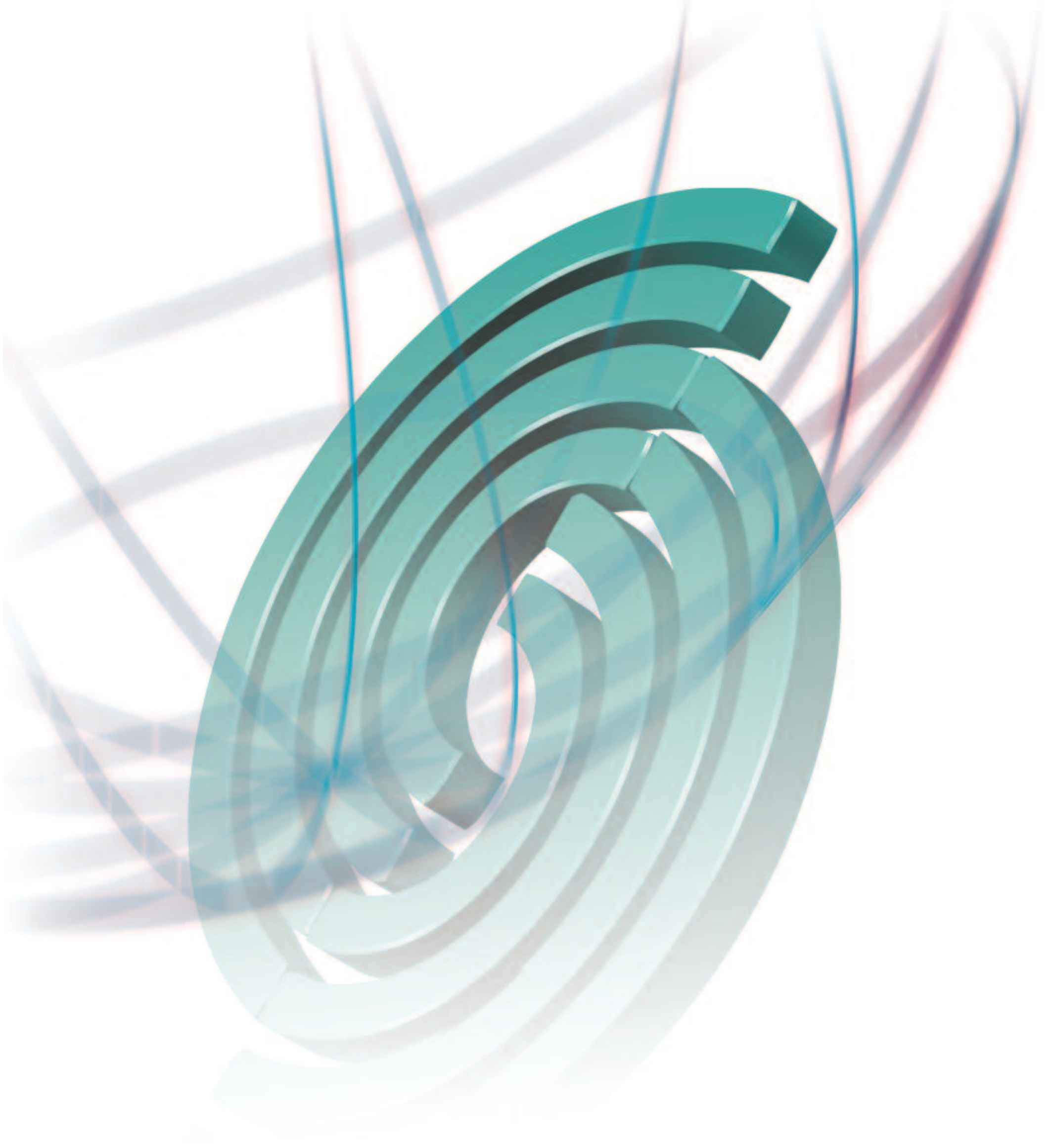
Standards Council of Canada
Conseil canadien des normes



Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities

CAN-P-1591C (ITSET)
April 2010

Canada

GUIDELINES FOR THE ACCREDITATION OF INFORMATION TECHNOLOGY SECURITY EVALUATION AND TESTING FACILITIES

LIGNES DIRECTRICES RELATIVES À L'ACCRÉDITATION DES INSTALLATIONS D'ÉVALUATION ET D'ESSAISDE PRODUITS DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

CAN-P-1591C (ITSET)

April 2010

Standards Council of Canada
Conseil canadien des normes

Standards Council of Canada
270 Albert Street, Suite 200
Ottawa, Ontario
K1P 6N7 Canada
Tel: (613) 238-3222
Fax: (613) 569-7808

NOTE: On peut obtenir un exemplaire français de ce document en écrivant au :
Conseil canadien des normes
200-270 rue Albert, OTTAWA (Ontario), K1P 6N7
Tél.: (613) 238-3222.
Télécopieur: (613) 569-7808.

NOTE : An English version of this document is available from the:

Standards Council of Canada
270 Albert Street, Suite 200,
OTTAWA, Ontario
K1P 6N7
Tel.: (613) 238-3222
Fax.: (613) 569-7808
Email: info.palcan@scc.ca
Website: www.scc.ca

TABLE OF CONTENTS

FOREWORD

The Standards Council of Canada ("Council") is a crown corporation established by an Act of Parliament in 1970, amended in 1996, to foster and promote efficient and effective voluntary standardization in Canada. It is independent of government in its policies and operations, although it is financed partially by Parliamentary appropriation. The Council consists of members from government and the private sectors.

The mandate of the Council is to promote the participation of Canadians in voluntary standards activities, promote public-private sector cooperation in relation to voluntary standardization in Canada, coordinate and oversee the efforts of the persons and organizations involved in the National Standards System, foster quality, performance and technological innovation in Canadian goods and services through standards-related activities, and develop standards-related strategies and long-term objectives.

In essence, the Council promotes efficient and effective voluntary standardization in Canada in order to advance the national economy, support sustainable development, benefit the health, safety and welfare of workers and the public, assist and protect consumers, facilitate domestic and international trade and further international cooperation in relation to standardization.

In addition, the Council serves as the government's focal point for voluntary standardization and represents Canada in international standardization activities, sets out policies and procedures for the development of National Standards of Canada, and for the accreditation of standards development organizations, of product certification bodies, of testing and calibration laboratories, of quality and environmental management systems registration bodies and of quality management systems and environmental auditor certifiers and training course providers, and promotes and supports the principle of recognition of accreditation or equivalent systems as a means of decreasing the number of multiple assessments and audits, both in Canada and with Canada's trading partners.

This document is one of several issued by the Standards Council of Canada to define the policies, plans, and procedures established by the Council to help achieve its mandate.

Requests for clarification and recommendations for amendment of this document, or requests for additional copies should be addressed to the publisher directly.

PREFACE

In 1998, the Communications Security Establishment (CSE) committed to working with government and industry to develop a commercial information technology security (ITS) testing and evaluation capability for widespread use both within the government and the private sector.

In cooperation with the CSE, this document, CAN-P-1591C, has been produced by SCC as a framework for accreditation of ITS Evaluation and Testing (ITSET) facilities within Canada.

This document is intended for information and use by accreditors, staff of accredited ITSET facilities, those facilities seeking accreditation, other laboratory accreditation systems, customers of facility services and organizations or individuals needing information about the requirements for accreditation under the ITSET accreditation program.

CAN-P-1591C (ITSET) is a specific guideline document that amplifies CAN-P-4E, *General Requirements for the Competence of Testing and Calibration Laboratories*, which is a verbatim Canadian adoption of ISO/IEC 17025:2005, *General Requirements for the Competence of Testing and Calibration Laboratories*. Technical requirements are explained to indicate how they are to be applied to the ITSET Program Specialty Area (PSA).

Any facility (including commercial, manufacturer, university, and federal or provincial government laboratory) that performs any of the test methods that comprise the ITSET PSA may apply for SCC accreditation. Accreditation will be granted to a facility that conforms to the requirements for accreditation as defined in this document and those of the PALCAN Handbook CAN-P-1570. Accreditation does not imply a guarantee of facility performance or of product test data; it is a recognition of facility competence.

INTRODUCTION

The purpose of this document is to amplify, where appropriate, generic technical and organizational criteria as stated in ISO/IEC 17025: 2005 (CAN-P-4E) for SCC accreditation of facilities that could perform ITS evaluation and testing. In their respective ITS Approval Domains, recognized ITS Competent Authorities may recognize the accreditation of those facilities for activities such as, but not limited to, the following activity areas:

- Common Criteria product and system evaluations;
- Cryptographic module and algorithm testing (if also accredited to CAN-P-1621, *Requirements for the Accreditation of Cryptographic Module and Algorithm Testing Facilities*);
- ITS product reviews;
- Secure electronic commerce application evaluations;
- Biometric device testing;
- Vulnerability and tiger team testing; and
- Specialized commercial security device testing.

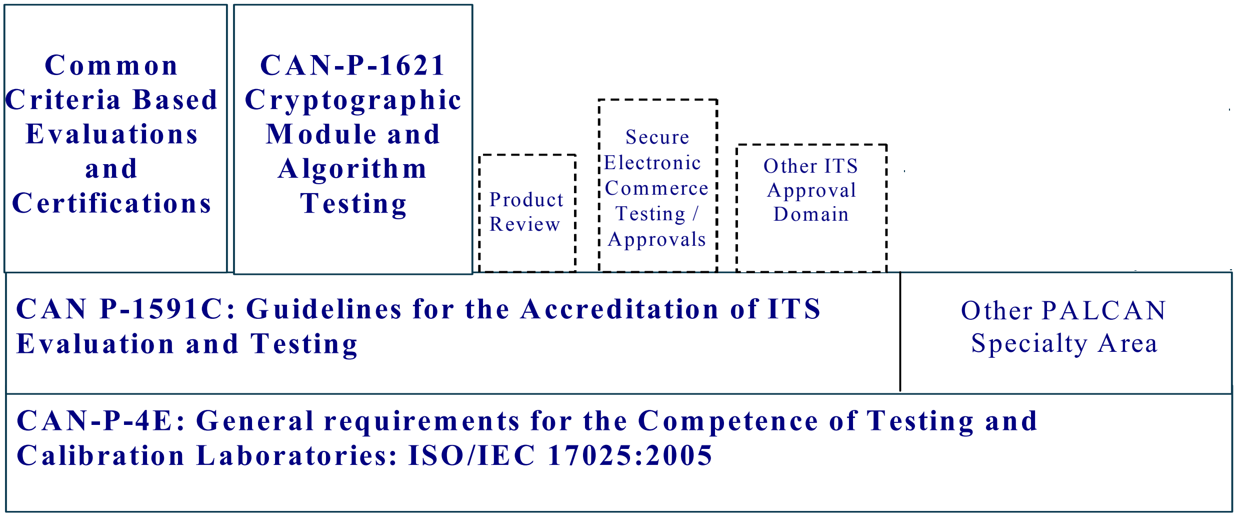

Common Criteria Based Evaluations and Certifications
CAN-P-1621 Cryptographic Module and Algorithm Testing
Product Review
Secure Electronic Commerce Testing / Approvals
Other ITS Approval Domain
CAN P-1591C: Guidelines for the Accreditation of ITS Evaluation and Testing
Other PALCAN Specialty Area
CAN-P-4E: General requirements for the Competence of Testing and Calibration Laboratories: ISO/IEC 17025:2005

Figure 1: This diagram shows specific and generic ITS Approval Domains

The Standards Council of Canada accredits laboratories for carrying out objective tests. Objective tests will be controlled by:

- Documentation of the tests, including test procedures;
- Validation of the tests;
- Training, qualifications and authorization of staff; and
- Maintenance of equipment and facilities.

And where appropriate by:

- Calibration of equipment;
- Use of appropriate reference materials;
- Provision of guidance for interpretation;
- Verification of results;
- Testing of staff for proficiency; and
- Recording of equipment and test performance.

GENERAL REQUIREMENTS

This document provides generic information for ITSET facilities, independent of ITS specialization. Detailed requirements for each specialization, as identified, will be produced and provided in accordance with customer demand. As the scope of ITS grows, more specialization areas may be added to the current list. Criteria in a specific specialization may amplify generic criteria where appropriate. In particular, each specialization area of ITSET testing and evaluation will have defined performance criteria necessary to maintain an ITSET facility's proficiency, as tested by the quality assurance programs, where these exist and are part of the accreditation requirements.

Cryptographic module and algorithm testing is one such ITS specialization. To accommodate this specialization, the requirements of this standard have been updated where appropriate. In addition a new Procedural Document, CAN-P-1621, *Requirements for the Accreditation of Cryptographic Module and Algorithm Testing Facilities* has been introduced. Facilities wishing to perform cryptographic module and algorithm testing should meet the requirements of CAN-P-1621 in addition to these requirements.

Facilities that are successful in obtaining SCC accreditation will be provided with a Certificate of Accreditation for Information Technology Security Evaluation and Testing and a Scope of Accreditation that will detail the scope of testing for which the accreditation has been granted. Accredited facilities may also enter into agreement with the SCC on the use of the SCC logo as part of their accreditation in accordance with the SCC Logo License Agreement.

1. REFERENCES

i. CAN-P-4E: *General Requirements for the Competence of Testing and Calibration Laboratories,* Standards Council of Canada.

ii. ISO/IEC 17025: 2005, *General Requirements for the Competence of Testing and Calibration Laboratories*.

iii. ISO/IEC Guide 28: 2004, *Conformity Assessment – Guidance on third-party certification system for products.*

iv. ISO/IEC 15408: 2005/2006, *Evaluation Criteria for IT Security: Part 1: Introduction and general model; Part 2: Security functional requirements; and Part 3: Security assurance requirements.*

v. *International vocabulary of basic terms in metrology* (VIM): 2004, issued by ISO.

vi. ISO/IEC 17000:2004, *Conformity Assessment Vocabulary and General Principles*.

vii. ISO/IEC Guide 2: 2004, *General Terms and Their Definitions Concerning Standardization and Related Activities.*

viii. CAN-P-15CA - SCC Conformity Assessment Accreditation Program Requirements and Procedures for the Suspension and Withdrawal of Accreditations and the Resolution of Complaints, Disputes and Appeals - September 2009.

ix. PALCAN Handbook (CAN-P-1570), *Program for the Accreditation of Laboratories (PALCAN),* Standards Council of Canada.

x. NIST Handbook 150, *NVLAP, Procedures and General Requirements*, National Institute of Standards and Technology/National Voluntary Laboratory Accreditation Program (NIST/NVLAP), Gaithersburg, MD USA.

xi. NIST Handbook 150-20 Checklist, *Information Technology Security Testing Common Criteria*.

xii. ISO/IEC 17011:2005, *Conformity assessment, General Requirements for accreditation bodies accrediting conformity assessment bodies.*

xiii. *Guidelines for Technical Assessors Conducting a Visit*, Standards Council Canada.

xiv. *Assessment Rating Guide for use With: CAN-P-4E (ISO/IEC 17025:2005) "General Requirements for the Competence of Testing and Calibration Laboratories"* F0410E: September 2009, Standards Council Canada.

2. DEFINITIONS

2.1 All definitions in CAN-P-4E (i.e. laboratory, testing laboratory, calibration laboratory, calibration, test, calibration method, test method, verification, quality system, quality manual, reference standard, reference material, certified reference material, traceability, proficiency testing, accreditation requirements) and those applicable from ISO 17000 (e.g. quality assurance, quality control) apply, as well as the following items specific to this document:

Approved Signatories: Persons qualified and authorized to sign test reports. and calibration certificates prerequisite to delivering a test report or calibration certificate to the customer.

Approval: Determination by an information security authority, that a facility is technically competent in a specific activity area for ITS evaluation and testing and the formal authorization enabling the facility to carry out testing within the context of the ITSET.

Architectural Design: The conceptual specification of the structure and operation of the ITS product.

Cryptographic Module: The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

Evaluation: Analysis and conformance testing conducted against national and international security evaluation criteria (e.g. the Common Criteria). Term is equivalent to SCC notion of "testing."

Information Technology Security Evaluation and Testing (ITSET) Facility: A facility that has been accredited by SCC through the ITSET to conduct security evaluation and testing of ITS products.

Facility: An organization that conducts security evaluations and tests. When a facility is part of an organization that carries out activities in addition to evaluations and tests, the term "facility" refers only to those parts of that organization that are involved in evaluation.

Facility Accreditation: A formal recognition that a facility has met the ITSET accreditation requirements. Facility accreditation identifies the facility as competent and capable to perform security evaluations and tests of ITS products and systems in accordance with ITSET.

ITS Approval Domain: A specialized IT Security area for which a recognized ITS Competent Authority exists, and for which:

a) standards exist (or will in the future) to govern specialized ITS evaluation and testing activities;

b) there exists a need for evaluating and testing of ITS products or services;

c) the recognition of individual and organizational competencies to perform specialized security evaluation and testing activities exists;

d) the requirement for control and oversight of a specified range of IT security product evaluation and testing exists;

e) there exists a need for reviewing and approving evaluation and testing results and;

f) accredited SCC ITSET lab(s) exist(s).

Information Technology Security: All aspects related to defining, achieving, and maintaining confidentiality, integrity, availability, accountability, or access control.

Key Technical Personnel: Facility personnel with the authority and responsibility to make the important technical evaluation decisions. The “chief”, “lead”, or “team leader” evaluator roles are examples.

On-site Assessment: The on-site examination of a facility to assess its compliance with the conditions and criteria for accreditation under the ITSET.

Product: Any IT security technology that is intended to protect assets and which is the target of security Evaluation and Testing activities. Such technologies may range from stand alone hardware or software components, through to fully integrated systems, and may include any procedural processes on which these technologies are dependant for secure use in the intended environment.

Proficiency Testing: Demonstration by a facility that it can successfully perform testing and evaluation activities applicable to its Scope of Accreditation. Under ITSET, facilities will be required to demonstrate theoretical and applied competence in the conduct of ITS product evaluations and tests.

Records: Documented evidence and data, intended for future reference, of a specific act, analysis, result, event or other activity, that is related to ITS Evaluation and Testing. Records should be kept in an appropriate form (which may be electronic or otherwise) that is permanent for their required useful life as determined by the Recognized ITS Competent Authority.

Recognized ITS Competent Authority: An organization which exercises leadership, official authority or direct influence over a specified ITS Approval Domain to control, and ensure compliance with, appropriate standards and best practices related to evaluation and testing of products within that domain. This organization is responsible for the approval of accredited ITSET facilities to conduct specialized security evaluation and testing activities in order that approval or certification of results for products applicable to the specific ITS Approval Domain may be granted.

Security Requirements: Specification of functionality or design controls for information technology that, when implemented, provide security.

Technical Review: A process whereby an ITSET facility's evaluation team gains sufficient knowledge of a product to permit a technical judgement regarding its likelihood of satisfying a particular security requirement.

Testing Tools: The complete set of equipment, including any hardware and software utilities and associated documented procedures, which are used to support Security Product Evaluation and Testing activities. Such equipment should be appropriate for the intended use, and should be managed, operated and maintained in accordance with the manufacturer's requirements and any other appropriate practices.

Validation: Validation of a test tool or procedure is the process of verifying as far as possible that the test tool will behave properly or that the test procedure will produce results that are consistent with the specifications of the relevant test suites, relevant standards, or previously validated versions of the test tool.

3. SCOPE OF TESTING

3.1 ITSET activities range from tests with clearly defined results, such as firewall penetration tests, password strength verification tests and biometric false acceptance rate tests, to activities which may require a great deal of interpretation, such as the implementation robustness of the security functions and features of a software/hardware ITS product.

3.2 ITSET involves the analysis of security features implemented within a software/hardware ITS product which can provide the following security services:

- Confidentiality of information;
- Integrity of information;
- Availability; and
- Accountability.

3.3 Specific security features that can be tested for may include but are not limited to the following:

- Identification and authentication;
- Security audit (audit trail generation and secure storage, analysis of security relevant events);
- Non-repudiation;
- Cryptographic services (cryptographic operations, cryptographic key management);
- Secure transport of information (implementation and enforcement of access control and/or information flow rules/policies);
- Stored data integrity;
- Management of security functions, security relevant data and security management roles;
- Protection of security functions, including non-bypassability and domain separation;
- Resource utilization (fault tolerance, priority of service, resource allocation);
- Fail-safe;
- Self-test; and
- Physical protection (tamper detection/prevention).

3.4 Techniques used to evaluate security features may include but are not limited to the following:

- Known answer tests;
- Vulnerability analysis to ensure that that the customer has considered all potential vulnerabilities within the ITS product under evaluation;
- Software code reviews;

- Detailed analysis of the development environment and associated documentation to determine the effectiveness of the configuration management system applicable to the ITS product under evaluation;
- Detailed examination of delivery documentation to determine if it describes adequately all of the procedures required to maintain the integrity of the ITS product under evaluation;
- Examination and testing of installation, generation and start-up procedures to determine if they are complete and sufficiently detailed to result in a secure configuration of the ITS product under evaluation;
- Detailed analysis of development documentation such as functional specifications, high-level designs, low-level designs to ensure they accurately instantiate all interfaces and security functions inherent of the product under evaluation;
- Detailed analysis of user and administrator guidance documentation to determine that it sufficiently and unambiguously describes how to securely use and administer the product, and ensure consistency with the other documentation supplied for the evaluation;
- Examination and assessment of development security procedures during site visits to determine that they detail sufficiently the security measures for the development environment required to protect the confidentiality and integrity of ITS product design and implementation;
- Assessment of customer developed tests in terms of coverage and depth, independent functional tests, and independent penetration tests;
- Security policy mapping; and
- Security requirements tracing.

3.5 Generic ITS Testing Approach

3.5.1 The Security Testing methodology identifies four major elements in the planning and execution of the ITSET facility's security testing: Test Coverage Analysis; Test Plans; Test Procedures; and Test Results.

3.5.2 Test Coverage Analysis is usually comprised of mappings from security features to the tests that demonstrate the correct behaviour of those security features. Test Coverage can be used to demonstrate that all security features have been tested.

3.5.3 The Test Plan describes the extent to which each security feature will be tested, the approach for testing it as well as the resources, such as equipment, personnel and time necessary to carry out such an approach to testing.

3.5.4 The Test Procedures describe the sequence of actions conformant to the Test Plan necessary to set up the test environment, establish the necessary test prerequisite conditions, perform the testing, and document the expected test results. Test Procedures are recorded in sufficient detail to eliminate ambiguity during test conduct such that other evaluators can repeat the test procedures in the future, and obtain the same test results.

3.5.5 The Test Results document the actual test results observed during testing. These actual test results are recorded in sufficient detail not only to allow comparison with the expected test results, but also to facilitate comparisons if the tests are repeated in the future. Based on the actual test results, a determination can be made regarding correct security behaviour.

4. DEMONSTRATING TECHNICAL COMPETENCE

4.1 Composition of the Assessment Team

Facility accreditation identifies the facility as competent and capable to perform security evaluation and testing of ITS products and systems in accordance with defined standards. SCC in partnership with CSE offers accreditation to ITSET facilities. SCC provides the Lead Assessor for each accreditation or re-assessment, and CSE provides one or more Technical Assessors for the on-site assessment and proficiency testing.

4.2 Preparation for On-Site Assessment

4.2.1 The objective of the on-site assessment is to facilitate the demonstration of conformance of the facility's operations to CAN-P-4E. SCC will provide the following document – *Guidelines for Technical Assessors Conducting a Visit* to the CSE Technical Assessor as a reference for conducting the on-site assessment.

4.2.2 Prior to the on-site assessment the assessors will review the facility Quality Manual and staff resumes. Should the assessors require additional documentation from the facility to support proficiency testing the facility should be notified in advance of the assessment in order to allow for the submission of the requested documentation.

4.3 Proficiency Testing

4.3.1 Facilities are required to participate in proficiency testing for identified test methods. Under ITSET facilities will be required to demonstrate theoretical and applied competence in the conduct of ITS product evaluations and tests. Successful completion of proficiency testing is required prior to initial accreditation and periodically thereafter. Facilities renewing accreditation should have satisfactorily participated in all required proficiency testing during their previous accreditation period or have demonstrated the necessary improvements to overcome noted deficiencies.

To properly evaluate a facility, proficiency testing may consist of the following methods:

- Evaluation of the education and experience of facility technical staff against the requirements specified in clause 5.2.1 of Annex A and the required skills and competencies section found in Annex B;

- Evaluation of the facility's ability to apply applicable evaluation criteria and evaluation methods correctly and consistently by examining records of evaluation activities and any supporting documentation; and

- Observation of the IT security expertise (e.g., witnessing performance of functional/vulnerability/penetration testing) of facility staff and the technical processes in place within the facility.

For programs within a scope of accreditation for which evaluation technical oversight[1] is applied on an on-going basis (i.e. Common Criteria Program), the facility will have had an opportunity in the past to demonstrate their competence in security evaluation and testing of ITS products and systems. Where applicable, the results of technical oversight will be used as part of proficiency testing.

[1] The technical oversight process is detailed in Annex B.

ANNEX A

APPLICATION OF CAN-P-4E REQUIREMENTS FOR ITSET FACILITES

This Annex is to be used in conjunction with F0410E. Applications are considered an elaboration of the generally stated requirements of CAN-P-4E for which testing and evaluation criteria specifically applicable to ITSET will be used. The CAN-4E clause numbers for which the application applies are indicated in the table which follows.

4. Management Requirements

CAN-P-4E (ISO/IEC 17025: 2005 Section No.)	***SCC Application Notes for ITSET Facilities***
4.1 Organization	
4.1.5 b)	The ITSET facility shall establish policies and procedures for maintaining impartiality and integrity in the conduct of ITS testing, specifically: • The facility may, at the discretion of the ITS Competent Authority, develop ITS products; and • The facility may, at the discretion of the ITS Competent Authority, provide consulting services for and participate in the ITS testing of the same product.
4.1.5 h) and 5.2.1	At least one technical staff member shall have management responsibilities and be a qualified ITS professional meeting the basic education requirements (5.2.1) and have extensive experience in ITS. For Common Criteria evaluation facilities the sufficiency of education and ITS experience of facility staff members will be reviewed and assessed against a pre-defined skills matrix developed by the ITS Competent Authority/CSE.
4.2 Management System	
4.2.2	The Quality Manual shall include the facility's scope of calibrations and/or tests as detailed on the SCC website.
4.4 Review of Requests ,Tenders and Contracts	
4.4.1.a)	The ITSET facility and its customer shall agree in writing what constitutes the test item and the environment in which the test item will be tested, including: the specific test item, the test configuration and the external environment. The ITSET facility and the customer shall agree, in writing, to the following: • the specific test item; • the test configuration; • location(s) of testing/evaluation; • whether assistance for preparation of evaluation environment will be provided by the customer, such as shipping special equipments to the facility, installing special operating system and database systems etc; • deliverables to be provided by customer; • deliverables to be produced by facility; and • facility approach to testing. Final test reports shall be kept by the facility following the completion of

	testing for the duration specified by the customer and/or the ITS Competent Authority.
4.13 Control of Records	
4.13.2.1	The facility shall maintain a functional record-keeping system that is used to track test activities for each security product evaluation. Records of evaluation activities shall be traceable to recognized industry standards and methodologies where applicable. Records shall be easily accessible and contain enough evaluation evidence so that an independent body can determine what evaluation work was actually performed and can concur with the verdict. The ITSET facility shall produce records covering the following activities: • creation of and changes to evaluation procedures and methodology; • acceptance/rejection of products submitted for evaluation; • complete tracking of multiple versions of evaluation evidence and evaluation technical reports; • complete tracking of evaluation activities including initial analysis, verdicts and any subsequent changes to those verdicts (e.g., based upon modifications of evidence or additional analysis); and • information sufficient to reproduce any testing performed during the evaluation; • the configuration of all test equipment used during an evaluation along with analysis of that equipment to confirm the suitability of test equipment to perform the desired testing. Facility records shall be maintained, released, and/or destroyed in accordance with the facility's proprietary information policy and contractual agreements with customers.

5. Technical Requirements

CAN-P-4E (ISO/IEC 17025: 2005 Section No.)	***SCC Application Notes for ITSET Facilities***
5.2 Personnel	
5.2.1	The facility shall have at least three technical staff members with appropriate educational background (a university degree or college diploma in computer science, engineering, or a related discipline, or professional certification), and relevant experience in security product development, testing, or evaluation experience. In addition facility staff shall have knowledge or experience for any specific technology for which an evaluation is required.
5.2.2	The Management system shall document the policies and procedures (training program) governing the routine checks of the competence of all of the staff involved in the conduct and evaluation of tests. In the case where only one member of facility staff is competent to conduct a specific aspect of testing, audits shall at a minimum include a review of documentation and instructions, adherence to procedures and instructions, and documentation of the audit findings.
5.3 Accommodation and Environmental Conditions	
5.3.1	The facility shall maintain an environment capable of conducting ITS evaluations. This includes facilities for security evaluation and testing, staff training, record keeping, document storage and software/hardware storage.

	The facility shall regularly update all systems relevant to testing and evaluations against viruses and other malware. The facility shall have an effective back-up system in place to restore evaluation evidence (data and records) in the event of their loss. When testing is performed at the customer site or other location outside the facility, all ITSET requirements pertaining to equipment, accommodation and environment shall apply.
5.3.3	Processes and procedures shall be in place to maintain separation of different products under evaluation if evaluations are taking place simultaneously. This includes the product under evaluation and all associated testing and evaluation evidence.
5.3.4	A system shall be in place to safeguard customer proprietary hardware, software, evaluation deliverables, electronic and paper records. This system shall protect customer proprietary materials and information from unauthorized access. Technical safeguards (firewall, intrusion detection system etc.) shall be in place to protect internal systems relevant to ITS testing and evaluations from untrusted external entities.
5.5 Equipment	
5.5.1	For their scope of accreditation, the facility shall have appropriate hardware, software, and computer facilities to conduct ITS product evaluations and tests. The facility shall maintain on-site systems adequate to support IT security evaluations in keeping with the tests for which it is seeking accreditation. The facility shall have, or be able to provide with reasonable notice, a sufficient IT infrastructure to support: • word processing, for the production of reports ; • secure e-mail communication with customers, ITS Competent Authority etc; • internet access; and • specialized tools as may be required for evaluation work.
5.5.6	For ITSET, “equipment” refers to software and hardware products or other assessment mechanisms used by the facility to support the evaluation and testing of the ITS product. The facility shall maintain on-site systems adequate to support ITS product evaluations and tests. The equipment used for tests shall be operated and maintained as follows: • in accordance with the manufacturer’s recommendation; • as specified in the test method; or • as specified in the detailed requirements specific to the program specialty area. Facilities shall have procedures that ensure appropriate configuration of all test equipment. Facilities shall maintain records of the configuration of test equipment and all analysis to ensure the suitability of test equipment to

	perform the desired testing. The facility shall have procedures to ensure proper retention, disposal or return of software and hardware after the completion of the evaluation.
5.8 Handling of Test and Calibration Items	
5.8.1	The Quality Manual shall include procedures for: • the handling and integrity of products; • the handling and integrity of testing tools and software; and • the conduct of on-site testing.
5.10 Reporting the Results	
5.10.1	The ITSET facility shall issue test reports of its work which accurately, clearly and unambiguously present the test conditions, test set up, test results and all required information.
5.10.2	Test reports shall contain statements that the report should only be reproduced in full, unless otherwise authorized in writing by the facility.
5.10.3 e)	The test report shall reference standard tests or otherwise provide a description of the tests.

ANNEX B

SCOPE OF ACCREDITATION FOR COMMON CRITERIA EVALUATION FACILITIES

Introduction

Facility accreditation identifies a facility as competent and capable to perform security evaluations and tests of Information Technology Security (ITS) products and systems. This annex details the specific evaluation/test methods that such facilities may perform under the ISO/IEC 15408 standard (also referred to as the *Common Criteria*, or CC), by utilizing the methodology document ISO/IEC 18045 (also referred to as the *Common Evaluation Methodology*, or CEM).

The Communications Security Establishment (CSE) operates the Certification Body (CB) for the Canadian Common Criteria Evaluation and Certification Scheme (CCS). The CCS is a government-industry partnership, whereby commercial evaluation facilities conduct CC evaluations of IT security products, and CSE provides technical oversight and certification of the evaluation results. CSE is also responsible for approval of CC evaluation facilities (CCEF), and utilizes the ITSET PSA in determining technical competence; successful evaluation facilities receive the Scope of Accreditation identified below, which is specific to the CC standard.

This annex also details the skills and competencies required of facility staff and proficiency testing techniques specific to CCEFs.

Scope of Accreditation

In accordance with the following standards:

- ISO/IEC 15408: Evaluation Criteria for IT Security: Part 1: Introduction and general model; Part 2: Security functional requirements; and Part 3: Security assurance requirements; and
- ISO/IEC 18045: Common Methodology for Information Technology Security Evaluation,

the scope of accreditation comprises the following evaluation and testing activities:

- APE: Protection Profile Evaluation;
- ASE: Security Target Evaluation;
- EAL1: Evaluation Assurance Level 1;
- EAL2: Evaluation Assurance Level 2;
- EAL3: Evaluation Assurance Level 3;
- EAL4: Evaluation Assurance Level 4; and
- ALC_FLR: Flaw Remediation.

REQUIRED SKILLS AND COMPETENCIES

For the accreditation scope detailed above facility staff shall have a working knowledge of ISO/IEC 15408 and ISO/IEC 18045, and possess the skill and expertise required to perform the following activities in a manner that is compliant with the requirements of ISO/IEC 15408 and ISO/IEC 18045:

- Evaluate a Protection Profile;
- Evaluate a Security Target;
- Perform a detailed analysis of customer development environment and associated documentation to determine the effectiveness of the customer' s configuration management system;
- Perform a detailed examination of customer delivery documentation to determine if it describes adequately all of the procedures required to maintain the integrity of the ITS product under evaluation;
- Examine and test installation, generation and start-up procedures to determine if they are complete and sufficiently detailed to result in a secure configuration of the ITS product under evaluation;
- Perform a detailed analysis of development documentation such as functional specifications, high-level designs, low-level designs to ensure they accurately instantiate all interfaces and security functions inherent of the product under evaluation;
- Perform a detailed analysis of user and administrator guidance documentation to determine that it sufficiently and unambiguously describes how to securely use and administer the product, and ensure consistency with the other documentation supplied for the evaluation;
- Examine and assess development security procedures during site visits to determine that they detail sufficiently the security measures for the development environment required to protect the confidentiality and integrity of ITS product design and implementation;
- Perform a vulnerability analysis to ensure that that the customer has considered all potential vulnerabilities within the ITS product under evaluation;
- Perform an assessment of customer tests in terms of coverage and depth, conduct independent functional tests, and perform independent penetration tests;
- Perform a review the customer's test plan, test approach, test procedure and test results, and examine their test evidence to demonstrate that security functions perform as specified and that the security functionality has been systematically tested against the functional specification and high-level design;
- Develop functional tests by examining customer design and guidance documentation, examining the customer's test documentation, executing a large sample of the customer's test cases, and creating test cases that augment customer tests;

- Develop penetration tests based on vulnerability analysis, functional specifications, high-level designs, low-level designs and installation guidance; and
- Generate observation, evaluation and test reports in accordance with the requirements of the Canadian Common Criteria Scheme (CCS).

PROFICIENCY TESTING – TECHNICAL OVERSIGHT PROCESS

As noted above, the CB is responsible for performing technical oversight of CC evaluation work performed by CCEFs. Through this process of technical oversight, the CB can determine whether the CCEF is performing quality evaluations, or whether corrective action needs to be taken by the CCEF. To meet the requirements of technical oversight in the CCS the facility should be capable of the following activities:

- producing an Evaluation Work Plan (EWP) and evaluation schedule with appropriate resources assigned and activities included;
- providing a mature version of the Security Target (which has been obtained from the developer) and the Deliverables List;
- performing evaluation activities in compliance with the requirements of the CC and CEM, and produce evaluation evidence for the CB during the evaluation conduct stage;
- responding to Observation Reports raised by the CB;
- producing an Evaluation Technical Report (ETR) and Preliminary Certification Report (PCR) documenting the findings; and
- working as a coordinated team to successfully perform the evaluation.

The CB may choose to observe some evaluation activities more closely or repeat more evaluation activities than would otherwise be the case in other CC evaluations, in order to ensure that appropriate procedures and analysis are being applied. The results of the technical oversight process described above can be used for proficiency testing purposes.

In addition to the technical oversight process the CB assesses, tests and approves prospective CC evaluators. In order to participate as CC evaluators, personnel are required to demonstrate evidence of ITS education and relevant past experience, and to pass an exam administered by CB to test knowledge and ability in the application of the CC and the CEM. Once individuals successfully complete both of these requirements, the CB issues an evaluator certificate identifying the maximum EAL to which the evaluator is qualified to perform work under the CCS.