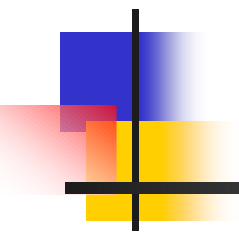
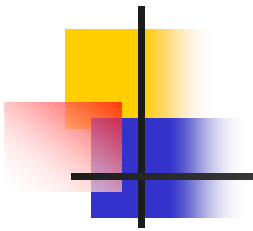


Testing to FIPS 140-2 Derived Test Requirements

Randall J. Easter, NIST



Agenda

- Philosophy
- Cryptographic Module Testing
- Laboratory Accrediation
- CMVP Testing Process and Goals
- Testing Metrics
- Derived Test Requirements
- Cryptik Tool

Philosophy

- Strong commercially available cryptographic products are needed
- Government must work with the commercial sector and the cryptographic community for:
  - security,
  - interoperability, and
  - assurance

Cryptographic Module Testing

- Federal systems that implement cryptography to protect sensitive information
  - *Must* comply with FIPS 140-1 and FIPS 140-2
  - … **shall** be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract.
  - Set of hardware, and/or software, and/or firmware
  - Implements a cryptographic algorithm
  - Contained within a defined boundary

Cryptographic Module Testing (concluded)

- Cryptographic modules are tested using Derived Test Requirements (DTRs)
- Independent accredited laboratories perform DTR testing
  - Six NVLAP-accredited testing laboratories
    - True independent 3rd party accredited testing laboratories
    - Cannot test and provide design assistance

Security Requirements for Cryptographic Modules (FIPS 140-2)

- Eleven areas of security requirements
- Increasing levels of security in most areas
- (up to 4 levels)
- Modules may meet different levels in different security requirements areas
  - Module meets level 2 overall, level 3 physical security with additional level 4 requirements

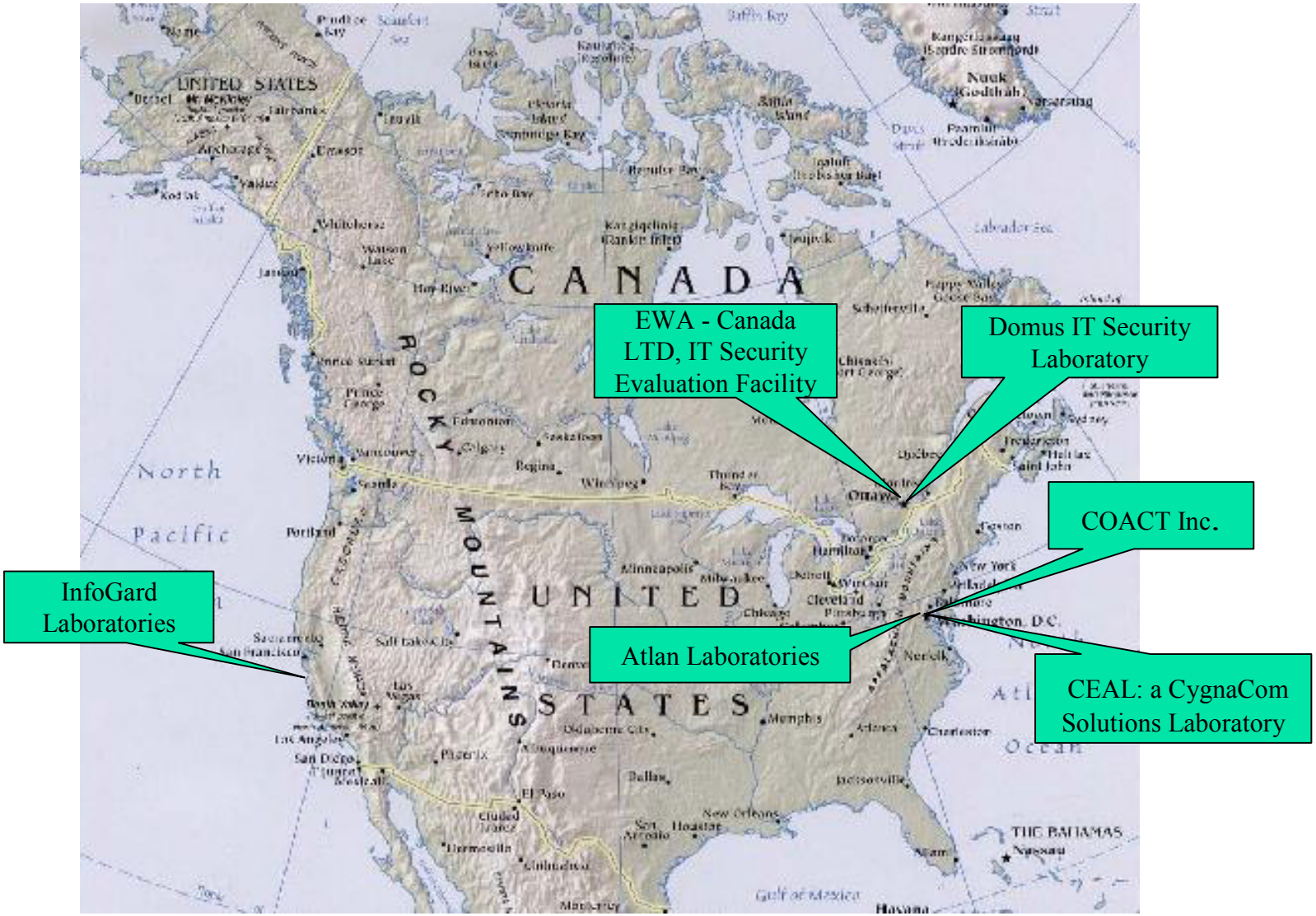
Laboratory Accreditation

- Laboratories accredited by NVLAP
  - Accreditation based on Handbook 150-17, Cryptographic Module Testing
    - Supplements Handbook 150, NVLAP Procedures and General Requirements
    - Encompasses requirements of ISO17025, General Requirements for the Competence of Testing and Calibration Laboratories
    - Handbook 150 includes relevant requirements of ISO9002, Quality systems -- Model for quality assurance in production, installation and servicing
    - Accreditation process includes proficiency testing specific to the CMVP and FIPS 140-1&2

Laboratory Accreditation

- Annual NVLAP review
- Biannual onsite NVLAP assessment

CMVP Accredited Laboratories



Sixth CMT laboratory added in 2001

Common Criteria and CMVP Lab Accreditation

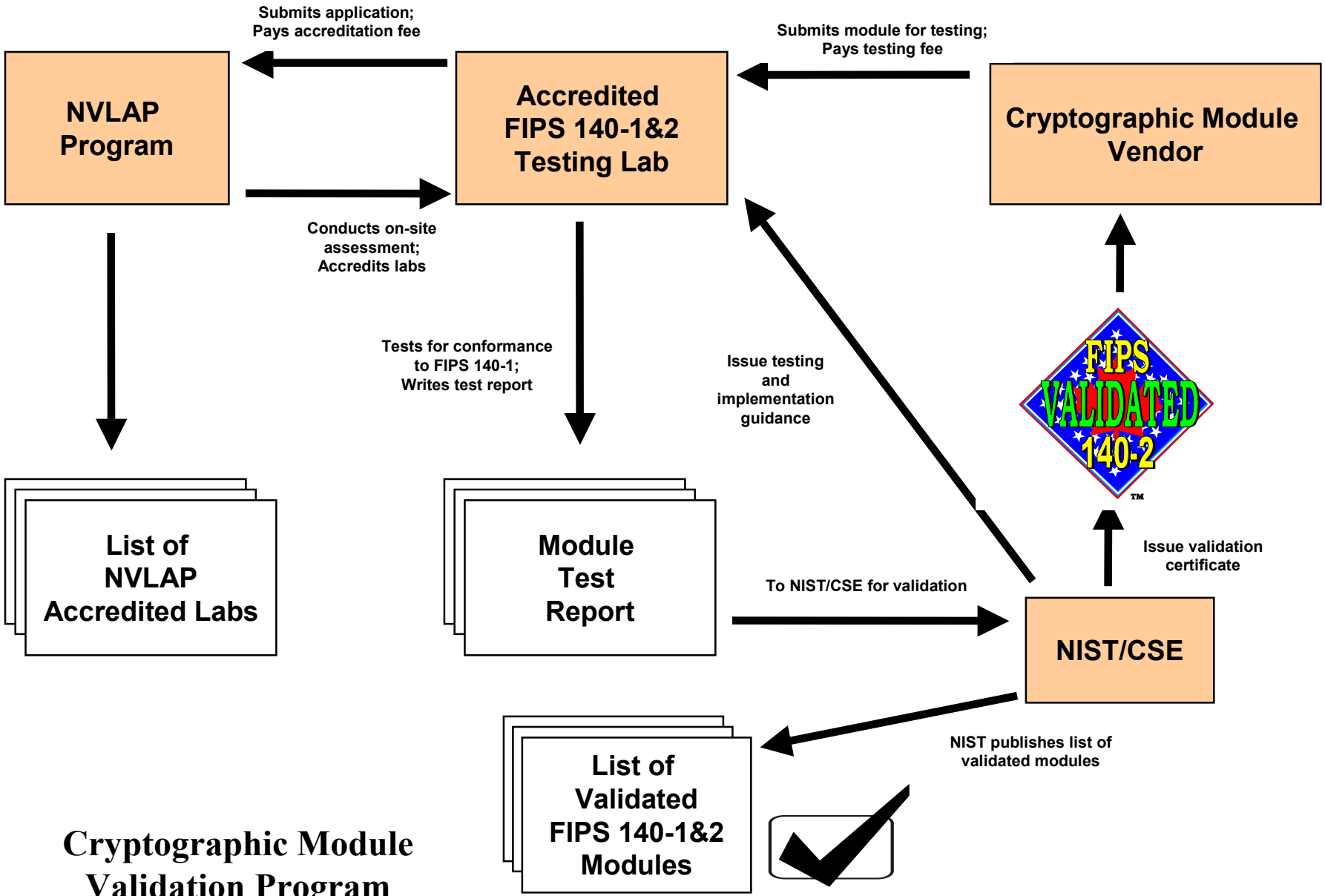
- NVLAP accredits all CMVP laboratories
- NVLAP accredits United States laboratories for CC evaluations
- Standards Council of Canada (SCC) accredits Canadian Common Criteria Evaluation laboratories
- Canada moving the accreditation of Canadian CMT laboratories from NVLAP to SCC

CMVP Responsibilities

- Vendors
  - Provide necessary and required information and documentation to the lab
  - Review DTRs, policy, and Implementation Guidance
- Cryptographic Module Testing (CMT) Laboratories
  - Perform 140-1 and 140-2 and algorithm testing
  - Intermediate between vendors NIST and CSE

CMVP Responsibilities (concluded)

- NIST/CSE
  - Review reports and issue validation certificates
  - Issue CMVP policy
  - Issue guidance and clarifications of FIPS 140-1, FIPS 140-2 and other cryptographic standards
  - Assist NVLAP in laboratory assessments
- National Voluntary Laboratory Accreditation Program (NVLAP)
  - Accredit laboratories for quality and competence
  - Perform periodic reassessments



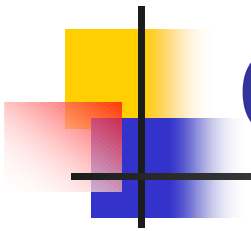
Cryptographic Module Validation Program

CMVP Testing Process

- Purpose of CMVP
  - Conformance testing of cryptographic modules using the DTR
  - Not evaluation of cryptographic modules. Not required are:
    - Vulnerability assessment
    - Design analysis, etc.
- Laboratories
  - Test submitted cryptographic modules
- NIST/CSE
  - Validate tested cryptographic modules

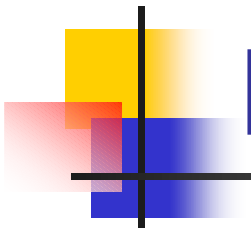
CMVP Testing Goals

- Among the laboratories…ensure
  - *Comparability* of test results
  - *Repeatability* of tests and test results
- Vendors
  - Required services are correctly performed by the laboratory
- Among users
  - Comprehensive testing of the module/product
  - Cryptographic and other security features correctly implemented



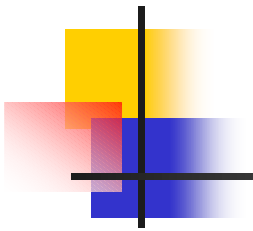
CMVP Testing Goals (concluded)

- Accreditation authority (NIST/CSE) and National Voluntary Laboratory Accreditation Program (NVLAP)
  - Competence of laboratories



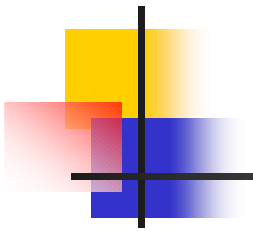
Buyer Beware!

- Does the product do what is claimed?
- Does it conform to standards?
- Was it independently tested?
- Is the product secure?



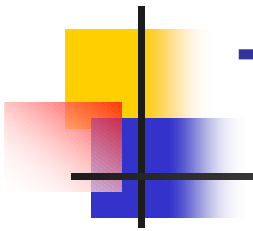
Testing Metrics

- Standards-based testing
  - General model
  - Applicable to:
    - Cryptographic algorithms/modules
    - Security modules/products
  - Tests are conducted using:
    - Standards
      - ANSI (X9.31, X9.52)
      - FIPS (3DES, DSS, SHA-1, etc.)
    - Criteria
      - Common Criteria
        - Functional Requirements
        - Assurance Requirements (EAL1 - EAL7)



Testing Metrics (continued)

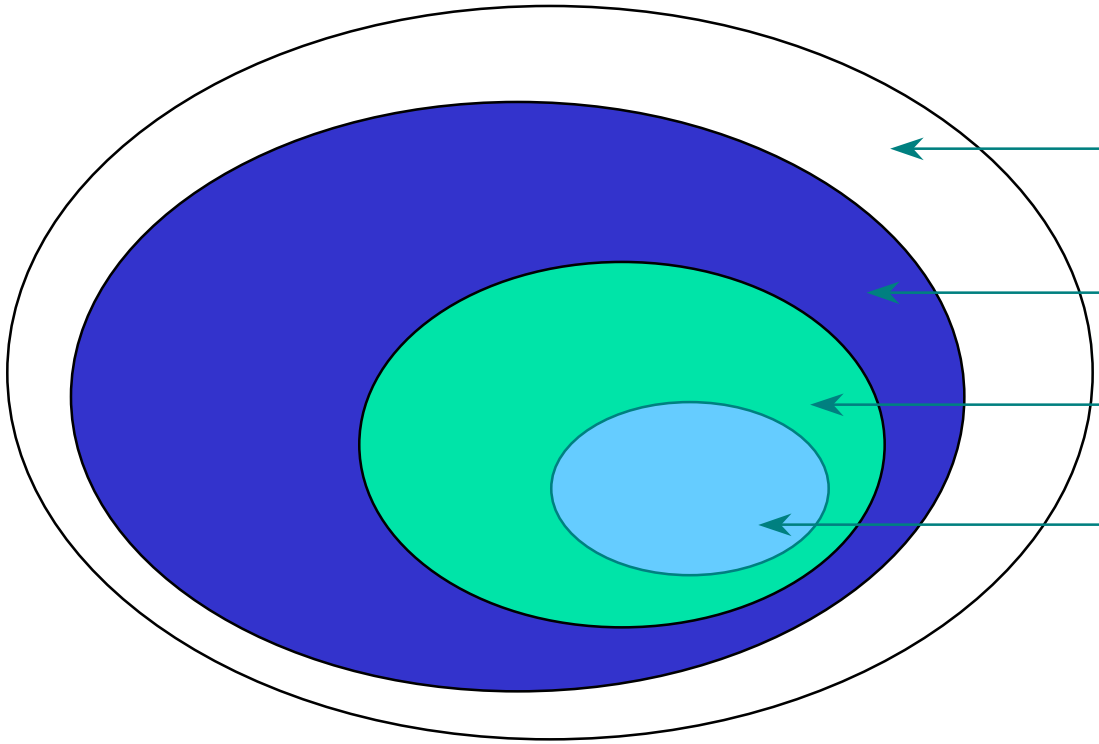
- Applications/systems testing
- Applicable to implementation-dependent systems
- Based on user requirements/needs
- Tests are conducted using:
  - Certification tests
  - Application/system specifications
  - Organization policies and procedures
- Also examine:
  - Network environment
  - Physical environment



Testing Metrics (concluded)

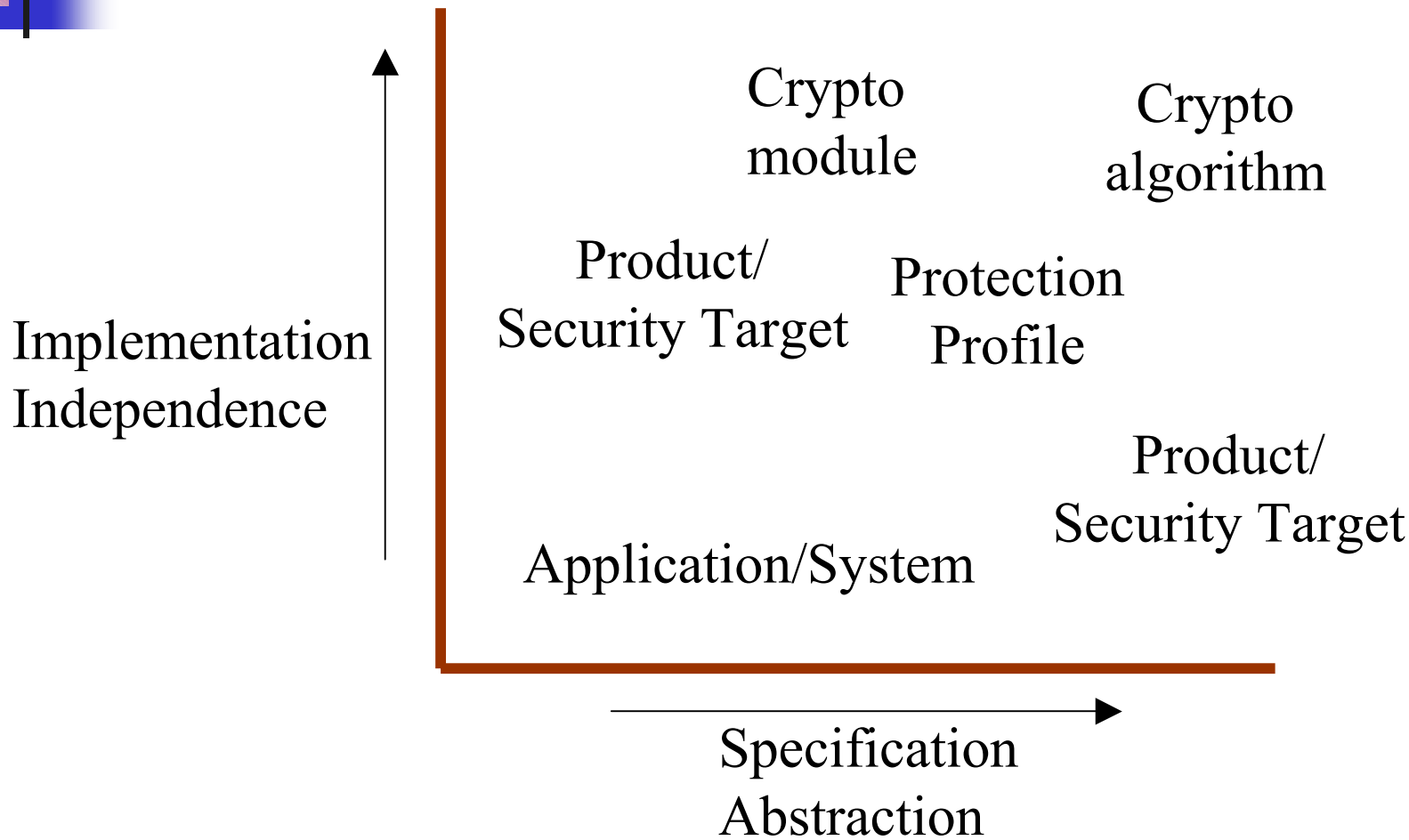
- May require…
  - FIPS-validated modules/products (Cryptographic Module Validation Program (CMVP)) *and*
  - CC evaluated modules/products

Testing - Algorithms to Systems

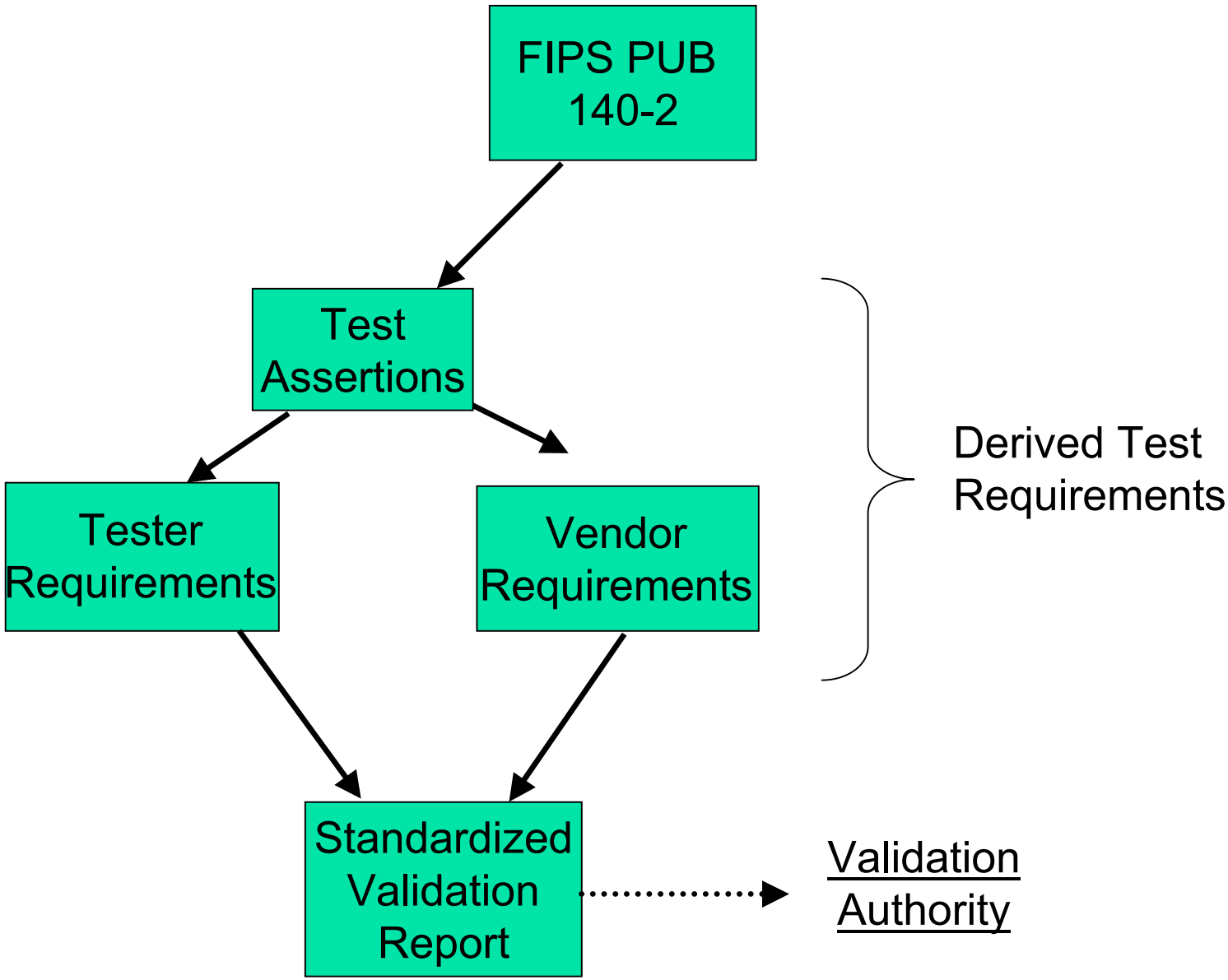


Level	Example	Specification
Application	Air Traffic Control	?
Product	Firewall	Common Criteria
Security Module	Crypto Module	FIPS 140-2
Algorithm	AES	FIPS 197

Testing: from standards-based to ….



Derived Test Requirements Development



Derived Test Requirements

- Cryptographic module testing is performed using the DTR
- Assertions in the DTR are directly traceable to requirements in FIPS 140-1 and FIPS 140-2
- FIPS 140-1 DTR assertions are either
  - Direct quotes from the standard or
  - Directly derivable from the requirements
- FIPS 140-2 DTR assertions map directly to FIPS 140-2 requirements

Derived Test Requirements
(concluded)

- All FIPS 140-2 requirements will be included in the DTR as assertions
  - Provides for one-to-one correspondence between the FIPS and the DTR
- Each assertion will include requirements levied on the
  - Cryptographic module vendor
  - Tester of the cryptographic module
- Modules tested against FIPS 140-2 will use the associated DTR

Derived Test Requirements

- DTRs are directly traceable to FIPS 140-1&2
- AS<reqmt_no>.<assertion_sequence_no>
  - reqmt_no - corresponding area in FIPS 140-1&2
  - assertion_sequence_no - sequential identifier for assertions within a section
  - Assertions map directly to requirements in FIPS 140-2
  - Example: AS03.13: Documentation shall provide a complete specification of all of the authorized roles supported by the module (1, 2, 3, and 4)

Derived Test Requirements
(continued)

- VE<reqmt_no>.<assertion_sequence_no>.<sequence_no>
  - reqmt_no - corresponding area in FIPS 140-1&2
  - assertion_sequence_no - sequential identifier for assertions within a section
  - sequence_no - a sequential identifier for vendor requirements within the assertion
  - Example: VE03.01.01: Vendor documentation shall specify each distinct authorized role, including its name, purpose, and the services that are performed in the role

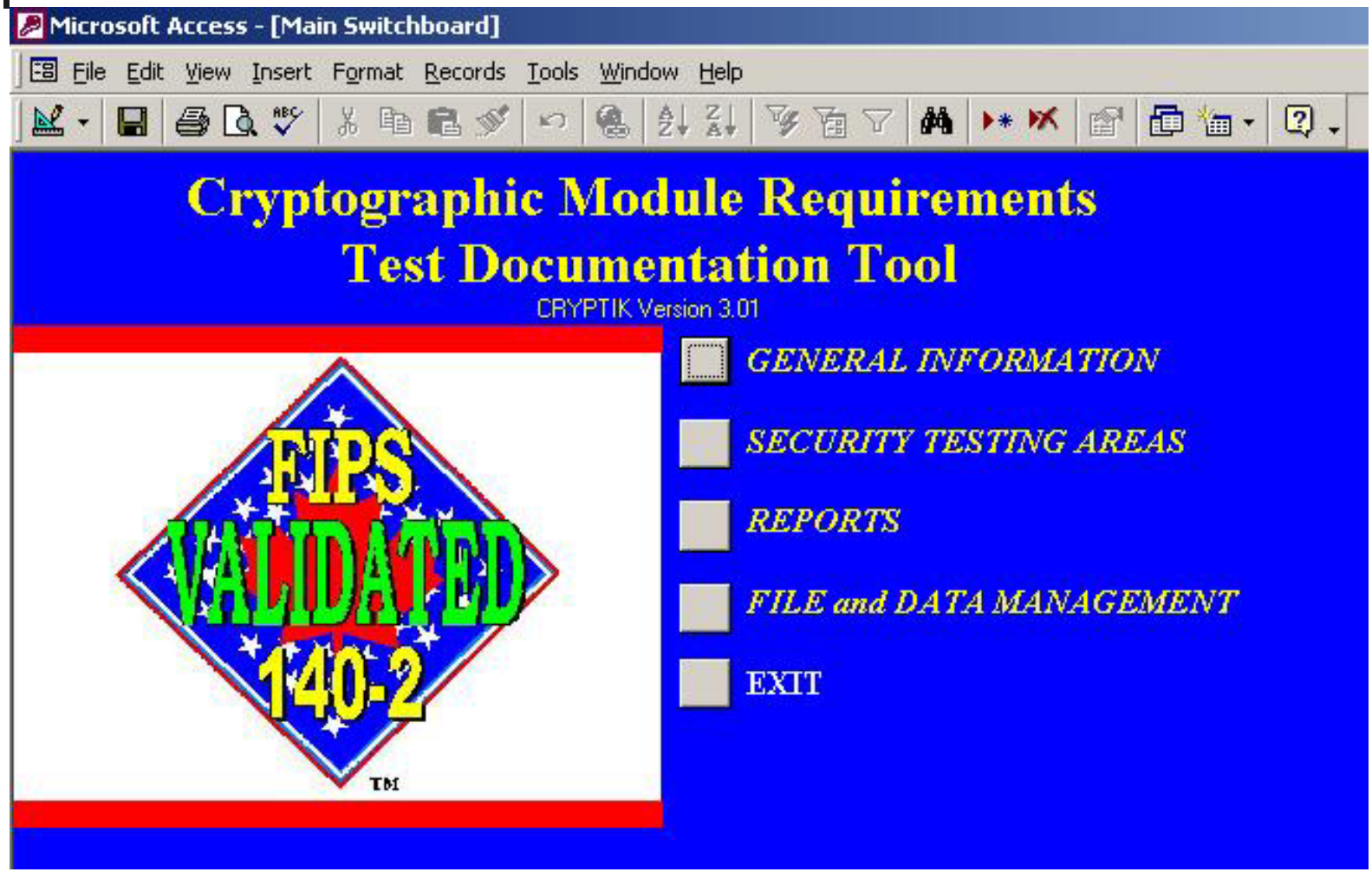
Derived Test Requirements
(concluded)

- TE<reqmt_no>.<assertion_sequence_no>.<sequence_no>
  - reqmt_no - corresponding area in FIPS 140-1&2
  - assertion_sequence_no - sequential identifier for assertions within a section
  - sequence_no - a sequential identifier for tester requirements within the assertion
  - Example: TE03.01.02: The tester shall assume each of the authorized roles described in the vendor documentation and verify that each of them can be assumed.

Traceability

- Traceability of test cases assured through use of Cryptik
- Traceability to requirements in FIPS 140-2 achieved through
  - Assertions and DTRs documented in Cryptik
- Assertions are
  - Direct restatement from the requirements
- DTRs divided into two sets of requirements
  - One set levied on the CM vendor
  - One set levied on the tester of the CM

Cryptik Tool



Revalidations

An updated version of a previously validated cryptographic module can be considered for a revalidation rather than a full validation depending on the extent of the modifications from the previously validated version of the module.

1. Modifications are made to hardware, software or firmware components that do not affect any FIPS 140-1 security relevant items.
   - *Signed Letter from Accredited Laboratory*

2. Modifications are made to hardware, software or firmware components that affect some of the FIPS 140-1 security relevant items.
   - *Re-validation TE's annotated as RE-Tested with an overall regression test performed*

How to Get Involved...

- FIPS 140-1 & 2 training and workshops
- Vendors of cryptographic modules may work with the CMT laboratories
- Federal agencies may work with NIST/CSE to develop technical and procurement requirements
- All users may request information from NIST/CSE

http://www.nist.gov/cmvp

- FIPS 140-1 & 2
- Derived Test Requirements (DTR)
- Implementation Guidance
- Points of Contact
- Laboratory information
- Validated Modules List
- Vendor List
- Useful Links

Points of Contact

NIST

- Annabelle Lee:
  annabelle.lee@nist.gov
  301.975.2941
- Ray Snouffer:
  ray.snouffer@nist.gov
  301.975.4436
- Randy Easter:
  randall.easter@nist.gov
  301.975.4641
- Janet Jing:
  janet.jing@nist.gov
  301.975.2920

CSE

- Jean Campbell
  Jean.Campbell@CSE-CST.GC.CA
  613-991-8121
- Ken Lu
  Ken.Lu@CSE-CST.GC.CA
  613-991-8122
- Robert Crooks
  Robert.Crooks@CSE-CST.GC.CA
  613-991-8130

QUESTIONS