enough level of detail to work for their operations.

The print shop participates in the Foundational Learning Curriculum.

Client Feedback:
There is no formal client feedback obtained.

Metrics:
The database that was set up provides volume metrics. However, it does not track the increased complexity of the work completed.

The print shop occasionally outsources some of their work which provides them with benchmark data. This information has been used to inform management on how well the print shop is doing relative to industry and to provide evidence that that they provide good value for money. They are currently planning to use this data to support a business case for another resource.

Impediments:
The IT Security Learning Centre is the print shop's biggest and most complex client (contributing to over 60% of the print shop's output). The workload from the Learning Centre has doubled in the last year because of an increase in the number of courses offered and an increase in the complexity of the work requested of the print shop.

Generally, the print shop is given about a month's notice that a course is happening. However, the lack of quality control is impacting the print shop. A lot of the Learning Centre's work is contracted out, and there is a noted lack of quality control conducted by the Learning Centre before sending the print job to the print shop. As a result, there have been times when the quality control has been completed by the print shop (such as correcting spelling mistakes, incorrect dates, page numbering, and formatting). The IT Services Catalogue was also sent prematurely to the print shop. As a result, 800 copies were printed, which then had to be thrown out because of errors found in the translation.

The IT Learning Centre should look at new ways of delivering courses (such as e-learning and providing course material via CD). Other ways to improve efficiencies include removing the name of the course instructor to permit re-use of un-used course material. Using a black and white plus 1 colour option instead of colour would produce huge savings (the difference in cost is 7 cents a copy for full colour versus under a penny for black and white plus one colour.)

Process Improvement Initiatives:
We are considering putting an MOU in place to have an ITS staff member, at the administrator level, work here to act as a liaison between the two groups and to do the QA and formatting. Currently, there is a lack of coordination, a doubling of courses offered and more consultants doing the work, straining our resources.

Through PinG we are getting one more person for the print shop.

We are developing a portal which should reduce the amount of printing.

Translation:
Client Service Management & Business Processes:
Key clients from the HA Program include COMSEC, CTEC and the ITS Learning Centre. There are currently two translators dedicated to IT Security. Client requests come in via a *Remedy* ticket and are prioritized according to documented service procedures published on the Public Affairs and Communication Services Web site.[16] Requests coming in on the Sabre system are received via email.

Client Feedback:
Although there are no formal methods to collect client feedback, there is a complaint mechanism found within Service Level Agreements established with each of the business lines.

For large clients such as the COTS and Procurement Group (ATA meetings are held to review client processes and discuss how Linguistic services can better meet client needs, and to set expectations and cycle times.

Metrics:
ARS metrics are used (with limitations) to assist the unit head with business planning and resource justifications.

Impediments:
Within IT Security, there seems to be little coordination and interaction between the Subject Matter Experts (SME) and the document authors. For example, small alterations, such as the title of a document changing, can impact turn around and delivery and can cause issues between the SME and author.

Within IT Security, processes vary from unit to unit; the translation team is not always informed as to who wrote the document, who provided the SME content, or who within the unit they should interact with to coordinate the service request. There are also instances of documents needing to be re-translated as they were worked on prior to the document's approval.

The translators have observed issues when documents are uploaded onto the Web: the validation of the French text is questionable due to the presence of fragmented sentences and missing accents. The quality of the final translated document is also impacted when clients make their own changes, introducing linguistic and content errors (for example, a client changed "malveillant" to "malicieux" changing the meaning from 'malicious" to "mischievous").

We also have concerns regarding potential copyright issues as documents are received with copied text and imported images from the web.

[16] http://www.cse-cst.gc.ca/index.jsp?lang=e&doc=/dgpc/pacs/policies-guidelines/service-procedures.xml

Process Improvement Initiatives:
Using Cyber Security funding, the Translation unit expects to hire an 'editor' to perform quality control, and ensure consistency with the language rules implemented by the Canadian Government. CSEC's new place in government has also provided an opportunity to hire an additional translator.

Employee Acquisition & Orientation (PAA 3.4.2)

Client Service Management & Business Processes:
Staffing advisors consult with clients to obtain a view of their priories. It was also reported that the HR planning team is also trying to increase its efforts to plan and prioritize client requests.

Clients have access to staffing guidance via the HR web site. Here they will find relevant HR policies and guidance. However, it was noted that the prevailing practice for managers was to call their staffing advisor in lieu of conducting any research of their own.

Client Feedback:
There is no formal client feedback system in place. The staffing team is very operational, responding to HRSRs and are trying to keep up with client requests. There is no time to survey; and it was once proposed that it be done at a more corporate level. Feedback is obtained informally. In many cases people volunteer feedback either calling or emailing the staffing manger or their HR Staffing Advisor.

Metrics:
A number of reports are available, but there is some concern about data accuracy. This is mostly the result of there being little time available to spend reviewing these reports.

Impediments:
Different Activity Areas use different prioritizing methods. For example, each ITS group works in its own silo. Within CIO, the PMO centralizes priorities across hiring in their area. Within SIGINT, priorities come from different groups. The Business Plans have not improved the staffing team's ability to prioritize and manage client requests.

Staffing is currently facing a lack of resources. In the short term, we will need to be over resourced to catch up to current demand. An assessment of business processes and how to improve them is not possible as we have no resources, thus the same processes are perpetuated. There are currently three people on maternity leave, with temporary staff replacing them. It is difficult to get someone from outside the organization on a temporary basis, so we are finding people from other groups, leaving vacancies in other places.

Another issue facing staffing is that staffing advisors are generally at the UNISON-07 level. Most of the other CSEC HR units have positions at the UNISON-08s and UNISON-09 levels. As a result, staffing becomes a feeder group to these other units, resulting in constant churn.

In addition, currently there are no documented procedures for new people. Admittedly, there is a need for better tools but there is a lack of resources to build them.

Process Improvement Initiatives:
We are currently reviewing our HR guidelines for staffing and recruitment, and we're about half way through. This document outlines the roles and responsibilities for managers.

Application/Data Development (PAA 3.7.2) /Productions and Operations Computing (PAA 3.7.3)

Client Service Management & Business Processes:
There is a Data Centre Working group that both sets and manages client priorities. For infrastructure support, the CIO does not use a first-in/first-out method, rather, using an incident warning system, priorities are assigned based on the severity of the problem.

To access CIO services, there is an on-line Service Catalogue. The CIO also has a presence within the Foundational Learning Curriculum.

Client Feedback:
The CIO uses a formal feedback system via Remedy. There are also Client Service Representatives working with each business line that collect client feedback.

Metrics:
A number of operational metrics are kept by the CIO including readings on power, storage and cooling. Others include number of dropped calls, queue sizes, server utilization, and network lag time.

Impediments:
The over use of 'back door' methods to obtain services and not hearing about issues or projects until very late in the process. The current method of business planning does not provide details that the CIO can plan around. For example, budgets do not account for how the services will be delivered, just how much the 'box' will cost.

Staffing is also a big concern as many in the CIO have been affected with the transition to the CIO. The Service Desk at the best of times is recognized as an entry level opportunity, thus staffing is a constant activity. However, the number of people leaving is pushing operational thresholds.

Process Improvement Initiatives:
The CIO is implementing a 'Capability Maturity Assessment Program (being led by CIO-). This program is intended to improve service delivery capability.

The CIO is also focusing on aligning their ITIL business processes with those of HP to facilitate transition into the Long Term Accommodation (LTA).

Real Property and Operations Management (PAA 3.8.1)

Client Service Management & Business Processes:
The Assets Management Group (AMG) was inundated until recently. Previous prioritization processes included a project management list (called Program of Works) which included around 90-100 projects at any given time. It was hard to prioritize so many projects. In order to do so, we met continually with the business lines and then consulted with the Accommodations Working Group and the Accommodations Committee (steering) to prioritize projects. Accommodation Group Coordinators also met regularly with Accommodations staff. Further meetings were also necessary with PWGSC, CSEC's project management service provider.

We are currently changing the process using the Remedy Action Request System (ARS). As the organization gets closer to the LTA there is an investment freeze because PWGSC doesn't want to spend money on the buildings and we need a static environment to prepare for decommissioning. A few months ago, all the outstanding projects were reviewed to determine which were still critical. This process eliminated roughly 70 of the 100 on the list. A number of criteria were used to determine what was critical. For example, anything that couldn't be completed by fall 2012 was cancelled. Only the corporate and mission priorities remain. CSMI is one of those priorities. However, not much can happen until the CIO moves out.

Clients have access to real property services via the AMG web site. The team also participates in many key meetings, for example, the Accommodations Committee (AC), the ACWG, Datacentre WG, the OSH Policy Committee and WG, Emergency Management Steering Committee and WG. AMG also has a booth at the FLC, where they provide a pamphlet of services to all new employees.

Most requests start with a Business Requirements Identification Template (BRIT) which can be reviewed right up to the AC.

Client Feedback:
AMG doesn't formally obtain client feedback. There have been CSEC wide surveys that have had a facilities piece to it, for example, the LTA survey. In addition, AMG monitors forums on an ad hoc basis, and they also receive feedback through the help desk and phone calls and emails sent to Group staff.

Metrics:
Metrics are being collected, but more could be done. Although AMG is able to pull data from ARS and help desk not much as been done lately as the team has been overwhelmed with dealing with escorting, CVAN and service request issues. There are plans in place to collect metrics again.

Impediments:
Most AMG staff are LTA affected staff; therefore it is hard to get people in. As a result, morale is low. People are looking for new positions instead of waiting until April 2012 when Priority Referral is starting.

Also growth projections for the organization are inflated. For example, for this time last year, 300 new positions were projected but only about 23 people were hired. As well, finance will say SIGINT has the money to hire 20 people and SIGINT states in their plans that they will hire 50. AMG has worked hard with the business lines to get them to accept a projection rate of 50% of their submission.

There is a disconnect between the space planners, HR and finance. The three groups don't speak together enough.

Process Improvement Initiatives:
AMG recently put in place a *Facilities Management Procedures* document as well as new parking procedures. There is ongoing work focused on the help function and a concept of operations for the LTA is being documented.

An AMG retreat to define 'essential services' is being planned to help address staffing shortages.

Services Acquisition (PAA 3.10.1) / Goods Acquisition (PAA 3.10.2)

Client Service Management & Business Processes:
We recognize that there has been minimal information on procurement process for the last several years. At a recent joint MLN/SLN, the need for 'procurement 101' was deemed a top priority.

Client Feedback:
There are no active measures to solicit client feedback.

Metrics:
An array of financial metrics are reported regularly to PPRC.

Impediments:
Due to pressures, Finance hasn't had the opportunity to train their officers as well as they should have and it is recognized that this often results in providing different responses to similar questions.

With the new ARS capability, there will be a procurement option, which will direct questions and requests to the contracting and procurement team. More training is planned for Finance staff and for RC Manages.

Requests often come in very late in the process. Finance staff would like managers to get Finance involved as soon as possible. The earlier Finance staff are aware of what is coming, the better prepared they will be. Too often a group will have worked on a future contract for months, having contacted companies themselves to get information, and then expect Finance to have the contract in place within a day or two. However, there are rules to follow and it is Finance's responsibility to ensure that the procurement process is done fairly and properly documented. There is a lot of time and effort wasted by this duplicated effort.

Process Improvement Initiatives:
As of December 2011, clients can now access ARS by calling up 'Contracting and Procurement requests' under Financial Services.

The Client Guide is under review and is projected to be finalized during FY 2012-13. There is also a course on procurement, which is being updated.

CIO is presently building a new internal procurement data base, Phase 1 of 5 is scheduled for testing in mid-December. This web based application will allow managers to log in and enter their own Purchase Requisitions and check the status of their procurement initiatives. This should offset the number of calls received by Finance staff. This will be an improvement over the current excel spreadsheet used internally to track contracts.

Going forward, all business lines have been asked to submit their 3 year business plans to procurement so that planning can commence for upcoming procurements.

Procurement modernization and PinG.
With PinG, CSEC has asked TBS for increased authority. For example, we currently have authority for and we've asked for We've also asked for increases in authority for In-House contracts and supply arrangements.

If approved, fewer procurement requests will go to PWGSC, but will instead by done in-house. Because of this, the Finance team has had to restructure. Over the summer, areas in finance held many competitions, including procurement. Four new positions were added to the contracting and procurement area as a result of procurement modernization and PinG.

Finance had previously asked for a change in authority for the Cyber Protection Supply Arrangement (CPSA) and had received it, but the authority was only given to the manager of Procurement, herself, not the position. We are trying to change it so the position has authority. Currently, with the Mission Application Systems Projects Supply Arrangement (MASP SA), Finance has no authority.

Finance has also been looking at additional procurement tools used at PWGSC.
There are numerous online tools available, but security does not allow us to use them. We have found others that we are allowed to use. For example, TBIPS (Task Based IT Professional Services). This database is huge and offers a Supply Arrangement or Standing Offer options. However, CSEC currently only has authority to for Supply Arrangements. Finance has asked for

There are also changes in standing offers. PWGSC has several Departmental Individual Standing Offers for software (DISOs). As of December 31, all DISO's expired. These DISO's are being replaced by the Software Licensing Supply Arrangement (SLSA), we were told that the SLSA may not be in fully available by the January 1, 2012. To sum up, we are looking at different tools to make the process better, but we need to have higher authority.

Another issue is the clauses. We are currently looking at the restrictions in place. MASP SA is a concern. Currently, if the MASP SA expires on July 31, 2012 then all call-ups made against this Supply Arrangement will also expire on July 31, 2012. With other tools, you can raise a call-up right up to the expiration date; the MASP SA refresh is expected to address this issue.

s.15(1)

Summary of Internal Services

Internal Service	How are Client Request Prioritized	Processes and servcies	Client feedback	Metrics	Pressures constraints	Continuous improvements
CIO	The Data Centre Working Group Priorities are set by the severity of the problem (there is an incident warning system). The CIO Executive sets the priorities for larger projects.	On-line Service Catalogue Client Service Reps within each business line. Documented processes.	The Service Desk and via Client Service representatives.	Operational indicators such as number of dropped calls, queue sizes, server utilization, network lag time, and improvements to incident management (system health at a macro level). Power, Storage and Cooling	•Use of back doors for client services •Too many priorities of the day •Staffing churn within area •Misaligned business planning processes	•Capability Maturity Assessment Program (CMAP). •Initiatives are underway to align with HP on ITIL
Real Property	Based on the following criteria: •Law/ Code/ •Standards Requirement •Growth •Operational Infrastructure •Co-location •Space •Optimization	All AMG services are on web 2.0 via the Corporate Services Operations Portal.	We don't specifically obtain client feedback.	ARS and Help	•Staff shortages •Low morale •Under the microscope	•Facility Management procedures document, •Parking procedures •Improvements to help function •Concept of operations for the LTA.
Procurement	Based on clients' need, and during peak period and at year end requests are reviewed and prioritized by the Contracting Review Committee.	Via Remedy: 'Contracting and Procurement requests' under Financial Services. (as of December 2011)	No formal process	Financial	•Late notices •Reliance on advisors as opposed to procedures resulting in inconsistent advice •Inadequacies of the Business Planning process •Lack of awareness of business processes (insufficient information and training)	•New client guide •New course on procurement •CIO is presently building a new internal procurement database •Business Lines to submit 3 year business plans to procurement
Printing	Based on clients' deadlines.	Internal database that tracks requests.	No formal process	Volume metrics and benchmarking	•Increased workload and job complexitity •Inadequate client quality control processes	Developing a portal which should reduce the amount of printing
Translation	There is a document that outlines how requests are prioritized. This information is advertised to the whole organization.	ARS Remedy or Email (Sabre only)	here is also a formal complaint mechanism in the SLA.	ARS metrics	•Inadequate client quality control processes •Lack of coordination and interaction between SME's and writers •Client administered changes affecting quality of output	Creating an editor position and increasing team by one additional Translator
Staffing	Arrival of HRSRS and consultation with Managers	HR Website	Feedback is obtained informally.	Staffing reports	•Insufficient resources complicated by being a feeder group •Inability to redefine business processes due to time and resource pressures •Lack of documented procedures for new staffing advisors	Working on a better recruitment system, but we need CIO's help. Migration to CERRID

ANNEX F: LIST OF ACRONYMS

ACRONYM	EXPANDED TEXT
ADM	Assistant Deputy Minister
AFU	Approval For Use
ARS	Action Request System
ATA	Architecture & Technology Assurance (Cyber Protection Branch)
ATA	Cyber Protection Branch)
ATA	(Cyber Protection Branch)
AWG	Architecture Working Group (CSMI)
BDRC	Business Development Review Committee
CCEB	Combined Communications Electronics Board
CCMB	Cryptographic Configuration Management Board
CCMP	Canadian Cryptographic Modernization Program
CDS	Cross Domain Solutions
CF	Canadian Forces
CSFC	Commercial Solutions for Classified (USA)
CIO	Chief Information Officer
CIOB/TBS	Chief Information Officer Branch/Treasury Board of Canada Secretariat
CMVP	Cryptographic Module Validation Program
CMWG	Configuration Management Working Group
COMSEC	Communications Security
COTS	Commercial Off-the-Shelf
CSFC	Commercial Solutions for Classified (USA)
CSIS	Canadian Security Intelligence Agency

ACRONYM	EXPANDED TEXT
CSMI	Canadian Security Management Infrastructure
CSWG	Client Services Working Group
CUG	COMSEC User's Group
DCITS	Deputy Chief IT Security
DFAIT	Department of Foreign Affairs & International Trade
DGCP	Director General Cyber Protection
DGPC	Director General Policy and Communications
Dir IM Secur	Director Information Management Security
DND	Department of National Defence
DSO	Departmental Security Officer
GC	Government of Canada
GCHQ	Government Communications Headquarters (UK)
GOTS	Government Off-the-Shelf
GTEC	Government Technical Electronics Conference
HA	High Assurance
HA Program	High Assurance Products and Services Program
HAWG	High Assurance Working Group
IA	Information Assurance
IAD	Information Assurance Directorate
IDAC	Inter-Departmental Advisory Committee (CCMP)
IP	Internet Protocol
IT	Information Technology
ITSB	IT Security Bulletin
JET	Joint Executive Team
KMSG	Key Management Strategy Group

ACRONYM	EXPANDED TEXT
	(Cyber Protection Branch)
MASP SA	Mission Application Systems, Projects Supply Arrangement
MITS	Management of Information Standard
MTA	Mid Term Accommodations
NIAP	National Information Assurance Partnership
NSA	National Security Agency (USA)
O&M	Operating and Maintenance
PAA	Program Activity Architecture
PCO	Privy Council Office
PGS	Policy on Government Security
PMC	ITS Program Management and Oversight Directorate)
PS	Public Safety
PWGSC	Public Works Government Services Canada
RADARSAT	Radar Satellite Program
RCMP	Royal Canadian Mounted Police
RDS	Red Distributed System
RWG	Requirements Working Group (CSMI)
SAB	Secret-and-Below
SDB	Senior Decision Board (CCMP)
SIGINT	Signals Intelligence
SMWG	Service Management Working Group (CSMI)
SPAC	Senior Project Advisory Committee (CCMP)
SSC	Shared Services Canada
	Cyber Protection Branch)

ACRONYM	EXPANDED TEXT
	(Cyber Protection Branch)
	Cyber Protection Branch)
	(Cyber Protection Branch)
TBS	Treasury Board of Canada Secretariat
TEMPEST	Telecommunications Electronic Material Protected from Emanating Spurious Transmissions
TRA	Threat and Risk Assessment
TSAB	Top Secret-and-Below
USG	United States Government
VFM	Value for Money
VPN	Virtual Private Network

Communications Security Establishment Canada

Security Posture Assessment

Of

Department of National Defence

Final Report

The report does not represent an endorsement of any particular product or tool by CSEC. The material in it reflects CSEC's best judgement, in light of the information available at the time of preparation. Any use that the client makes of this report, or any reliance on or decisions made based on it, are the responsibility of the client. CSEC accepts no responsibility for damages, if any, suffered by any party as a result of decisions or actions based on this report.

Dated: March 08, 2012

Manager
CSEC Security Posture Assessment

Executive Summary

In the third of a series of on-going information technology security-related audits Chief Review Services (CRS) engaged the services of the Communications Security Establishment Canada (CSEC) team to conduct a security assessment of the The assessment started on 28 March 2011 and ended on 30 November 2011. and was conducted in accordance with the specific rules stated in a Memorandum of Understanding (MOU), Reference A, and with the authority provided by a Ministerial Authorization (MA), Reference B, from the Minister of National Defence.

Since the internal portion of the network was assessed in 2009, this assessment concentrated on The results of this assessment should be combined with the internal assessment results to gain a complete picture of the security posture of the network. Due to the complex permission process to assess some of the networks connected to

To fulfill the objectives of all

Introduction

Page 55

is withheld pursuant to sections

est retenue en vertu des articles

15(1), 16(2)(c)

of the Access to Information Act

de la Loi sur l'accès à l'information

s.15(1)
s.16(2)(c)

Table of Contents

References

A. Memorandum of Understanding between the Communications Security Establishment (CSE) and the National Defence (DND), signed by Deputy Chief, IT Security, CSE and Greg Jarvis, Chief Review Services, Department of National Defence dated 7 December 2007.

B. Ministerial Authorization – Protection of Computer Systems and Networks of the Government of Canada (DND), dated 16 November 2010, signed by the Honourable Peter G. MacKay, Minister of National Defence.

C. 7050-33-5 (CRS) Client Letter of Validation for Activities, contains the received from DND, signed by John Turner, Assistant Deputy Minister Information Management, and by Jill Sinclair, Assistant Deputy Minister Policy, dated 8 March 2011, covers the

D. 7050-33-5 (CRS) Client Letter of Validation for Activities, contains the received from DND, signed by John Turner, Assistant Deputy Minister Information Management, and by Rear-admiral R.A. Davidson, Director of staff – Strategic joint Staff, dated 8 March 2011, covers the

E. 7050-33-5 (CRS) Client Letter of Validation for Activities, contains the received from DND, signed by John Turner, Chief of Staff, Assistant Deputy Minister Information Management, and by Brigadier-General D.W. Thompson, Commander Canadian Special Operations Forces Command, dated 20 June 2011, covers the

F. 7050-33-5 (CRS) Client Letter of Validation for Activities, contains the received from DND, signed by John Turner, Chief of Staff, Assistant Deputy Minister Information Management, dated 20 June 2011, cover the DWAN network.

Introduction

1. This report details the activities conducted as part of the assessment of the Department of National Defence (DND) and provides recommendations for improving this network's security posture. The assessment started on 28 March 2011 and ended on 30 November 2011. The activities were performed by the team in accordance with the Memorandum of Understanding (MOU) Reference A. Appropriate authority to perform this assessment was obtained as documented in References A, B, C, D, E, and F.

2. For any assessment, the team is limited to exploiting only publicly known vulnerabilities and to using only publicly known attack vectors. That is to say, the tools and techniques are known to any Internet threat agent and are not Although the computer tools are publicly known and available,

3. The information contained within this report is time-sensitive and subject to change as the network evolves. New vulnerabilities are constantly being discovered. The recommendations in this report are made to improve the security posture of DND's networks but there is no guarantee that the resulting posture is sufficiently secure against a sophisticated threat agent. DND is responsible for determining the level of acceptable risk, and this should be made in the context of a Threat and Risk Assessment. It is DND's responsibility to ensure that all recommendations are tested in a controlled environment to identify and resolve any unexpected effects resulting from the recommendations.

Timeline

4. The following table lists the major milestones of this assessment:

Milestone	Date
Signature of MOU	07 December 2007

Signature of Ministerial Authorization	16 November 2010
Assessment Activities	28 March – 30 November 2011
Presentation of Findings to DND	08 February 2012
Draft Report Delivered to DND	08 February 2012

Pages 59 to / à 101

are withheld pursuant to sections

sont retenues en vertu des articles

15(1), 16(2)(c)

of the Access to Information Act

de la Loi sur l'accès à l'information