The Security Management Challenge: *Bounding a Moving Target*

- Building and Maintaining Security Infrastructures
- Managing "Security Gaps"
- Security Planning
  - Support both IT Vision and Security Policies
  - Marketplace dependence
  - Best Value Solutions

Role of Security Standards

- Support Management Process for New IT Services(?)
  - Business case for IT Investment
  - Cost Containment Strategies
- Requirements and specifications
- Equivalence and Interoperability
- Voluntary consensus vs "de facto"
- Limited operational practices context
- Compliance assurances

Standards Development Process

- Business need driven
- Scope – within a business context
- Balanced participation
  - open to buyers and sellers of technology as well as technology experts
- Document requirements/specifications
- Voting process for consensus and resolving disagreements
- Public comment

What is the Common Criteria

- International Standard Meta-language for describing IT security requirements
  - Features and assurances
  - Supports both buyer "I need" and Seller "I provide"
- How "one applies" the Meta language is:
  - Constituent (Seller or Buyer) dependent
- Security Management Tool

Infrastructure Support for Common Criteria

- International Registry of Buyer and Seller requirements
- Assurances Laboratories for both Buyer and Seller
- International Mutual Acceptance of Features and Assurances

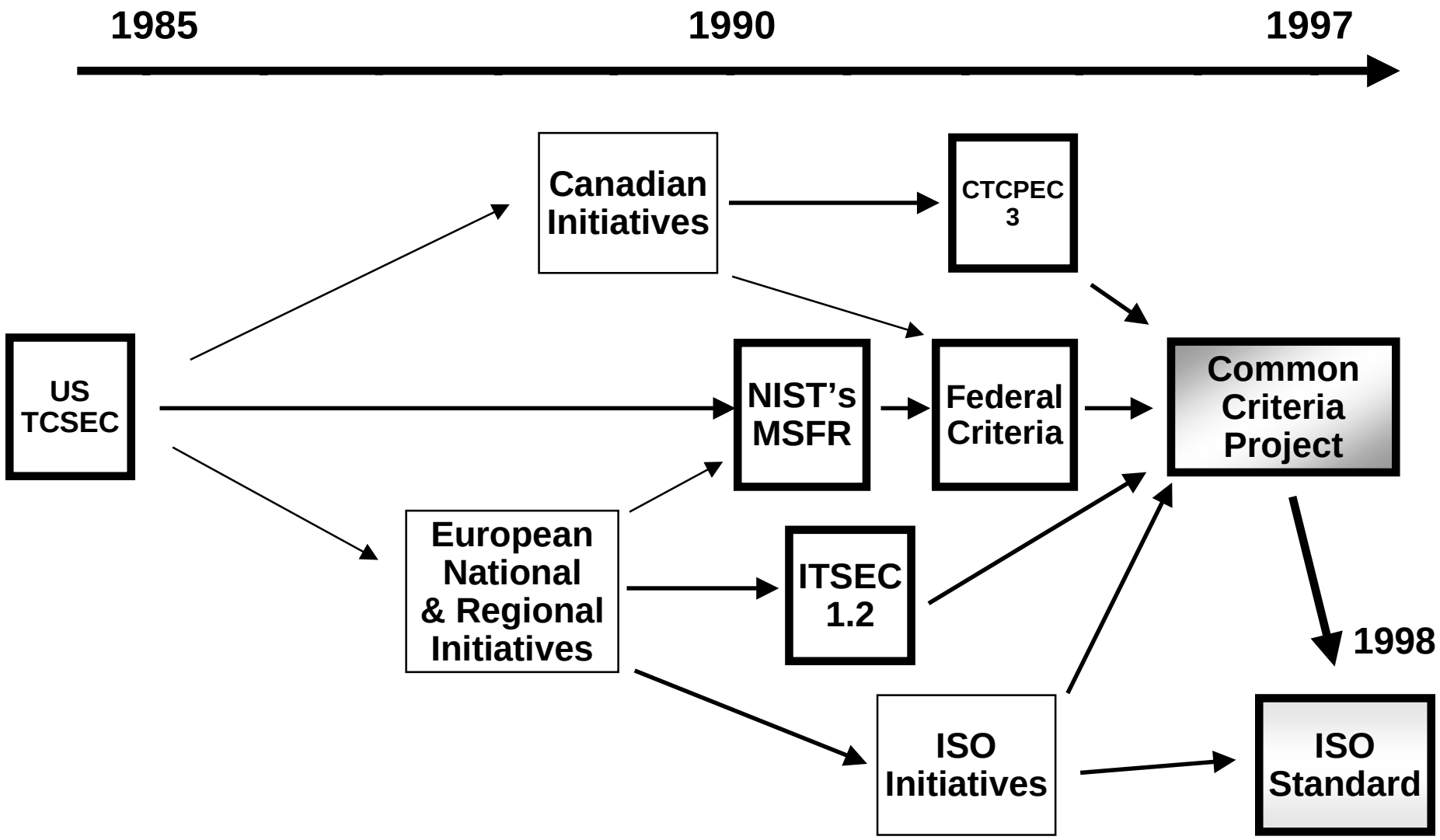
Common Criteria Potential Benefits

- Better Tool to Bound problem(s)
  - More accurate definition of requirements
  - Threat and policy
  - IT and Non-IT assumptions
  - Interoperability and equivalence
  - Features and Assurances

Common Criteria
Potential Benefits (cont.)

- Market friendlier
- Friendlier to integrating both established and emerging security technologies and practices
- Supports buyers IT business case development
- Supports Seller's business case to bring IT services to market

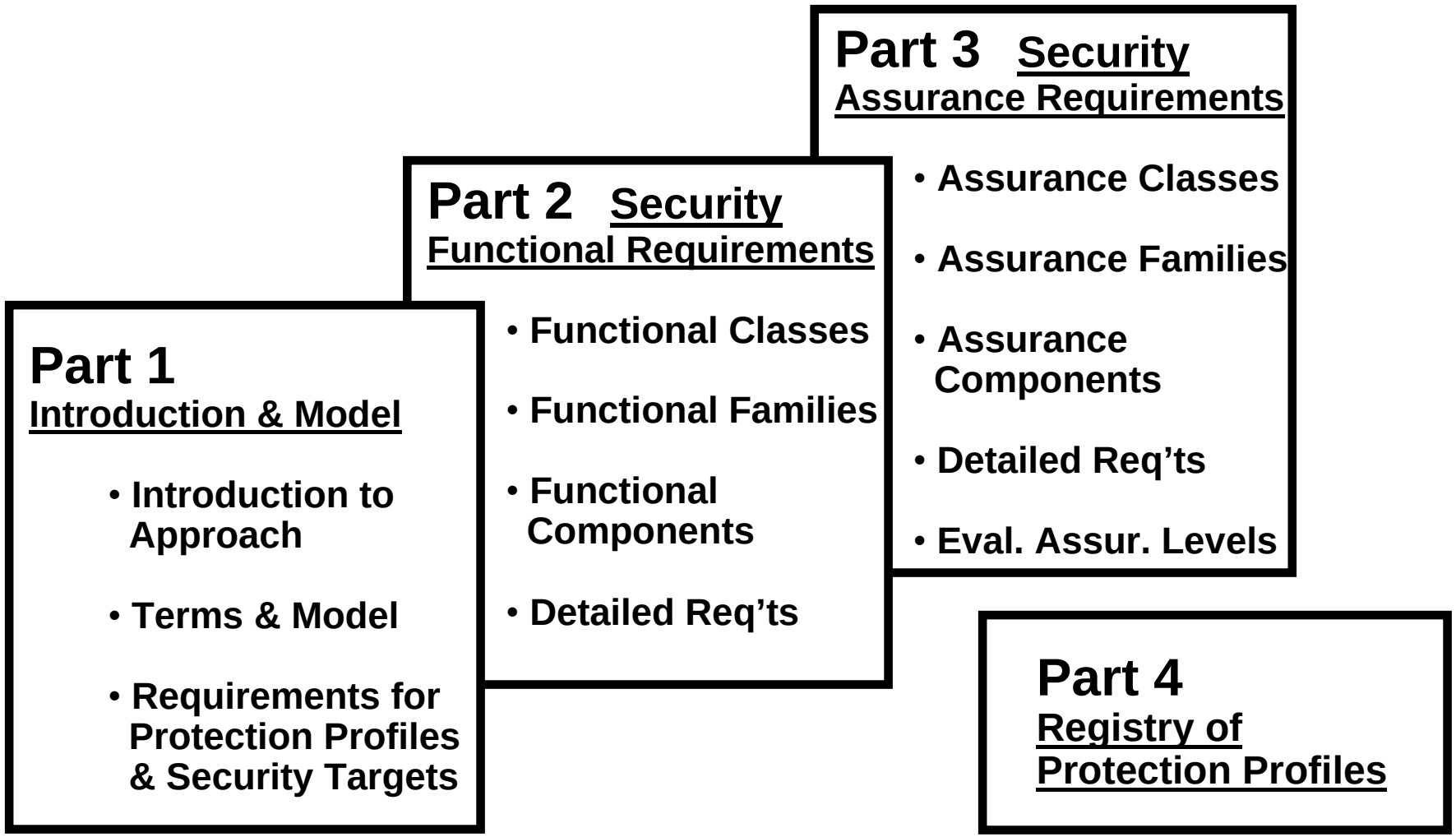
A Brief History of Common Criteria



Common Criteria as International Standard

- 1990 - Working Group 3, Subcommittee 3, Joint Technical Committee 1 begins addressing IT security
- 1993 - Member Nations pool resources and assist WG3
- Common Criteria (CC) Version 2 provided, May 1998
- CC, Version 2, as International Standard ISO/IEC 15408 being reviewed and voted upon

Overview of Common Criteria Structure



Common Criteria Look and Feel

- Official title - Common Criteria for Information Technology Security Evaluations
- Part 1, Introduction
- Part 2, Functional Requirements
  - Desired information technology security behavior

Common Criteria Look and Feel (cont.)

- Part 3, Assurance Requirements
  - Measures providing confidence that the Security Functionality is effective and correctly implemented
- CC intro at <http://csrc.nist.gov/cc/info/cc-sum/content.htm>

Functional Requirements Classes

- FAU -- Security Audit (35)
- FCO -- Communication (Non-Repudiation) (4)
- FCS -- Cryptographic Support (40)
- FDP -- User Data Protection (46)
- FIA -- Identification & Authentication (27)
- FPR -- Privacy (Anonymity, etc.) (8)
- FPT -- Protection of Trusted Security Functions (43)
- FRU -- Resource Utilization (8)
- FTA -- TOE Access (11)
- FTP -- Trusted Path (2)

Evaluation Assurance Levels

- Levels - EAL 1 through 7
  - increasing rigor and formalism from 1 up to 7
- Seven classes addressed for each level
  - Configuration Management
  - Delivery and operation
  - Development
  - Guidance documents
  - Life-cycle support
  - Testing
  - Vulnerability Assessment

Vendor/Customer Requirements

- Protection Profiles (PP)
  - User requirements ("I need")
  - Multiple implementations may satisfy
- Security Targets (ST)
  - Vendor claims ("I will provide")
  - Implementation specific
- Methodology
  - First, threats and policy stated
  - then Features and Assurances selected

CC Product Validation and Evaluation Scheme

- Targeted to begin in 1999
- Using security specifications from Common Criteria (CC)
- Procedures based upon Common Evaluation Methodology (CEM)
- Testing and evaluations performed by NVLAP accredited commercial labs
- International recognition of evaluations (Mutual Recognition)
- Results posted on NIAP's WWW page

Laboratories

- NSA's TTAP laboratories are the Interim CC labs
- ARCA Systems, BAH, COACT, CSC, Cygnacom Solutions, NSTL and SAIC
- Will have to reapply for CCEVS accreditation
- Mutual Recognition between Canada, France, Germany and UK and US for CC-based evaluations
- Netherlands are developing their scheme
- Australia and New Zealand applying

Product evaluations
As of 19 Oct. 98

- CC-based Evaluation Completed:
  - ITT Dragonfly EAL 2 Guard
  - Milkyway Black Hole V3.01 EAL3 Firewall in Canada
- CC-based Evaluations Underway
- 3 EAL2 Firewalls
  - Checkpoint
  - CISCO Pix
  - Lucent Managed Firewall

Product evaluations (cont.)

- "OS" evaluations underway:
  - IBM RS6000 - C2 OS
  - IBM NT 4.0 - C2 OS
  - IBM SQL Server - C2 DB
  - Sybase Anywhere Adaptive Server - C2 DB

Assistance

- Classes
  - schedule on web page (niap.nist.gov)
  - CC familiarization, 1 day
  - PP development, 4 days
- CC Toolbox
  - CCDA version 1, (ST), Oct. 98
  - PDA version 2, (PP), Dec. 98
  - PDA version 1, July 99
  - CCDA version 2, Jan. 00

Right Time for Common Criteria?