# Perspectives on NIAP and the Common Criteria

Stuart W. Katzke, Ph.D.
Senior Research Scientist
Computer Security Division
National Institute of Standards and Technology
skatzke@nist.gov
(301) 975-4768

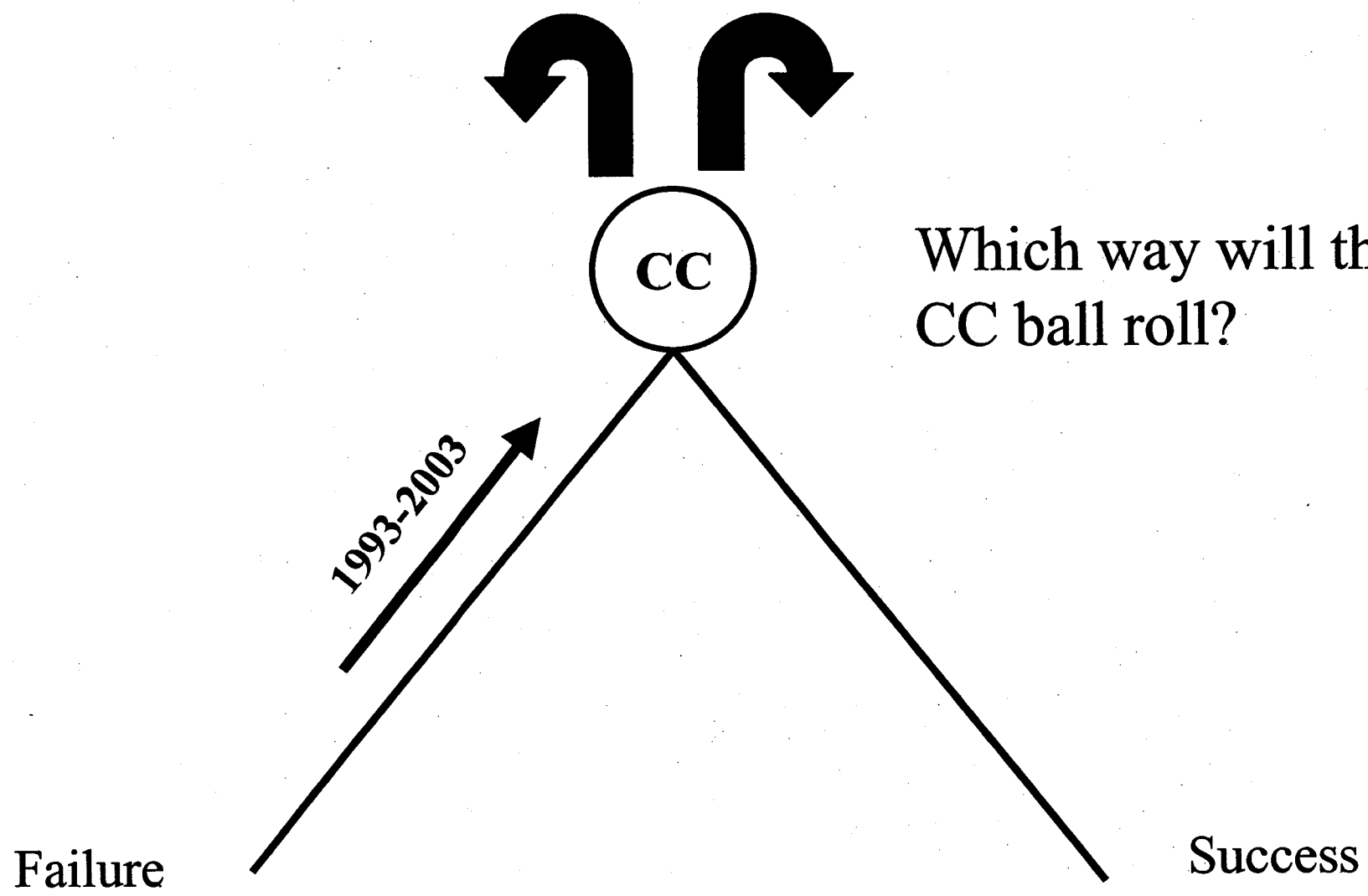
Dec 2004 - ISPAB

# Presentation Contents

- CC Paradigm
- My Impressions of ICCC5 Berlin
- Terminology
- NIST's role in CC and NIAP development
- Comments on:
  - Use of CC as a requirements definition language
  - Role/value of CC evaluations
- NIST's FISMA Implementation Project and the CC
- Recommendations on What is Needed (Broader than CC & NIAP)

# CC & NIAP Issues

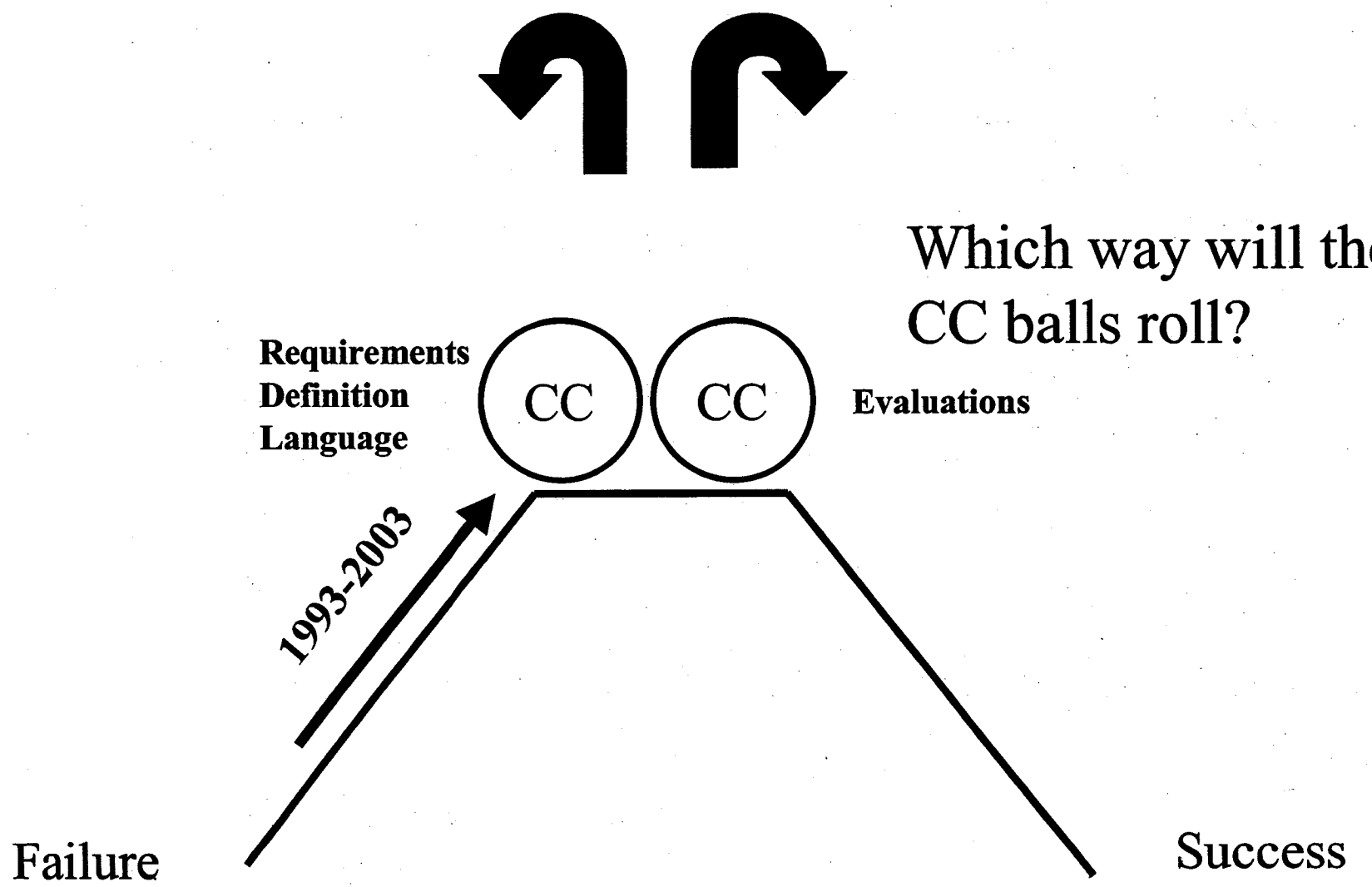
- Past & current status of CC & NIAP, including issues and concerns, well represented by NIAP/CC stakeholders in reports below & by NSA.
  - National Cyber Security Partnership's Technical Standards and Common Criteria Task Force's *Recommendations Report*, April 2004 (Hereafter referred to as the "TF Report")
  - Cyber Security Alliance's, *NIAP Certification: Proposals by CSIA for strengthening Security Certification*
  - Stu Katzke's personal opinion on: *The Common Criteria (CC) Years (1993-2008): Looking Back and Ahead* expressed at ICCC4 Stockholm, September 2003
  - NIAP Review (when completed)




Question raised by Stu Katzke at ICCC4 2003

# CC Paradigm

- International Standard (ISO/IEC 15408) is a standard security requirements definition language
  - Provides a taxonomy of functional & assurance requirements
  - STs (product specific)
  - PPs (generic product specification)
  - Functional requirements sets (e.g. BITS Functional Packages)
  - Contains predefined assurance packages EAL 1-7 (for voluntary use) that are (somewhat) map able to Orange Book assurance requirements
  - Does not define "good security requirements"
- The standard provides a basis for performing evaluations against CC-based security specifications (STs, PPs, Functional packages)
  - Evaluation activities are performed within government schemes using government accredited private labs
  - Common Evaluation Methodology (CEM) adopted by the CC Schemes as part of the CCRA to ensure comparability of evaluations across Schemes
  - CEM is not part of the standard




Question raised by Stu Katzke at ICCC4 2003
(Modified October 2004)

# ICCC5 Berlin

- Attendance
  - Joint ICCC & Information Security Solutions Europe (ISSE) Conference
  - 630 Total
  - 143 ISSE
  - 487 ICCC (upper bound)
- ICCC past attendance
  - ICCC4 Sweden: 350
  - ICCC3 Canada: 381
  - ICCC2 UK: 450
  - ICCC1 US: approx. 600

# My Impressions of ICCC5 Berlin (1)

- Many of same issues raised as those in my ICCC4 presentation. Validation of my prior concerns.
- No one said "throw it all away" (except Colin Williams, Software Box, Ltd.)
- All had constructive criticism for improvement
- Vendors:
  - Would not go through evaluation if not mandated by DoD. At EAL4 & below:
    - Most (not all) indicated that CC evaluation does not provide significant reduction in vulnerabilities
    - Most (not all) indicated that other internal (i.e., corporate) developmental activities provide better vulnerability reduction
    - A CC evaluation requires too much time be spent on audit & documentation requirements vs. true vulnerability reduction
      - Now: 50-50
      - Should be more like: 30-70 (vulnerability reduction)
  - Cost/time/value still an issue

# My Impressions of ICCC5 Berlin (2)

- Constructive criticism by:
  - Steve Lipner, Microsoft (Keynote presentation)
  - Mike Nash, Gamma Secure Systems (Simpler STs)
  - Catherine Webb (Scott Logan), IBM (IBM's experience)
  - Ray Potter, Cisco (Check box or meaningful assurance?)
  - Renaud Presty, AXALTO (smartcard area)

# My Impressions of ICCC5 Berlin (3)

- CCRA Members & Schemes
  - CCRA membership growing (2 new members; about 20 now)
  - New CCRA management structure seems to be working better; members volunteer to take on actions & committee work at their expense
  - CCRA group working more closely with ISO/IEC SC27 WG3 on CC v3.0
  - CCRA group claims to be addressing significant issues
  - TBD if things will progress faster than before

# My Impressions of ICCC5 Berlin (4)

- Governments
  - UK (Cabinet level?) establishing alternative to CC evaluation called General Information Assurance Products & Services Initiative (GIPSI)
  - Japan joined CCRA as certificate authorizing member
  - Korea applied to join CCRA as certificate authorizing member (announced at ICCC5 awards ceremony)
  - India investigating scheme establishment
  - Russia getting closer to applying for certificate authorizing membership

# My Impressions of ICCC5 Berlin (5)

- Composition/Evaluation Reuse Issue
  - Still a significant research problem
  - Excellent paper by Helmut Kurth, Atsec & Paul Karger, IBM Watson Research Center
    - Layering
    - Networked
    - Component
  - Numerous papers presented on this subject (full track)

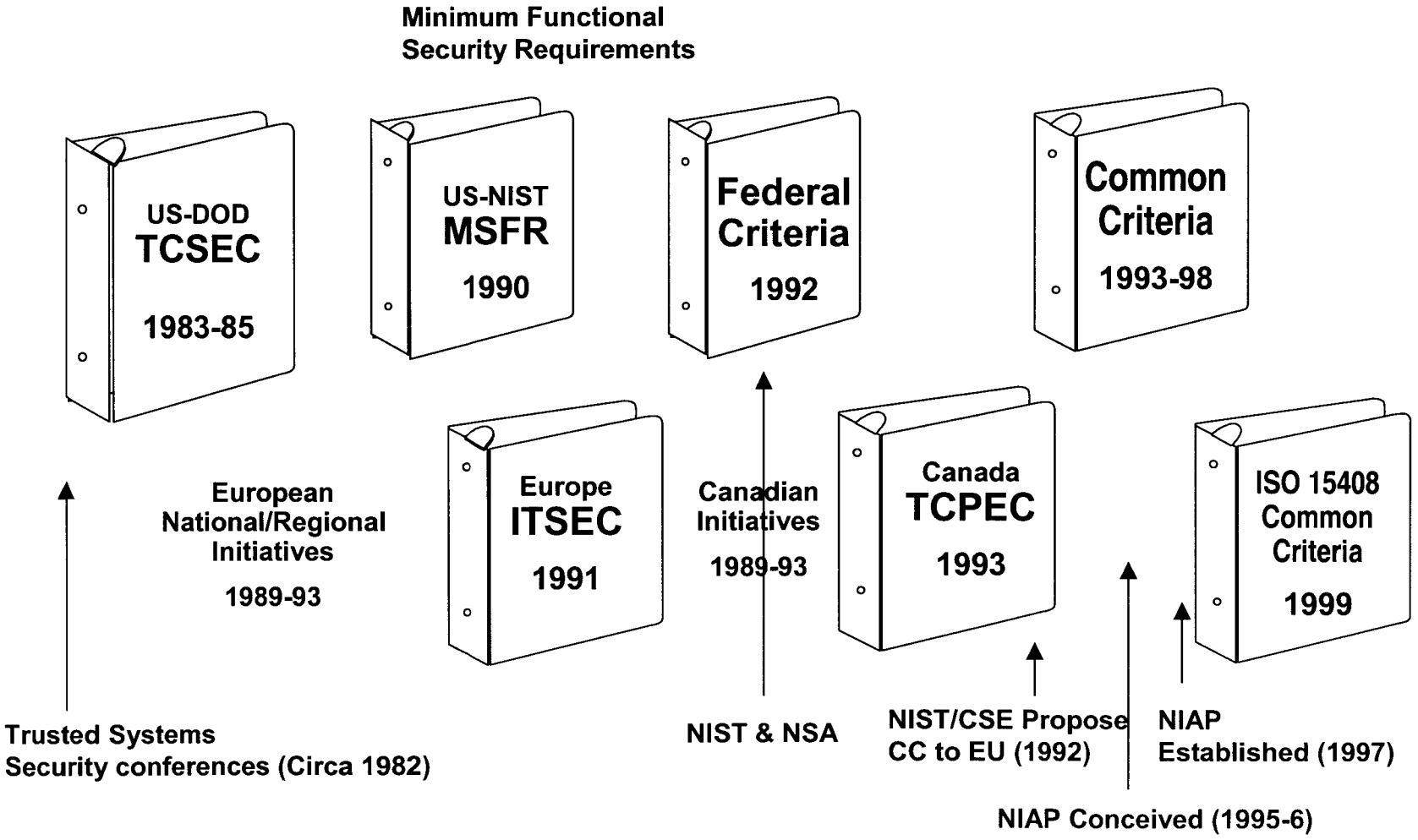
# Terminology (1)

- Certification & Accreditation used in multiple ways
- CC context
  - Oversight, review, & approval of evaluations
  - *CC Validation* in U.S.; called *CC Certification* outside U.S.
  - Approval of labs to operate within a CC scheme
  - Called *accreditation* in all schemes

# Terminology (2)

- System security context
  - *Security Certification (certification):* a comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
  - *Security Accreditation (accreditation)* : the official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations, agency assets, or individuals based on the implementation of an agreed-upon set of security controls.

# NIST's Role in CC and NIAP Development



# Use of CC as a Requirements Definition Language (1)

- TF Report:
  - Highlighted need for "market appropriate" requirements sets.
  - Recommended NIST receive $12M upfront & $6M/yr to develop consensus-based requirements sets
  - Recommended NIST develop best practices and methodologies to evaluate products against the requirements sets

# Use of CC as a Requirements Definition Language (2)

- The $12M/$6M "check" is NOT in the mail
- Anticipate obtaining funding in FY 2005 to work on a few requirements sets of 15 candidate technology areas
- Anticipate obtaining funding in FY 2005 to work on assurance packages supportive of the security impact levels of FIPS 199 & NIST SP 800-53
- Agree on need to develop tests and test methods for specific technology areas to improve efficiency and effectiveness of evaluations (not funded). Models include:
  - FIPS 140-2 Derived Testing Requirements (DTRs)
  - Smartcard testing in Europe

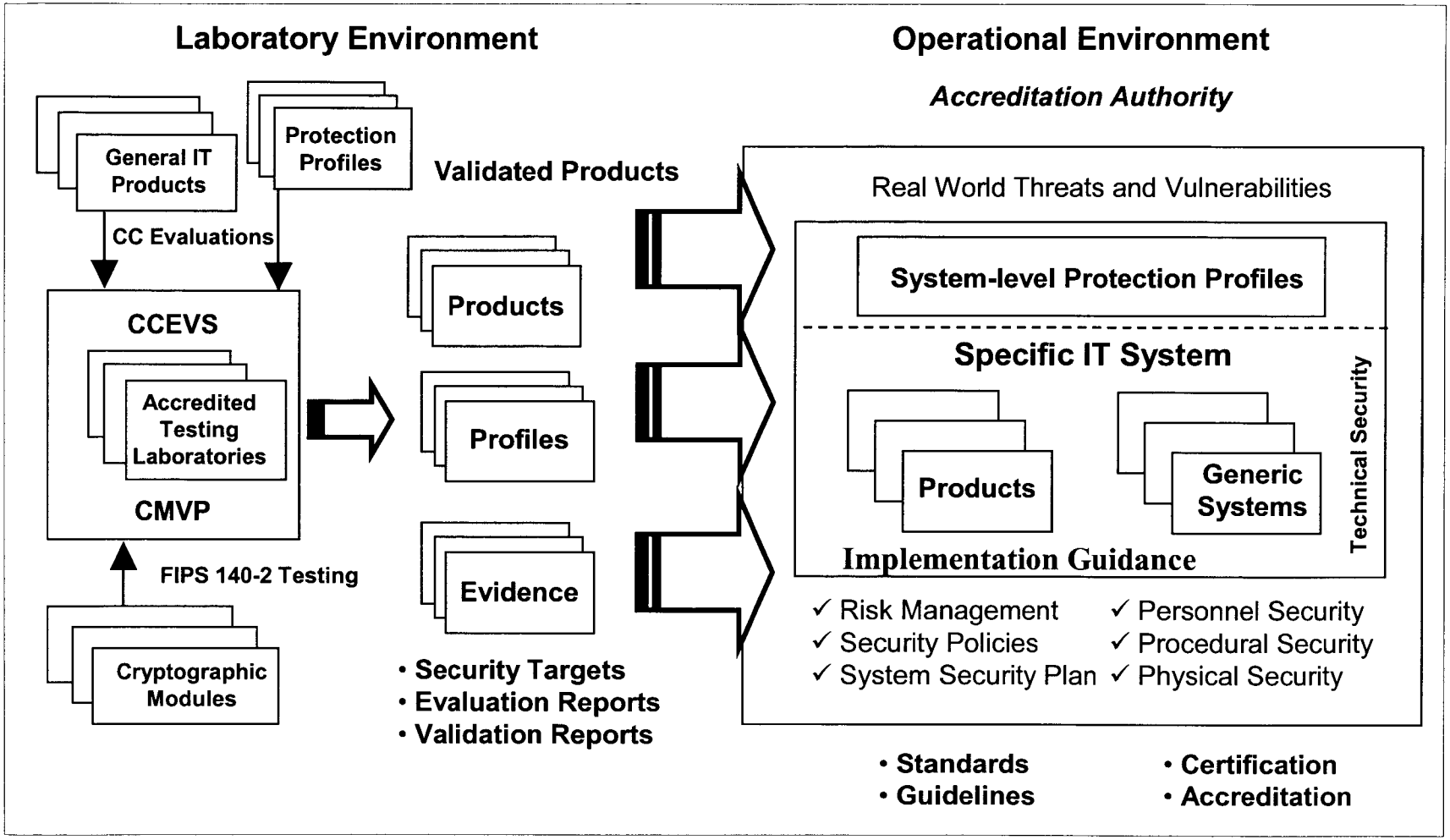
# Use of CC as a Requirements Definition Language (3)

- We see a need for:
  - Consensus-based standards/requirements sets
  - Conformance Tests/Test methods
  - Security Checklists/Implementation Guides/Configuration settings
- NIST has traditionally addressed the first two (e.g., crypto standards)
- NIST has and is addressing the last area as well: http://csrc.nist.gov/pcig/index.html

# Role/Value of CC evaluations (1)

- Relationship of validated products (CC & CMVP) to system development, integration, & evaluation addressed on next slide

# Contribution of Validated Products to System Development, Integration, & Evaluation



# Role/Value of CC evaluations (2)

- Believe cost/time of CC evaluation must be commensurate with security improvement
  - To the product
  - To overall system security
- Recommend, for CC evaluations, a solid business case be developed (or at least document evidence of security improvements that result from CC evaluation)
- We challenge schemes, evaluation sponsors, and user organizations to build the business case (or document actual security improvements/benefits)
- These are necessary to obtain general acceptance and use of CC evaluated products by all sectors

# Role/Value of CC evaluations (3)

- Recommend development of assurance packages that more reasonably reflect:
  - The value obtained for the effort expended
  - Realistic threat spaces
- Recommend review & revision of CC Part III to ensure that it contains the necessary assurance requirements to develop the new assurance packages
  - FIPS 199 assurance packages mentioned earlier

# Role/Value of CC evaluations (4)

- Believe outputs (reports/evidence) of CC evaluation activity must be expanded to better meet needs of the most important customers:
  - Systems developers/integrators
  - Systems security certifiers and accreditors (as in system security certification &accreditation)
  - End user organizations
- Primary focus of schemes has been CC & CEM interpretation, evaluators, validators, & lab accreditation/oversight
- Recommend more support for:
  - customers that use evaluated products in their system development
  - certification agents that could reuse CC evaluation evidence in performing system security certification

# NIST's FISMA Implementation Project and the CC

- Responding to FISMA has become a NIST/Computer Security Division (CSD) high priority
  - NIST assigned significant tasks with deadlines
  - Required immediate transition of CSD resources to meet FISMA assignments
- FISMA requirements and the need for updating system security certification and accreditation (C&A) FIPS has resulted in a suite of standards & guidelines collectively supporting the "FISMA Implementation Project Risk Management Framework" (or Information System Security Assurance Architecture in an IEEE standards working group).

# FISMA Implementation Project: Risk Management Framework

**FIPS 199 / SP 800-60**

**Security Categorization**

Defines category of information system according to potential impact of loss

**SP 800-53 / FIPS 200**

**Security Control Selection**

Selects minimum security controls (i.e., safeguards and countermeasures) planned or in place to protect the information system

**SP 800-37**

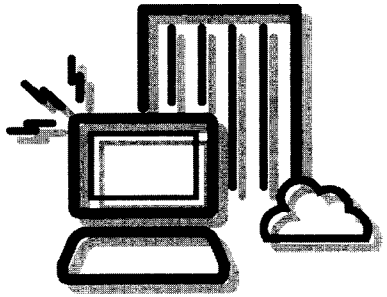
**Security Control Monitoring**

Continuously tracks changes to the information system that may affect security controls and assesses control effectiveness

**SP 800-53 / FIPS 200 / SP 800-30**

**Security Control Refinement**

Uses risk assessment to adjust minimum control set based on local conditions, required threat coverage, and specific agency requirements



**SP 800-37**

**System Authorization**

Determines risk to agency operations, agency assets, or individuals and, if acceptable, authorizes information system processing

**SP 800-18**

**Security Control Documentation**

In system security plan, provides a an overview of the security requirements for the information system and documents the security controls planned or in place

**SP 800-64**

**Security Control Implementation**

Implements security controls in new or legacy information systems; implements security configuration checklists

**SP 800-53A / SP 800-37**

**Security Control Assessment**

Determines extent to which the security controls are implemented correctly, operating as intended, and producing desired outcome with respect to meeting security requirements

# Using The CC for System Security Certification: Today

- Reports/evidence from CC evaluated products used in systems integration could provide useful information for system security certification -- if better tailored for that function
- As mentioned above, current CC evaluation reports/evidence not intended for this purpose

# Using The CC for System Security Certification: Today

- Theoretically, CC could be used for system certification/evaluation but:
  - CC lacks functional requirements for the non-IT aspects of the IT system (e.g., physical, administrative, personnel, training)
  - CC part III may need new/different assurance requirements
  - CEM has analogous shortcomings
  - Labs not accredited to perform system evaluation

# Using The CC for System Security Certification: Today

- CC can be used to perform:
  - Generic system evaluations (fixed grouping of integrated IT components evaluated in a laboratory environment)
  - Composite evaluations (e.g., smart cards)
  - Early/experimental use of "system level" PPs & use of the CC for system evaluation (e.g., UK)

# Using the CC for System Security Certification: Future

- Expansion of CC to include:
  - Non-IT functional requirements of the operational environment (e.g., physical, administrative, procedural, personnel) as found in ISO 17799 and other control documents
  - New assurance requirements/packages
  - ISO/IEC JTC 1/SC 27 WG 3 Work Item: Operational System Evaluation
- Expansion of CEM to include assessment methods for the non-IT functional requirements of the operational environment
- Accreditation of labs to perform CC-based system evaluations

# NIST's FISMA Implementation Project:

- Is on a much faster track than CC extension to systems
- Will submit its results to SC 27 WG 3 as a U.S. contribution
  - Candidate functional and assurance requirements
  - corresponding evaluation methodology for the non-IT aspects of the operational environment
- Phase II will establish a program and technical criteria, to qualify/recognize/accredit organizations to perform system security certification in accordance with NIST guidance (not funded to date).
- The technical criteria will also be provided to SC 27 as a contribution

# Security Control Selection: NIST SP 800-53

- Second draft of Sept 30, 2004 on NIST's csrc.nist.gov website for public comment
- Contains a catalogue of security controls
  - 17 Families (e.g., I&A, access control, physical/environmental, ID)
  - Basic control with supplemental guidance (when needed) and enhancements (none → several)
- Contains minimum control baselines for FIPS 199/SP 800-53 security impact levels (i.e., Low, Moderate, & High Impact systems). The baselines will become mandatory in FIPS 200.
- Baselines selected from control catalogue
  - Baselines are hierarchical
- Contains a set of assurance requirements corresponding to each security impact level (control independent & hierarchical corresponding to Low, Moderate, High impact baselines)
- 800-53 is essentially an extension of CC Parts II & III to systems

# Security Control Assessment: NIST SP 800-53A

- Will start development in FY 2005
- Will specify, for each control in 800-53, a corresponding assessment procedure
- Will be an analogue to the CEM extended to systems but:
  - More control-specific than CEM
  - Assessment procedures will increase in rigor with security impact levels
- Still investigating alternative models/approaches

# Recommendations on What is Needed (Broader than CC & NIAP)

- Balanced consideration given to development of:
  - Consensus-based standards/requirements sets
  - Conformance Tests/Test methods
  - Security Checklists/Implementation Guides/Configuration settings
- Improvements in:
  - Product/system developmental approaches
  - Product/system evaluation and testing

# What is Needed: Product/System Developmental Approaches

- Development practices/methods that contribute to improved security, safety, and reliability of products and systems
  - Establish environment for developers and other stakeholders to share information about such practices (e..g., Microsoft Press: *Writing Secure Code* by Michael Howard and David LeBlanc, 2002 & *Threat Modeling* by Frank Swiderski and Window Snyder, 2004.)
  - Establish metrics to compare practices/methods and to verify improvements such as reduction of vulnerabilities
  - Establish/adopt as industry-wide standards
  - Incorporate into the CC
  - Develop automated tools that support the practices/methods

# What is Needed: Product/System Evaluation and Testing

- R &D of new test methods/approaches that are more objective and less subjective
- Development of technology-specific tests and test methods (e.g. DTRs, smartcards)
- Development of automated testing and evaluation tools
- R & D of alternative approaches to gaining assurance about evaluation/testing results

# Summary/Conclusions (1)

- As an international standard for security requirements definition, the CC will continue to evolve. That aspect is:
  - Not dependent on the success/failure of national CC evaluation schemes
  - Useful even if evaluations never performed
- Demonstrating a product conforms to its security specification is worthwhile but:
  - Cost/time/effort must be commensurate with security improvement/value achieved
  - Particularly in "system" context
- CC schemes need to:
  - Pay more attention to the cost/benefit issues of CC evaluation, particularly relevance, effectiveness & efficiency of the evaluation process
  - Provide better support the most important users: system integrators & developers

# Summary/Conclusions (2)

- In big picture, we need to focus on:
  - Consensus-based standards/requirements sets
  - Conformance Tests/Test methods
  - Security Checklists/Implementation Guides/Configuration settings
  - Improvements in:
    - Product/system developmental approaches
    - Product/system evaluation and testing