FOUNDATIONS FOR THE HARMONIZATION OF INFORMATION TECHNOLOGY SECURITY STANDARDS

Item: Deliverable #1

Source: Cooperation on Security of Information Systems
Joint Task 01

Status: Revised Draft, Version b

Date: April 1993

ABSTRACT

This paper is the first work product of Joint Task 1 (JT01) defined in the Joint Workplan for cooperation on Security of Information Systems [1]. The objectives of JT01 are to:

(a) Establish a common set of security functionality classes, representative of international and regional market-driven needs.

(b) Develop a common approach to the creation of profiles from these security functionality classes consistent with current regional and international activities.

(c) Create guidelines to support the prototyping of such profiles and their interoperability.

This paper provides a base for common understanding of critical terms and concepts. It discusses the efforts and terms used in the four major Information Technology Security efforts:

(a) The U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC) [2], also known as the Orange Book.

(b) The European Information Technology Security Evaluation Criteria (ITSEC) [3].

(c) The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [4].

(d) The U.S. Federal Criteria for Information Technology Security [5].

In addition, this paper looks at the terms and concepts used in the development of International Standards Organization (ISO) standards for Open Systems Interconnection (OSI).

This paper is presented as a base for the JT01 work and is not intended to analyze the good or weakness of various approaches to defining functionality classes or profiles. It attempts to point out where there are differences or conflicts in the terminology, or the terminology is not precise to allow for a common international acceptance.

TABLE OF CONTENTS

LIST OF TABLES

1. INTRODUCTION

Considerable effort has been expended by many countries to develop Information Technology (IT) Security Standards. Over the past decade the concepts and criteria for the evaluation of security products has matured in the European Community (EC), United States (U.S.), and Canada. The wide spread availability of products in the international market place has dictated the need for a standard that can have wide acceptance and applicability for vendors in international markets. Vendors cannot afford to build and have evaluated products in multiple countries against multiple standards. The goal of this effort is to develop an approach that allows for the harmonization of standards and the stimulation of the market place to allow vendors to produce products that can be sold with sound security properties in an international market.

The first set of criteria that received widespread use and acceptance was the U.S. Department of Defense Trusted Computer System Evaluation Criteria (TCSEC). This criteria standard, also known as the Orange Book, defines six classes divided into four hierarchical divisions. Each class defines the features necessary to satisfy the broad control objectives of Security Policy, Accountability, Assurance, and a fourth, Documentation, which describes the type of written evidence in the form of user guides, manuals, and the test and design documentation required for each class. The TCSEC is not limited to the definition of security requirements for monolithic systems, however, several interpretations were developed to address database management systems, networks, and components. The TCSEC was developed specifically for the U.S. Defense industry and has been applied to a much wider market that now includes most of the U.S. government and NATO.

The first attempt at developing a harmonized criteria was the development of the Information Technology Security Evaluation Criteria (ITSEC) developed by France, Germany, the Netherlands, and the United Kingdom. The ITSEC introduced the concept of separating the functional requirements and the assurance requirements. This was achieved by the introduction of six assurance evaluation levels defined as E1 through E6. The structure of the ITSEC allows for the selection of arbitrary security functions to be matched against one of the six assurance levels. The ITSEC defines functionality classes as a means to specify a set of complementary security enforcing functions, and provides ten example specifications, five of which relate to the six TCSEC defined classes[1].

The Canadian Trusted Computer Product Evaluation Criteria (CTCPEC), released within a year of the ITSEC, attempts to avoid the need for criteria interpretations such as those that have evolved in the U.S., by widening the targeted products to include monolithic systems, multi-processor systems, databases, subsystems, distributed systems, network systems, and others. This was done by splitting the criteria into two distinct groups: functionality and trust. There are four criteria defined as Confidentiality Criteria, Integrity Criteria, Availability Criteria, and Accountability Criteria. For trust the criteria is defined as Assurance Criteria

The CTCPEC introduces the concept of a profile as a logical grouping based upon constraints. These profiles are used to define systems which are currently under development, have completed evaluation, or are considered useful configurations and have been evaluated in either the U.S. or the EC. The Canadian approach to profiles allows for the infinite development of profiles to meet customer requirements that do not break any of the Criteria's constraints. The approval of profiles in Canada is by the Communications Security Establishment (CSE).

[1] TCSEC classes B3 and A1 do not differ as far as functionality is concerned.

The latest Information Technology (IT) Security Criteria development effort is the U.S. Federal Criteria for Information Technology Security conducted jointly by the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). This project, which is called the Federal Criteria, is producing a Federal Information Processing Standard (FIPS) for the specification, development, and evaluation of information technology security products. Key to this effort is the advancement of the state of the art of IT security and the harmonization of international efforts. Key features of this standard effort are:

(a) Protection profiles that unite functionality, assurance, and dependency considerations to describe generic protection needs.

(b) Compatible with an IT security development process that accommodates market need, timeliness constraints, and varying degrees of assurance.

The Federal Criteria standard provides a process for user or interest groups to state their distinct protection needs, or vendors can describe the protection needs of an identified market niche. The Protection Profile is intended to represent customer needs throughout the international market for IT security products. A methodology is included for the analysis and approval of Protection Profiles to ensure their consistency, uniqueness and evaluatability. The methodology encourages the development of Protection Profiles from predefined functionality and assurance "building blocks". The registry of protection profiles is envisioned to grow and change in response to new protection needs, technology advances, and market demands; and to entice vendors to meet protection profiles to satisfy customer requirements. This approach also protects the investment of vendors and users in existing products and methods while supporting the rapid changes in technology and innovation.

The final standards effort that must be included in the evaluation by JT01 is the work by the International Standards Organization (ISO) for Open Systems Interconnection (OSI). In recognition of the need for functional standards and profiles to be produced and harmonized, a new type of international standard known as an International Standardized Profile (ISP) [7] has emerged with an initial orientation toward OSI. There are a number of groups working at the regional level that are involved with the production of profiles. These profiles are really sets of compatible base standards with selected options and parameters that insure interoperability.

In all of the above efforts there are a variety of definitions and terms used to describe similar concepts. The terms profile, functionality class, security sub-profile, protection profile and security target are further developed in following sections. The goal of harmonization can be achieved through a sound common understanding of the goals, benefits and relationships of the various efforts. The remaining sections attempt to identify the concepts and terms in a structure that can lead to harmonization of criteria and stimulation of the international market for IT security products.

2. TERMS AND DEFINITIONS

The goal of harmonization of standards efforts requires that the technical requirements and foundations be formed such that a common understanding and acceptance can be achieved. There are several obstacles to this progress that must be overcome. First is the desire of everyone to push their national or regional view, and second, the language differences between the parts of the world. This description of terms and definitions attempts to clarify the second issue without being judgmental on the correctness or validity of any national or regional view. To achieve harmonization this paper attempts to build on each of the national efforts and attempt to show a meaningful progression or advancement that each has provided to the field of IT Security.

2.1 Components of Standards

Looking at the existing set of criteria and standards shows some consistent components to security standards that should form the foundation for harmonization efforts. These building blocks begin with the basic components of a system that provide for security. Most of the existing efforts divide the basic elements into functionality, assurance, and product definition. Each of the efforts to define criteria for IT Security and the international standards activities bring slightly different perspectives to this problem. The following sections layout the definitions and approaches to the structuring of functionality requirements, assurance requirements, and product definition approaches. The information is taken from the latest draft or version of the ITSEC, CTCPEC, Federal Criteria, and the Taxonomy of Security Standards [8].

2.2 Functionality Requirements

2.2.1 Building Blocks

Each of the criteria efforts provides a way of organizing functionality to meet security objectives, referred to here as "building blocks". These building blocks are defined in Table 1 for the various efforts.

Table 1: Building Blocks

Source	**Term**	**Definition**
ITSEC	Generic Heading	A natural grouping of security enforcing functions to give a sensible order for their presentation.
CTCPEC	Division	A functional aspect or mechanism defined to satisfy a specific task (i.e., on a per task basis).
Federal Criteria	Functional Component	A set of rated requirements for protection functions to be implemented in an IT product.
OSI	Base Standard	Defines generalized procedures to provide a conceptual service interface.

Note that these terms are not at the same level of discourse. The ITSEC begins with security enforcing or security relevant functions to be arranged under the appropriate generic headings for a specification. The CTCPEC and Federal Criteria provide established categories of functions to meet defined objectives, whose use is encouraged, but not mandated. This is intended to provide a degree of structure and quality to a specification, since a comprehensive and consistent set of building blocks can be used as the starting point. It is also meaningful that at this level the issues of dependencies and constraints are addressed in both the Federal Criteria and the CTCPEC.

2.2.2 Groupings

Each criteria effort provides a means to assemble the standard building blocks into a group that addresses a perceived threat or security requirement. These groupings provide the sets of requirements that must be implemented to counter a threat or provide support for a specific control objective. Table 2 lists the means to assemble groups of basic building blocks provided by the current efforts.

Table 2: Groupings

Source	**Term**	**Definition**
ITSEC	Functionality Class	Predefined groupings of security enforcing functions assembled under generic headings.
CTCPEC	Functional Criteria	A specific set of mechanisms to implement a security requirement. Four criteria are defined as confidentiality, integrity, availability, and accountability. Constraints are placed on functionality criteria.
Federal Criteria	Functional Package	Grouping of functional components assembled to ease specification and common understanding of an IT product's capabilities.
OSI	Security Sub-Profile	A distinct set of security-related functions in an International Standardized Profile (ISP). The security sub-profile contains the field of application, functionality and quality requirements.

As before, these terms are at different levels of discourse. However, the common thread through each of these groupings is the intent to focus the basic building blocks on the threat or control objective that is required to build a secure product. The binding of functional building blocks to meet the well understood threats and protection requirements provides a focus on the role and need for a variety of functions, mechanisms or services.

2.2.3 Market Directed Requirements

The next level of assembling requirements is based on market directed definitions. Looking at the approaches of the various criteria efforts, each attempts in some way to provide flexible definitions to meet a variety of market requirements for secure products. As can be seen in Table 3 below, each criteria effort has addressed this issue differently with respect to validation and review of perceived market requirements. This level of definition and understanding of requirements are expected to be key to criteria harmonization efforts in the future. The agreement of requirements in a market or threat environment provides a foundation for the mutual acceptance of evaluation against these requirements.

Table 3: Market Directed Requirements

Source	**Term**	**Definition**
ITSEC	Predefined Functionality Classes	The ITSEC allows the definition of functional requirements either by using a predefined functionality class, or by reference to an existing functionality standard, or by directly specifying the security enforcing functions using the generic headings. These may be combined with the predefined assurance levels in order to allow appropriate flexibility for new market developments and to avoid confusing the IT users with too different evaluation results.
CTCPEC	Security Functionality Profiles	A logical grouping based on constraints used to define systems which are currently under development and undergoing evaluation, have completed evaluation, or are considered useful configurations and have been evaluated in either the U.S. or EC.
Federal Criteria	Protection Profiles (Functionality Portion)[2]	Statement of security criteria; shared by IT product producers, consumers, and evaluators; built from functional, development assurance, and evaluation assurance requirements; to meet identified security needs through the development of conforming IT products.
OSI	International Standardized Profiles	These types of standards are especially useful for procurement, product certification and services accreditation. They essentially aim at a common industry approach to the way base standards are used to enable non-specialist to understand what is being sought or proposed. They generally provide a reduced set of base standard options for users, procurers, designers etc. to use as a referencing system for claiming functional conformance.

The trend in specifying profiles is toward a market focus that provides a definition of the requirements for secure IT in an identified market. This provides a great deal of flexibility in that several sources of profiles can

[2]The Federal Criteria has no specific term defined to refer to the functionality portion of a protection profile.

direct the standards development and the vendors are influenced by market pressure to meet the defined requirements. Thus the medical, transportation, or banking industry may develop a profile that defines the requirements in their market and vendors who want to sell into that market could have their products evaluated against the defined profiles. This approach also places greater emphasis on evaluation of requirements when the profile is registered or balloted as in the Federal Criteria or OSI model. Therefore, requirements are validated, to some extent, before vendors build products to meet them. This establishment of well understood and agreed requirements should help encourage vendors to develop compliant products.

2.2.4 Common Structure

The definitions and structure of functionality requirements has evolved differently in the four criteria efforts. As has been pointed out earlier, while there may be differences in approach or specifics, all four efforts appear to structure functionality in a similar manner. The following table attempts to summarize the four efforts and provide rough equivalences among terms.

Table 4: Functionality Requirements

Effort / **Level**	**ITSEC**	**CTCPEC**	**Federal Criteria**	**OSI**
Market Requirements	Predefined Functionality Classes	Security Functionality Profile	Protection Profile	International Standardized Profile (ISP)
Groupings	Functionality Classes	Functional Criteria	Functional Package	Security Sub-Profile
Building Blocks	Generic Headings	Divisions	Functional Components	Base Standards
Basic Elements	Security Enforcing Functions	(Services/ Mechanisms)	Protection Functions	

2.3 Assurance Requirements

The second component of the criteria and standards efforts are the assurances that are built into the product or applied to the product. Each of the criteria efforts have their own slant on assurance starting with basic types of assurance and building into assurance profiles. Taking the same approach as the above analysis of functional requirements, the different descriptions of assurance in the criteria standards are reviewed.

2.3.1 Base Assurance Factors

The basic assurance factors for the criteria efforts focus on the assurances built into the product as well as the evaluation or evidence gathering that the product meets the specified functional requirements. The basic assurance factors for the three national efforts are listed in Table 5. Note that no relationships across columns are maintained or intended for any row in the table.

Table 5: Basic Assurance Factors

ITSEC	**CTCPEC**	**Federal Criteria**
Effectiveness	Architecture	Development Process
Effectiveness Criteria – Construction	Development Environment	TCB Property Identification
Suitability of Functionality	Development Process	TCB Design
Binding of Functionality	Configuration Management	Element Identification
Strength of Mechanism	Development Evidence	Modular Decomposition
Construction Vulnerability Assessment	Functional Specification	Structuring Support
Effectiveness Criteria – Operation	Architectural Design	Design Disciplines
Ease of Use	Detailed Design	Interface Definition
Operational Vulnerability Assessment	Implementation	TCB Implementation Support
Correctness	Operational Environment	TCB Testing & Analysis
Construction – Development Process	Security Documents	Functional Testing
Requirements	Security Functionality User's Guide	Penetration Analysis
Architectural Design	Trusted Facility Manual	Covert Channel Analysis
Detailed Design	Security Testing	Operational Support
Implementation		User Guidance
Construction – Development Environment		Administrative Guidance
Configuration Control		Flaw Remediation
Programming Languages and Compilers		Trusted Generation
Developers Security		Development Environment
Operation – Operational Documentation		Life Cycle Definition
User Documentation		Configuration Management

ITSEC	CTCPEC	Federal Criteria
Administration Documentation		Trusted Distribution
Operation - Operational Environment		Development Evidence
Delivery and Configuration		TCB Protection Properties
Start-up and Operation		Product Design & Implementation
		Product Testing & Analysis
		Functional Testing
		Penetration Analysis
		Covert Channel Analysis
		Product Support

2.3.2 Assurance Groupings

Each criteria includes a set of assurance groupings that define various levels of assurance with respect to the base assurance factors. These assurance groupings provide the definition of assurance to address the requirements for broad sections of the market. Table 6 defines the structures of the assurance groupings in the three major national efforts. Again, OSI is not provided, since the definitions of assurance groupings is not clearly identified in this standards effort.

Table 6: Assurance Groupings

ITSEC	CTCPEC	Federal Criteria
Levels	Levels	Assurance Packages
E6	T7	T7
E5	T6	T6
E4	T5	T5
E3	T4	T4
E2	T3	T3
E1	T2	T2
E0	T1	T1
	T0 (Non-compliant)	

Note that in the case of the Federal Criteria the assurance groupings, T1-T7, are only examples of development assurance. Furthermore, unlike the other criteria standards that have fixed levels, the assurance packages in the Federal Criteria are variable and may be specified as part of the protection profile development.

2.3.4 Diversified Approaches

The base assurance concepts defined in the different standards efforts do not map well across efforts. Rather, they appear to be used as a means to provide focus on the important assurance issues as perceived by each effort. The OSI area appears to be the most open of them all when addressing assurance. Table 7 contains the list of assurance terms used.

Table 7: Assurance Concepts

Source	**Term**	**Definition**
ITSEC	Assurance	The confidence that may be held in the security provided by the Target of Evaluation. Assurance includes correctness and effectiveness aspects.
	Correctness	A property of a Target of Evaluation such that it accurately reflects the stated security target for that system or product.
	Effectiveness	A property of a Target of Evaluation representing how well it provides security in the context of its actual or proposed operational use.
CTCPEC	Trust	The rating granted under the Assurance Criteria. The basic components of the Assurance Criteria are defined as Architecture, Development Environment, Development Evidence, Security Manuals, Security Testing, and Trusted Distribution and Generation.
Federal Criteria	Assurance	Encompasses all the factors that contribute to a sense of confidence that the product satisfies its security requirements.
	Development Assurance	Specifies requirements for all phases of an IT product’s development from initial product design through implementation. Includes the development process, the development environment, operational support, and development evidence.
	Evaluation Assurance	Specifies requirements for the kind and intensity of evaluation to be performed on an IT product developed to meet a protection profile, in accordance with the expected threat, intended method of use, and assumed environment.

Source	Term	Definition
OSI	Conformance Testing	Involves testing both the capabilities and the behavior of an implementation, and checking what is observed against both the conformance requirements in the relevant standards and what the implementor states the implementation's capabilities are. (ISO 9646)

The description of assurance requirements is not as consistent as the functionality requirements in the various criteria efforts. There appears to be a need to study further the assurance requirements and how they apply to IT products in general and how to describe these characteristics in a way that can be accepted in the global market. There are many similarities in the descriptions and the basic assurance factors across criteria. One interesting point is that the Federal Criteria allows for the specification of additional or unique assurance requirements in the Protection Profile. This may be an approach that would allow for national development of Assurance Profiles and the ability to add other specific assurance requirements in the Protection Profile.

2.4 Product Definitions

The terminology used in the standards efforts and the definitions of the elements seems to be consistent with one another. The OSI work does not define the product or system being defined in any specific way. The other three efforts provide the definitions listed in Table 8.

Table 8: Product Definitions

Source	Term	Definition
ITSEC	Product	A package of IT software and/or hardware, providing functionality designed for use of incorporation within a multiplicity of systems.
	System	A specific IT installation, with a particular purpose and operational environment.
	Security Target	A specification of the security required of a Target of Evaluation, used as a baseline for evaluation. The required contents are: either a system security policy or product rationale, a specification of the required security enforcing functions, a definition of required security mechanisms (optional), the claimed rating of the minimum strength of mechanisms, and the target evaluation level.
	Target of Evaluation (TOE)	An IT product or system which is subjected to security evaluation.

Source	Term	Definition
CTCPEC	Products	Monolithic systems, multi-processor systems, databases, subsystems, network systems, and others.
Federal Criteria	Security Target	Product specific description, elaborating the more general requirements in a protection profile and including all evidence generated by the producers, of how a specific IT product meets the security requirements of a given protection profile.
	Product	Package of IT software and/or hardware designed to perform a specific function either stand alone or incorporated into an IT system.

The CTCPEC is the only one of the three that does not require the definition of the products approach to meeting the security requirements defined in the Profile. The ITSEC document contains the only criteria that defines requirements for both IT products and systems

3. SUMMARY

This paper looks at the structure and definition of the evolving IT security standards, and provides a baseline for the discussion and understanding of the various approaches used in their development. There is a concern that the development of standards and criteria disjoint from the methodology used to evaluate against those requirements may produce less than acceptable results. Close vigilance must be given to the evaluation process to ensure that the results are aligned with the goal of a market oriented approach.

Each of the evolving efforts discussed, provides beneficial additions to the results of previous efforts. It is not necessary for each of the national organizations to conform to a single approach or methodology. However, the goal of harmonization is that there be a common understanding of requirements, and that vendor products can be focused on market needs without the overhead of multiple national evaluations.

REFERENCES

[1] Joint Workplan for EC/U.S. Cooperation on Security of Information Systems, Edition 1, Brussels, February 1992.

[2] Department of Defense (DoD) Trusted Computer System Evaluation Criteria (TCSEC), DoD 5200.28-STD, December 1985.

[3] Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, June 1991.

[4] The Canadian Trusted Computer Product Evaluation Criteria (CTPEC), Version 3.0e, April 1992.

[5] Federal Criteria for Information Technology Security, Version 1.0, December 1992.

[6] Security Sub-Profiles, Functionality Classes and Security Targets, Draft Version 4.0, June 1992.

[7] ISO/IEC/TR 10000, Information Technology - Framework and Taxonomy of International Standardized Profiles, February 1990.

[8] ITAEGV N69, Taxonomy of Security Standardization, Version 2.0, April 1992.