

# Evaluation Issues

Marshall D. Abrams and Harold J. Podell

---

In this essay we present an introduction to evaluation issues in the United States and European Community (EC) to illustrate the two schools of thought. Following development of draft national and regional criteria, the US, Canada, and EC are working on Common Criteria (CC). We compare the proposed evaluation approaches in the hope that in the international process of developing the Common Criteria there will be a convergence to assist the multinational producers of secure products and systems in evaluation by different national entities. Interoperability of IT and IT security to support electronic commerce depends, in part, on an acceptance of evaluated products in different countries and regions. Therefore, an important aspect of evaluation is the development of international agreements for reciprocity of evaluations of secure products.

Our focus is on the evolving importance of evaluation issues that pertain to IT security. These issues are national, regional, and international in scope. We consider evaluation to be the security evaluation of products and systems.

Terminology differs between the TCSEC and ITSEC. In some cases, the difference is superficial. We suspect that the varying cultures and, to some degree, the “not-invented-here” phenomenon may have had something to do with the differences. In other cases, there are fundamental differences in outlook and philosophy. Harmonization of criteria is desirable. Following development of draft national and regional criteria, the US, Canada, and European Community are working on Common Criteria. The current multilateral work on developing the CC could contribute to the convergence necessary for a harmonized standard. For this essay, we focus on what the TCSEC and ITSEC documents are saying. To that end, we present side-by-side discussion of related concepts.

In the EC, the term is target of evaluation (TOE), which includes products and systems. However, the US terms vary. For example, the Na-

tional Security Agency (NSA) evaluates secure products and produces an Evaluated Products List (EPL). Secure systems are evaluated within US organizations in a phased process. For example, a system may first be certified to a level of IT security by a technical official or team. The final acceptance of the system can be referred to as **accreditation**, which is the managerial review and approval or rejection. If approval is granted, the implication is that management is accepting a degree of residual risk.

## **Evaluation of products and systems**

There are two fundamental questions addressed in this essay: What is evaluated, and who does the evaluation? There are essentially two sets of answers considered in this essay: one represented by the practices of the United States National Computer Security Center and the other proposed for use by the EC in the Information Technology Security Evaluation Criteria (ITSEC) and its companion documents.

**What are products?** Products are developed by a company with the expectation that when they are offered for sale enough copies will be purchased to enable the developer to make a profit. In the computer and related industries, products are usually combinations of hardware, firmware, and software that can be purchased commercially. Some of the terms used to identify products are “commercial off the shelf,” abbreviated COTS, and “nondevelopment item,” abbreviated NDI.

There is also a class of trusted (security-enforcing) products designed specifically for networks, such as trusted network components. The Verdex VSLAN is an example of such a network product. In addition to “traditional” trusted system products, VSLAN provides an NTCB (network trusted computing base) that supports “trusted” interconnectivity between user systems. This interconnectivity should comply with a defined security policy. The VSLAN network component performs access control, identification, authentication, and audit. Other security-enforcing products can be used with VSLAN, such as the AT&T System V/MLS (Multilevel Security).

Products are developed for some generalized environment that the vendor selects based on market research, prior experience, and other business factors. With respect to security, products are designed to withstand generic threats. Standardization bodies or government agencies help formulate generic environments when they publish evaluation criteria such as the Trusted Computer System Evaluation Criteria (TCSEC) [DOD85] and the Information Technology Security Evaluation Criteria (ITSEC) [ITSE91].

The developer may have a general conceptual target, such as “a large insurance company.” In general, the user (an individual person or an organization) who purchases a product must make sure that product is

suitable for the actual environment in which it will be used. There are various ways for the user to increase the probability that the product is suitable for its intended purpose, but that is outside the scope of this discussion.

**What are systems?** In contrast to products, systems are designed and built for the needs of a specific user community. A system has a unique operational environment because the real-world environment can be defined and observed. The security threats are real-world threats. The user performs a risk analysis or takes some equivalent action to determine which threats are to be met with countermeasures. The strength and assurance of countermeasures are likewise selected by the user.

A system may consist of a single product, but more likely a system will be built by assembling products. The system integrator is responsible for making sure that the subsystems work together, from both functional and security viewpoints.

The integration of trusted products into systems is nontrivial. The security policies and mechanisms of the individual subsystems must be made compatible and consistent for the entire system to meet its security objectives. One way of expressing this requirement is to say a system must have a security architecture and design.

While the TCSEC introduced the distinction between products and systems, this distinction has not received much attention. When the TCSEC was used as the criteria for evaluating systems, such as SACDIN and Blacker, it was necessary to redefine the criteria for the system context. The TCSEC also anticipated issues such as identifying the TCB boundary when a trusted computer is embedded in a larger system.

Different practices and regulations have evolved in the US for the evaluation of products and systems. In contrast, the developers of the ITSEC saw a similarity that they attempted to take advantage of by introducing a generic term for both systems and products: target of evaluation (TOE). The intent was to apply the same evaluation criteria to both products and systems as far as possible. We will use the term TOE in our discussion.

## **Evaluation**

Evaluation of the technical security capabilities of the TOE is performed to confirm the claims made about it. The function of independent evaluation is to assess the merit of the assertions about the TOE's security characteristics. These assertions may be stated in terms of conformance to published standards, criteria, or procurement specifications; or may simply be statements describing the TOE's security characteristics.

Security requirements are technically complex; they are not well or widely understood. Requirements and interpretations change. There are many requirements that are not susceptible to objective measurement so that repeated tests would yield the same result. Rather, these requirements call for subjective decisions by security subject area experts. Procedures are used to enhance consistency, but human variation cannot be eliminated.

Chronologically, the first independent evaluation function was provided by the National Computer Security Center (NCSC) at the National Security Agency (NSA). These evaluations focused on the NCSC objective of building up an Evaluated Products List (EPL). On a few occasions, NSA assisted in system evaluations in support of what is called certification and accreditation (C&A) in US usage.

NCSC product evaluations are performed primarily at government expense. There is no transfer of funds between the vendor and the NCSC. The NCSC and the vendor each pay the salaries and incidental expenses of their own employees.

At the time of writing, the European Community is developing the ITSEC and related evaluation policy and working with the US and Canada in the joint development of a draft CC. The UK has published an approach to evaluations that is probably applicable to the entire EC. Commercial licensed evaluation facilities (CLEFs) will be designated as approved organizations to confirm vendor security assertions and claims. CLEFs will be commercial organizations, operating on a fee-for-service basis. Although CLEFs may be independent business entities, it is more likely that they will be parts of larger organizations. There will be safeguards to enforce a CLEF's independence from influence from the parent organization. The CLEFs will evaluate both products and systems, their fees being paid by the sponsor of the evaluation, who is usually the manufacturer or vendor of a product or the user of a system. The results of an evaluation are reviewed and approved by a government certification body.

Note the difference in use of "certify" in US and EC usage. In the EC case, certification applies to the thoroughness and impartiality of the CLEF's evaluation process. In the US, certification generally is the technical evaluation of the IT security features for a system. After certification is complete, accreditation is the managerial approval or disapproval of the system. Table 1 illustrates the US and EC approaches to evaluation.

Some organizations may perform their own evaluations — at least until CLEFs get established and perhaps even after that, depending on the answers to the following questions: Will commercial fee-for-service evaluators have a conflict of interest? Some people are skeptical about whether CLEFs will be able to maintain their independence and protect the sponsor's and vendor's proprietary interests. There are also ques-

tions about the cost-benefit trade-offs of a user organization using a CLEF as compared with performing its own evaluations.

**Table 1. Evaluation schemes compared.**

<b>Where</b>	<b>US</b>	<b>EC</b>
Criteria	TCSEC, TNI, TDI	ITSEC
Product evaluation	NCSC, EPL (government)	Licensed laboratory
System evaluation	Purchaser	(Government review)
Direct cost	Government purchaser	Vendor
International evaluation acceptance	Canada, Australia, New Zealand	Not in EC

**Key**

- TCSEC: Trusted Computer System Evaluation Criteria
- TNI: Trusted Network Interpretation of TCSEC
- TDI: Trusted Database Interpretation of TCSEC
- ITSEC: Information Technology Security Evaluation Criteria
- EC: European Community
- NCSC: National Computer Security Center
- EPL: Evaluated Products List

**Scope: Type of system**

Operating systems were the first concern of computer security. All of the research leading up to publication of the TCSEC was concerned with the technology of the 1970s, namely time-sharing operating systems. In fact, many of the mechanisms used to separate time-shared users are still in use today.

It is no longer sufficient to evaluate only operating systems. In the late 1980s and the early 1990s, the NCSC produced interpretations of the TCSEC for computer networks, the Trusted Network Interpretation (TNI), and for database management systems, the Trusted Database Interpretation (TDI). These interpretations recognized several advances in information technology (IT). Very few computer systems were sold without a communications capability. Point-to-point communications, the secu-

rity of which was previously treated as communications security, were being replaced by computer networks.

The utility of computers continues to be enhanced by major applications and utilities, such as database management systems (DBMS). Networks and DBMS are considerably different from operating systems; they usually have their own security functionality in addition to the operating system. In producing the TNI and TDI, the NCSC took the position that the TCSEC contained the basic principles of information security and interpreted these principles for networks and DBMS.

## **US evaluation approach**

In the US during the 1980s, the NCSC saw its primary mission as encouraging the commercial availability of trusted products. This is often expressed as “populating the Evaluated Products List (EPL).” NCSC conducted product evaluations that concentrated on commercial off-the-shelf products.

As mentioned, the evaluation of systems in the United States is termed system certification and accreditation. NSA occasionally participated in such system evaluations, but the responsibility typically rests with the organization procuring the system. Evaluations are conducted by the government at its expense. Vendors incur expenses, of course, in preparing for evaluations and providing training and evidence to the government evaluators.

The NCSC product evaluation process determines whether a commercial off-the-shelf product satisfies the TCSEC. The evaluation may be assisted by an interpretation such as the TNI. The primary goal is to encourage widespread availability of trusted computer systems. Evaluation is focused on technical evaluation of protection capabilities.

The NCSC product evaluation phases are evolving. These phases start with the *proposal phase*, during which the government checks for majority foreign ownership, performs market analysis to determine product viability, and issues a preliminary technical assessment (PTA). In the vendor assistance phase (VAP), two evaluators are assigned, with the major responsibility to make sure that the vendor understands the requirements. During the VAP, the rating maintenance phase (RAMP) is developed to provide for the continuation of the trust rating as product updates are released. RAMP is being expanded in scope to include the categories C2 through A1. The design analysis phase (DAP) begins one year before scheduled beta testing. Several evaluators are assigned, and an initial product assessment report (IPAR) is produced and reviewed by a technical review board (TRB). Product design is frozen and a beta test begins. The culmination is the *formal evaluation phase*, including formal testing, a final report drafted by the evaluation team and reviewed by

the TRB, and the product rating on the EPL. If the vendor is unresponsive at any phase, the company returns to the proposal phase.

Technical system certification consists of a technical evaluation of a system's security features as part of the approval, acceptance, and accreditation process. This process is necessary to establish the extent to which system design and implementation meet a set of specified security requirements. Hardware, firmware, system software, applications software, communications equipment, and the operational facility must be configured, evaluated, and tested. To ensure objectivity, evaluations are performed by technical personnel independent of the development organization. Evaluation results in a statement identifying whether system security requirements are met. This statement lists problems and suggests solutions (if known), describes all known remaining vulnerabilities, and advises the Accreditor relative to the accreditation decision in a Certification Report of Findings submitted to the Accreditor.

The certification analysis includes the results of security test and evaluation. Certification is the technical evaluation of a system's security features — part of and in support of the approval/accreditation process to establish the extent to which a particular system's design and implementation meet a set of specified security requirements. Accreditation is the managerial authorization and approval granted to an ADP (automated data processing) or computer system or network to process sensitive data in an operational environment. Management needs to decide whether to operate a system or network using specific safeguards, against a defined threat, at an acceptable level of risk, under a stated operational concept, with stated interconnections, in a specific operational environment, with a specific security mode of operation.

Accrediting officials are agency officials or corporate management who have authority to accept or reject a system's security safeguards and issue an accreditation statement documenting their decision. They must also have authority to allocate resources to achieve acceptable security and to remedy security deficiencies. The ultimate responsibility for system security rests with the Accreditor. Systems must be accredited before they process or use sensitive or classified information unless a written waiver is granted by the Accreditor. The Accreditor must trade off technical shortcomings against operational necessity and may determine that it is preferable to accept a residual security risk rather than preclude mission-critical functions.

Considering all the responsibility and authority vested in the Accreditor, it is prudent for the Accreditor to be involved in system design decisions. The management practice of "no surprises" suggests that the Accreditor be at least informed and preferably allowed to participate in important decisions to be knowledgeable about the system when accreditation time arrives.

## **UK evaluation approach**

At the time of writing, the EC is developing instructions for evaluation conducted against the ITSEC and, as mentioned, participating in the development of the CC. We believe that the UK information technology (IT) security evaluation scheme is a valid model for the EC scheme. The UK IT security evaluation and certification scheme establishes a UK Certification Body to

1. certify results of evaluations to common technical standards,
2. monitor all evaluations,
3. approve all proposed evaluations, and
4. deal with other nations on mutual recognition of certificates.

The objective is to offer evaluation services to industry and government so that vendors can demonstrate security claims of products, and users can be satisfied that security objectives are met by systems.

Government supervision is jointly provided by the Communications Electronics Security Group (CESG) of the Government Communications Headquarters (GCHQ) and the Department of Trade and Industry (DTI). Evaluations are conducted by commercial licensed evaluation facilities (CLEFs) and performed in accordance with the ITSEC against an explicit security target. A product target is a list of claims made by the vendor. These may be predefined targets included in the ITSEC or may be the capabilities of the product selected by the vendor as based on a marketing decision. A system target depends on the real-world applications environment. The Certification Body cannot assess completeness or accuracy of a system target; the fitness for purpose is determined by the sponsor of the evaluation, the user in this case. When the user is a UK government agency processing classified information, the CESG acts as the National Technical Security Authority advising government and contractors on national minimum standards for protection of classified information. This role is independent of the scheme.

Evaluations are conducted by an evaluation facility on behalf of the sponsor, who commissions and pays for the evaluation, and receives the evaluation and certification reports. The developer may be separate from the sponsor. For example, a contractor who is the developer normally must assist in the evaluation. The deliverables required for evaluation are normally the property of the developer. The deliverables include hardware, firmware, and software documentation, technical support, and access to the development facility. The developer may wish to limit the sponsor's access to proprietary information.

The sponsor determines the security target, which defines the security functions of the TOE, may describe threats or security mechanisms, and includes the evaluation level desired, specified in ITSEC terms. It is

the sponsor's responsibility to determine the security target, which may derive from the sponsor's circumstances, may be a marketing decision, and/or may be required by law or corporate policy. The CLEF reviews the security target, prepares an evaluation work plan, and obtains the Certification Body approval. The development and evaluation process is illustrated in Figure 1.

**Figure 1. Development and evaluation process.**

US and EC evaluations are based on factors that are both similar and different. Furthermore, the factors described in the ITSEC have yet to stand the test of use over time. It is reasonable to anticipate that the interpretation of the ITSEC factors will undergo further refinement and gradually move toward aspects of the evolving CC. The best we can do today is present the two sets of factors so that you can compare them.

## US evaluation criteria factors

The NCSC “rainbow series” creates a set of common factors affecting the evaluation process, which differ, in part, from the ITSEC factors. In this section we will examine these sets of factors. Keep in mind that US practice will change as the draft FC is revised to move toward the evolving CC.

The US NCSC criteria are divided into three groups: functionality, strength of mechanism, and assurance.

Functionality is the objective and approach of a security service, including features, mechanism, and performance. Alternative approaches for providing specified functionality may be more suitable in different applications environments.

Strength of mechanism refers to how well a specific approach may be expected to achieve its objectives. Selection of parameters can significantly affect strength of mechanism. For example, the number of bits used in a checksum or the number of permutations used in an encryption algorithm may directly influence the strength of mechanism. For inadvertent threats, strength of mechanism refers to the ability to operate correctly after natural disasters, emergencies, operator errors, and accidents. This is particularly critical for prevention of denial of service as a consequence of inadvertent threats. For deliberate attack, strength of mechanism refers to the ability to resist that attack. Since a skillful attacker can make the attack look like an inadvertent threat, it is usually not useful to distinguish among the causes of threats.

Assurance refers to the basis for believing that the functionality will be achieved, including tamper resistance, verifiability, and resistance to circumvention or bypass. Assurance is generally based on analysis involving theory, testing, software engineering, and validation and verification. The analysis may be formal or informal, where formal implies mathematical techniques, such as those discussed in Essay 8.

When considering communications, the TNI provides additional definitions concerning strength of mechanism, which it considers a metric of how well a specific approach may be expected to achieve its objectives. The evaluating ratings available are none, minimum, fair, and good. Mechanisms that only protect against accident and malfunction are rated as minimum. Mechanisms must provide protection against deliberate attack to be rated as good. Criteria are specified for each security service. The TNI Environments Guideline (TNI EG) additionally recommends that inadvertent threats and malicious threats be analyzed separately; traditional risk management techniques are applicable only to inadvertent threats. The TNI EG suggests that malicious threats may dominate inadvertent threats and that malicious users can often duplicate circumstances of inadvertent threats.

In the TCSEC and all other “rainbow” documents and NCSC policy, the trusted computing base (TCB) is a very important concept. The network TCB (NTCB) is introduced in the TNI as a generalization of the TCB for a stand-alone computer. The NTCB reduces the risk of unauthorized modification to objects within a network system by maintaining the integrity of programs that provide security services. In the TCSEC, security services support confidentiality and accountability. In particular, the implementation of one security service can be prevented from degrading assurance of other services. This ensures that protection provided by one security service is not diluted by other security services.

The security services listed in Part II of the TNI are authentication, communications integrity, nonrepudiation, continuity of operations, protocol-based protection, network management, data confidentiality, traffic flow confidentiality, and selective routing. The assurance of these security services described in Part II of the TNI is related to the TCSEC operating system assurance included in Part I of the TNI. This is because a security service depends on the NTCB to protect it from unauthorized modification. It is very appealing, but wrong, to think that you can increase the assurance level of a network by adding security services. You can add functionality, but the assurance of this added functionality has an upper limit in the assurance of the NTCB. Even if the added security services are developed at a very high level of assurance, when installed in a real system the assurance can be no higher than that provided by the NTCB. This is analogous to saying that a chain is no stronger than its weakest link.

Some security services are strongly dependent on the computers in the network and can be directly evaluated under Part I and Appendix A of the TNI. Appendix A was written to support the evaluation of components and subsystems. Note that the TNI was a little imprecise in its definitions and has been corrected in the TNIEG as follows:

A component is an individual physical unit that does not provide a complete set of end-user services. A system or subsystem is a collection of hardware, firmware, and software necessary [and] configured to collect, create, communicate, disseminate, process, store, and/or control data and information.

The recursive definition of the overall network security policy is discussed in Essays 2, 6, and 7.

The required strength of mechanism is determined using a risk index only slightly different from that used in the Yellow Book or DoD Directive (DODD) 5200.28 for stand-alone computer systems. The risk index computation takes the difference between the maximum data sensitivity,  $R_{\max}$ , and the lowest clearance of a user who can gain physical access to some system device,  $R_{\min}$ . Note that there is a difference from a

Yellow Book risk index calculation, where the lowest cleared user is of concern; but that lowest cleared user includes indirect access, as discussed in Essay 2. This network risk index must also consider the most sensitive information in the network.

The general case is  $R_{\min} < R_{\max}$ , in which case

$$\text{Risk Index} = R_{\max} - R_{\min}$$

In the special case  $R_{\max} \geq R_{\min}$ , if there are any categories in the system to which some users are not authorized access

$$\text{Risk Index} = 1$$

otherwise

$$\text{Risk Index} = 0$$

The rating scale for maximum data sensitivity is given in Table 2.

**Table 2. Rating scale for maximum data sensitivity. Risk Index =  $R_{\max} - R_{\min}$ .**

$R_{\max}$ without Categories	Rating	$R_{\max}$ with Categories	Rating
U	0		
N	1		2
C	2		3
S	3	1 category in S	4
		>1 category in S	5
TS	5	1 category in S or TS	6
		>1 category in S or TS	7

**Table 3. Rating scale for minimum user clearance.**

Minimum User Clearance	Rating
U — Uncleared	0
N — Access to Sensitive Unclassified	1

C — Confidential	2
S — Secret	3
TS — Top Secret with Background Investigation (BI)	4
SBI — TS with Special Background Investigation	5
1 Category	6
>1 Category	7

The rating scale for minimum user clearance is given in Table 3. Note, however, that the two different background investigations have been recently abolished. No guidance has been issued on how this risk index calculation specified in DODD 5200.28 should be amended.

The operating modes are the same for networks and stand-alone operating systems; they indicate how much trust is placed in technical security by specifying who may use the network. Briefly, the modes are identified as follows: A **dedicated** network is exclusively used for one classification. In **system high** mode, the entire network is operated at, and all users are cleared to, the highest sensitivity level of information stored (historic definition). In a **partitioned** network, all personnel have clearance, but not necessarily formal access approval and need-to-know, for all information. A **multilevel** network has two or more classification levels, and not all users have clearance or formal access approval for all data.

The TNI/TNIEG security metrics include the security riskindex, the evaluation structure for network security services, the minimum strength of mechanism requirement, the minimum assurance requirements, and the TNI Part II security service assurance rating. Table 4 shows the relationships among risk index, security mode, and minimum security class.

**Table 4. Risk index, security mode, and minimum security class.**

<b>Risk Index</b>	<b>Security Mode</b>	<b>Minimum Security Class</b>
0	Dedicated	No minimum class
0	System high	C2
1	Multilevel, partitioned	B1
2	Multilevel, partitioned	B2
3	Multilevel	B3

4	Multilevel	A1
5-7	Multilevel	*

\* Beyond current state of computer security technology.

**Table 5. Evaluation structure for network security services.**

<b>Network Security Service</b>	<b>Criterion</b>	<b>Evaluation Range</b>
Communications integrity Authentication	Functionality Strength Assurance	None   present None-good None-good
Communications field integrity	Functionality Strength Assurance	None-good None-good None-good
Nonrepudiation	Functionality Strength Assurance	None   present None-good None-good
Denial of service Continuity of operations	Functionality Strength Assurance	None-good None-good None-good
Protocol-based protection	Functionality Strength Assurance	None-good None-good None-good
Network management	Functionality Strength Assurance	None-good None-good None-good
Compromise protection Data confidentiality	Functionality Strength	None   present Sensitivity level

	Assurance	None-good
Traffic flow confidentiality	Functionality Strength Assurance	None   present Sensitivity level None-good
Selective routing	Functionality Strength Assurance	None   present None-good None-good

Table 5 shows the evaluation structure for network security services, Table 6 the TNI minimum strength of mechanism requirements and the assurance ratings for networks, and Table 7 the dependence of the TNI Part II assurance on the assurance of the NTCB.

**Table 6. Minimum strength of mechanism and assurance requirements.**

<b>Risk Index</b>	<b>Strength of Mechanism</b>	<b>Part II Assurance Rating</b>
0	None	None
1	Minimum	Minimum
2	Fair	Fair
>2	Good	Good

**Table 7. Parts I and II assurance dependence.**

<b>Part II Assurance Rating</b>	<b>Minimum Part I Evaluation</b>
Minimum	C1
Fair	C2
Good	C3

### **ITSEC evaluation factors**

Under the ITSEC, the evaluation factors are functionality, correctness, and effectiveness. Functionality refers to the security functions (for example, access control, auditing, and error recovery), which may be individu-

ally specified or referenced by predefined functionality class. There are three levels of abstraction:

- **Objectives.** Why the functionality is wanted; the contribution to security.
- **Enforcing functions.** What functionality is actually provided; the features of the TOE that contribute to security.
- **Mechanisms.** How the functionality is provided; the logic or algorithm that implements a particular function.

The ITSEC requirements for functionality mandate the existence of a security target consisting of:

1. a system security policy or a product rationale,
2. a specification of the required security-enforcing functions,
3. an optional definition of required security mechanisms,
4. the claimed rating of the minimum strength of mechanism, and
5. the target evaluation level.

The following generic headings are recommended for specification of the security target:

1. identification and authentication,
2. access control,
3. accountability,
4. audit,
5. object reuse,
6. accuracy,
7. reliability of service, and
8. data exchange.

The ITSEC provides 10 predefined functionality classes that can be used as the basis for individual system and producer security targets, or can be used as guidelines to assist users in selecting appropriate security functionality for their environment or to help vendors configure their products. The first five predefined functionality classes are designed for close correspondence with the functionality requirements of the TCSEC classes. For easy reference, these classes are identified as F-C1, F-C2, F-B1, F-B2, and F-B3. Remember that the TCSEC classes B3 and A1 differ in assurance, not functionality.

The predefined functionality class F-IN is for targets with high integrity requirements for data and programs; databases are identified as a possible application. The predefined functionality class F-AV is for targets with high availability requirements, such as manufacturing process control computers. The predefined functionality class F-DI sets high re-

quirements for safeguarding data integrity during communications. The predefined functionality class F-DC sets high requirements for data confidentiality during communication; this requirement might apply to cryptographic devices. The predefined functionality class F-DX is intended for networks with high demands for both confidentiality and integrity of communication. For example, public networks may require F-DX functionality for the transmission of sensitive information via insecure networks.

The ITSEC does not prescribe the particular methods or styles for the specification of security functions. Three styles are identified in the ITSEC: informal, written in a natural language with the aim of minimizing ambiguity; semiformal, using a graphical or restricted natural language presentation; and formal, written in a formal notation according to mathematical concepts of syntax, semantics, notation, proof rules, and logical reasoning.

The ITSEC requirements for assurance of **effectiveness** are based on the proposed use of the TOE as described in its security target. The assessment of effectiveness involves consideration of:

- suitability of the TOE's security functionality to counter identified threats specified in its security target;
- whether individual security functions and mechanisms of the TOE bind together in a way that is mutually supportive and provides an integrated and effective whole;
- the ability of security mechanisms to withstand direct attack;
- whether known security vulnerabilities in construction and operation of the TOE could, in practice, compromise security; and
- whether the TOE can be configured or used in a manner that is insecure but which an administrator or end user of the TOE would reasonably believe to be secure.

The ITSEC strength of mechanism evaluation applies to all critical mechanisms whose failure would create a security weakness; these mechanisms are assessed for their ability to withstand direct attack. A **basic** rating means that all critical mechanisms provide protection against random accidental subversion, although knowledgeable attackers may be able to defeat them. A **medium** rating means that critical mechanisms provide protection against attackers with limited opportunities or resources. A **high** rating means that all critical mechanisms could be defeated only by attackers possessing a high level of expertise, opportunity, and resources, and successful attack is judged to be beyond normal practicality.

A TOE will fail evaluation only on effectiveness grounds and receive an overall evaluation level of E0, if an exploitable vulnerability found during evaluation is not eliminated before the end of evaluation.

The ITSEC requirements for assurance of correctness are expressed in seven hierarchical levels; E0 is the lowest and E6 the highest:

- E0 Inadequate assurance.
- E1 There is a security target and an informal description of the TOE security architecture, and functional testing indicates that the TOE satisfies its security target.
- E2 (beyond E1 requirements) There is an informal description of the detailed design; evidence of functional testing is evaluated; there is a configuration control system and approved distribution procedure.
- E3 (beyond E2) The source code and/or hardware drawings for the security mechanisms are evaluated; evidence of testing these mechanisms is evaluated.
- E4 (beyond E3) There is a formal model of the security policy; security-enforcing functions, architectural design, and detailed design are specified in a semiformal style.
- E5 (beyond E4) Close correspondence exists between detailed design and source code and/or hardware drawings.
- E6 (beyond E5) Security-enforcing functions and architectural design are specified in a formal style consistent with the formal model of policy.

The rating awarded to a TOE consists of a reference to the TOE security target, the assurance evaluation level for correctness and effectiveness, and the strength of mechanism rating. A TOE rated E0 is not rated on strength of mechanism.

### **Issues for consideration**

This discussion of the US and EC approaches to criteria and evaluation raises certain issues that have been considered for the draft US FC and the evolving CC, including:

1. bundling of evaluation criteria factors,
2. ITSEC/TCSEC relationship and implications,
3. conceptual ITSEC issues,
4. implications of the ITSEC on the US computer industry,
5. whether criteria should prescribe policy,
6. evaluation by parts, and
7. a proposal for a US Information Security Foundation (ISF).

The TCSEC, TNI Part I, and TDI bundle (predetermine) functionality, strength of mechanism, and assurance; the TNI and ITSEC separately evaluate security factors. The claimed advantages of bundling are that fewer evaluation points simplify choices for vendors and users, and that these evaluation points provide government guidance. Having a limited number of security targets was quite important in the start-up phases of computer security in that the TCSEC provided indirect guidance to purchasers as well as vendors. However, the TCSEC was written by DoD for the defense sector; it is not necessarily applicable, without interpretation, to civil government and commercial applications. The draft FC introduced the Protection Profile, which specifies security aspects of an IT product.

The claimed advantages of unbundling are that there are fewer targets for vendors who are more free to offer products determined by market factors, and that it is easier for users to select systems. But many consumers are unsophisticated with regard to applying security evaluation criteria. These consumers do not know what they need, and they do not understand the IT security state of the art. Similarly, vendors may not understand the consumer's IT security needs. The flexible TOE claims structure permits an accurate representation of the TOE's capabilities, but excessive flexibility could lead to confusion.

The ITSEC is policy neutral; it is directed only at the evaluation of security targets. It leaves the policy to be defined externally. The TCSEC, in comparison, has US DoD confidentiality policy woven through it and has been interpreted to also apply to one form of integrity policy. Nevertheless, the ITSEC has included explicit measures for compatibility with the TCSEC by its definitions of the predefined functionality classes (F-C1, F-C2, F-B1, F-B2, and F-B3). The decision to make the ITSEC independent of a specific security policy leaves a void with respect to policy guidance. There is a need for supplementary guidance on the relationship between functionality and assurance requirements. Users could use guidance concerning the assurance required by each security mechanism.

Purchasers and users who are not experts need policy guidance from central policy-making government agencies, and from professional, legal, and ethical organizations and experts. A possible solution is to rely on the civil and defense establishments to make government security policy, and professional boards and societies to recommend commercial security policy. Perhaps the framers of the ITSEC intended such guidance to come into existence. The international CC developments may serve as a catalyst in this process.

The ITSEC effectiveness requirements, coupled with architectural and design constraints, correspond to the TCSEC concept of a trusted computing base. When combined with the appropriate effectiveness rating, a product meeting the ITSEC class should meet the corresponding

TCSEC class. The reverse is not true, due to wider requirements in the ITSEC. Table 8 shows the intended correspondence.

The ability to configure products to satisfy TCSEC and ITSEC requirements does not solve all the problems. As long as the criteria are subject to separate interpretations by national bodies, there is no guarantee that evaluations in one country will be accepted in another country. Reciprocity is being tested by several vendors who are seeking multinational security evaluations for their products. This process could be facilitated as international agreements are developed that are based on the evolving CC.

**Table 8. Intended correspondence between ITSEC and TCSEC classes.**

<b>ITSEC Classes</b>	<b>TCSEC Classes</b>
E0	D
F-C1, E1	C1
F-C2, E2	C2
F-B1, E3	B1
F-B2, E4	B2
F-B3, E5	B3
F-B3, E6	A1

Compatibility of ITSEC predefined classes with the TCSEC is a “mixed blessing.” The TCSEC has not been updated since its publication. The rewording of the TCSEC functional requirements is quite laudable. Unfortunately, well-known “defects” in the TCSEC are propagated. There is an opportunity to make improvements in the CC process. There is debate among security practitioners concerning some of these “defects.” This healthy discussion of differences is reflected in this collection. Essay 2 takes a different position on some of these issues. Here are some TCSEC issues that could be addressed:

- The definition of DAC in the TCSEC is inadequate; it does not clearly explain what is discretionary. This is really a question of delegation of authority that could be explained much more clearly.
- The TCSEC DAC definition is so poorly worded that it permits the fundamental flaws identified in the DAC guideline [NCSC87b]. A more careful statement of transitivity and secondary delegation of authority could close or reduce these defects.

- The DAC statement concerning propagation of rights has proven to be unclear and ineffective. Here is an opportunity to be more effective and explicit.
- It is now understood that DAC is an example of an identity-based access control (IBAC). There are other stronger IBAC, such as ORCON (Organization Control), defined in DCID 1/7. In fact, these IBAC are nondiscretionary; there is disagreement among researchers about whether ORCON can be implemented using the TCSEC mandatory controls. These distinctions should be made much more clear.
- Addressing only human-readable labels onto printed output is obsolete; it is a gross oversight not to include all forms of human-readable output, especially video display.

There are potential implications for the international computer industry. For example, where do international computer companies submit their trusted products for evaluation? Will existing NCSC criteria and evaluations be changed to conform to the ITSEC, the draft FC, and/or the evolving CC? What role will the US National Institute of Standards and Technology (NIST) play in the security evaluation process? What will be the transition plans? Should US evaluations use the UK evaluation scheme?

Industry representatives have expressed a need for evaluation by parts, including parts sold by different vendors or parts previously evaluated but changed or rehosted. NCSC addresses part of the problem through the Rating Maintenance Phase (RAMP) Program, NCSC-TG-013 [NCSC89a], and another part of the problem through the concept of TCB subsets in the TDI.

While it is desirable that an entire assessment does not have to be redone for every software, hardware, or firmware upgrade or error correction, it is currently not possible to determine trust characteristics of an arbitrary collection of subsystems. The TDI may answer some of the evaluation requirements, if use of the TDI successfully provides: (1) a clear description of parts considered for separate evaluation, (2) a clear description of conditions for evaluation by parts, and (3) an interpretation of evaluation criteria for evaluation by parts.