Title of Panel: Security Assurance: Does Anybody Care?
Panel Chair: S. Katzke, NIST
Panelists: S. Katzke, NIST; S. Chokhani, Cygnacom Solutions; J. Schindler, Hewlett-Packard; D. Webb, SRI

Session abstract:

Security Assurance of an IT system is the level of trust one has that the system correctly meets its functional specifications, and does not perform unintended functions that compromise its security. Since current IT systems are extremely complex, distributed, and often not under unitary control, technical methods for assessing the SA of systems are still more art than science. However, methods/approaches do exist for assessing the SA of the IT components/products that are used as building blocks for such systems. While these assessments do not provide the system SA one desires, it is reasonable to assume that SA of the components/products is a necessary condition for assessing the SA of a system. This Forum Session will focus on assessing the SA of IT components/products (hereafter referred to as just "products")

Security Assurance (SA) of an IT product is the level of trust one has that the product (e.g., operating system, firewall, database, webserver, telecom switch) meets its functional security specifications, and does not perform unintended functions that compromise its security. The panel, drawn from IT product developers, security consultants, and security evaluation/testing labs; will:

- examine the need/desire for SA in IT products
- describe alternative approaches for achieving SA
- discuss how one assesses SA.

In particular, the aim of the Session is to engage the audience in a discussion around the following types of questions:

As a concept, is product SA useful/important to you?
How do you assess products you use?
Vendor self assurance/certification (first party)?
Self assessment (second party)?
Third party assessment? At what cost?

Do the methods you are using meet your needs?
Are you willing to accept independent testing/evaluation by independent labs/organizations (e.g., ICSA)?

Does the type of testing make a difference to you (e.g., execution of test suites, specification-based testing, known vulnerability tests, penetration tests)?

Does the origin/derivation of the test suites, specifications, and other tests methods applied make a difference to you (e.g., derived by: vendor, vendor groups, independent lab, user community affinity groups, standards groups, government labs)?

Would you prefer to use or request the use of commercial testing labs that have been accredited through an "approved" process (e.g., NIST's National Voluntary Laboratory Accreditation Program (NVLAP))?

What should be the government's role in facilitating SA?

How important is a mark or brand on a product?

Does it make a difference who issues it?
Would you select a product based on a mark or brand?
Would a government certificate be more desirable than other choices (e.g., vendor associations, independent labs)?

Each panelist will have the opportunity to present their views on the above topics with the hope of generating controversy that will engage the audience.

Position statements from each panelist:

Stu Katzke, NIST: Stu Katzke will begin the session with some opening remarks and tutorial information about SA. He will then take the position that third party, specification-based testing by commercial labs that have been accredited using the NIST NVLAP provides an approach that has significant advantages over other approaches. He will inform the audience about a commercial testing program that is being established by NIST & NSA to assist the commercial sector meet its testing needs. It will result in better, faster, cheaper testing of IT products than has been achieved under prior government security evaluation programs and will be responsive to market demands. In addition, the test results will be accepted (i.e., mutually recognized) by Canada, UK, France, Germany, and the Netherlands.

Jim Schindler, Hewlett Packard: Jim Schindler will discuss the Orange Book evaluation model and then present a new model for SA that responds to commercial demand, international applicability, real-world systems, minimizing impact on vendor/developers, and vendor liability. He will propose an approach similar to one that has worked in the hardware community and then conclude with several issues that still need to be resolved.

Santosh Chokhani, Cygnacom Solutions: Santosh Chokhani will share his thoughts about SA based upon the practical experience he has gained through direct participation in evaluations and through the experiences his laboratory has obtained from performing security evaluations. He will discuss his views on SA, which SA activities are high payoff, the benefits of third party evaluation by accredited labs, what consumers need to know about SA, and why evaluation programs fail. He will conclude with some recommendations to improve the SA process.

Douglas Webb, SRI Consulting: Doug Webb will discuss a NY City Elections project he worked on that required SA and the approach used to determine how much was needed. Since the project addressed functional requirements for voting machines, the issue of “how much SA is needed” was political as well as technical. Doug will share with the audience the factors involved in making the decision and the steps taken to insure that SA was achieved.

Security Assurance

Stuart Katzke

Chief, Computer Security Division

National Institute of Standards and Technology

Information Technology Laboratory

katzke@nist.gov

Computer Security Resource Clearinghouse:
csrc.ncsl.nist.gov

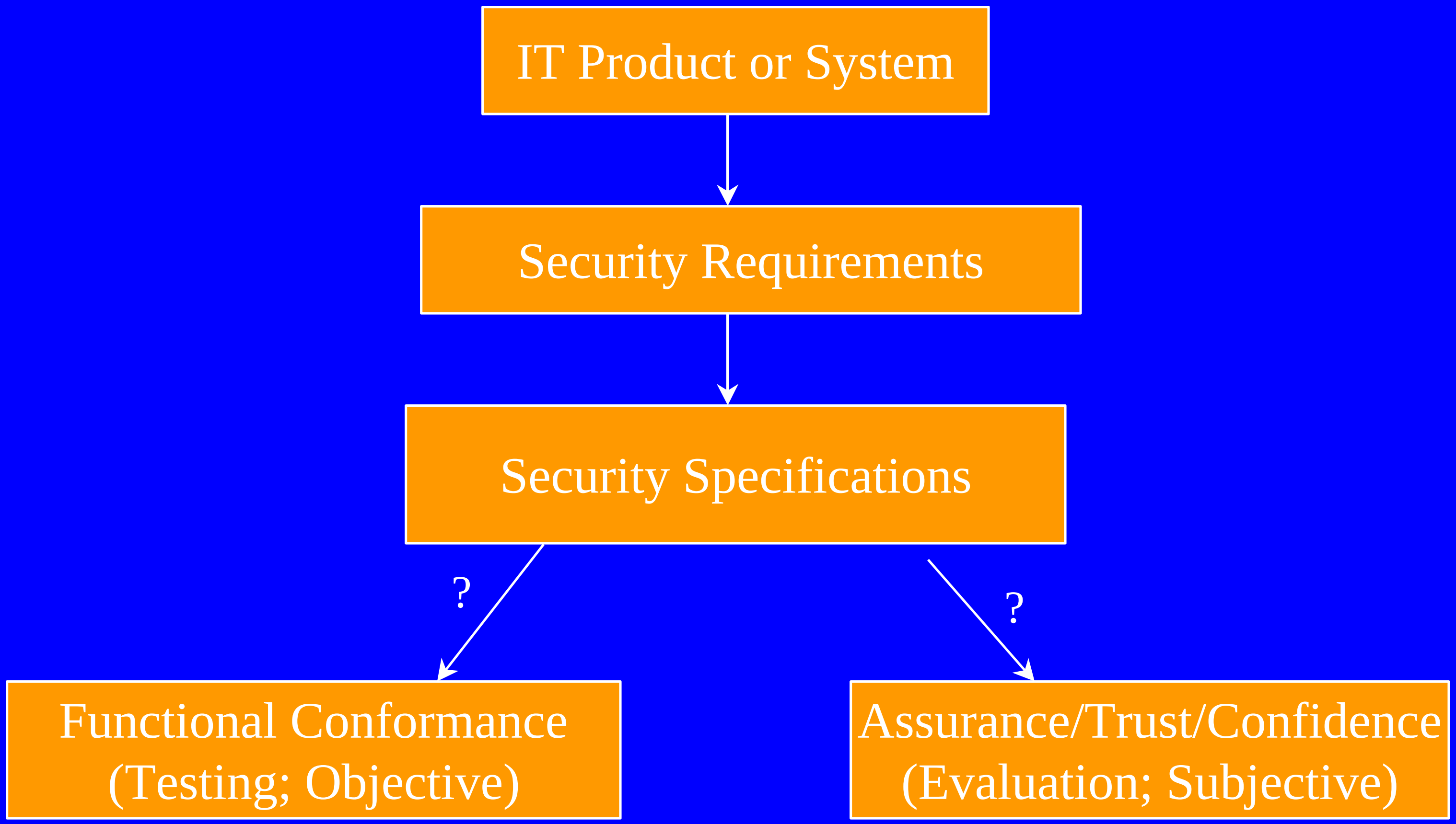
Presentation Overview

- Security Assurance
- NIST/NSA Security Testing/Evaluation (T/E) Initiatives

Security Assurance (SA)

Level of trust that a system or product conforms to its functional security specification; and does not perform unintended functions that compromise security

Security Specifications: Testing/Evaluation (T/E)



IT Product or System

Security Requirements

Security Specifications

Functional Conformance (Testing; Objective)

Assurance/Trust/Confidence (Evaluation; Subjective)

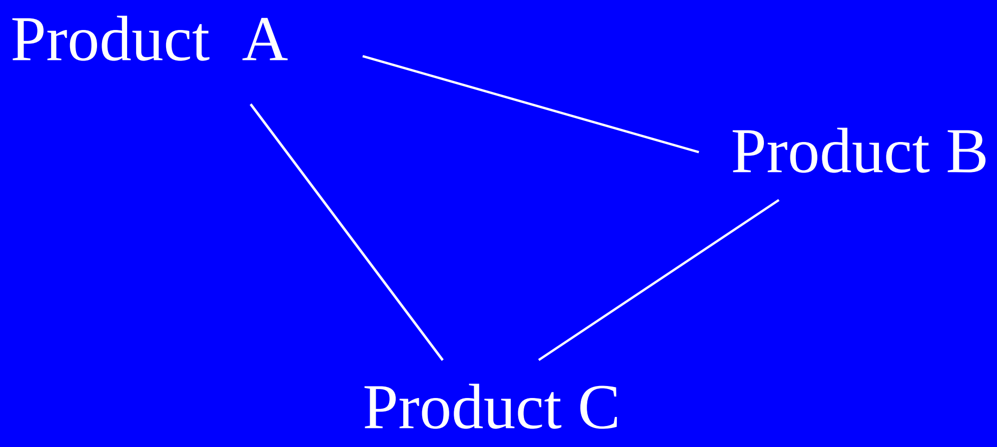
- functional testing

- development process
- security design analysis
- aggressive testing

This Presentation: Focus on SA of Products

- SA of a complex, distributed, multi-vendor, system is a research problem
- SA of systems is more art than science
- Product assurance is necessary (though not sufficient) for system assurance
- Can improve evaluation of products (faster, better, cheaper)
- Systems are one-of-a-kind (poor leveraging)

System: Composition



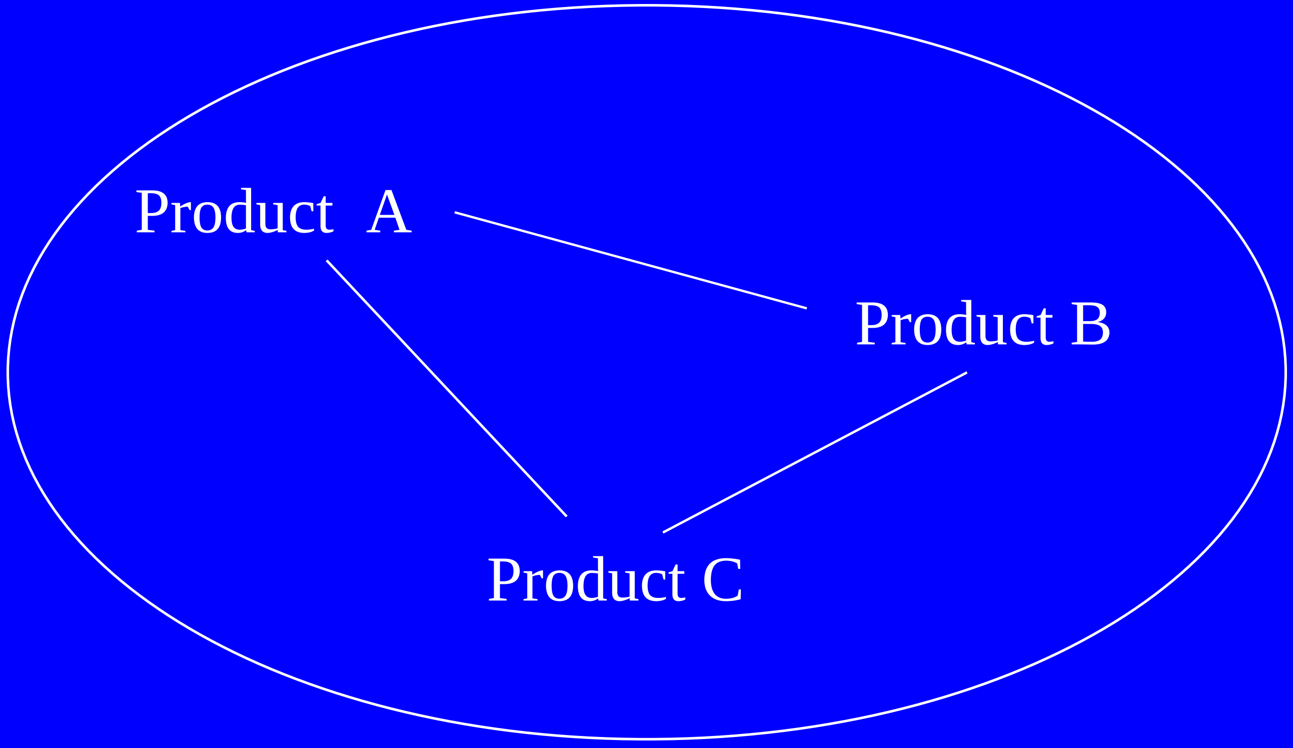
Product A

Product B

Product C

System or sub-system

System: Black Box

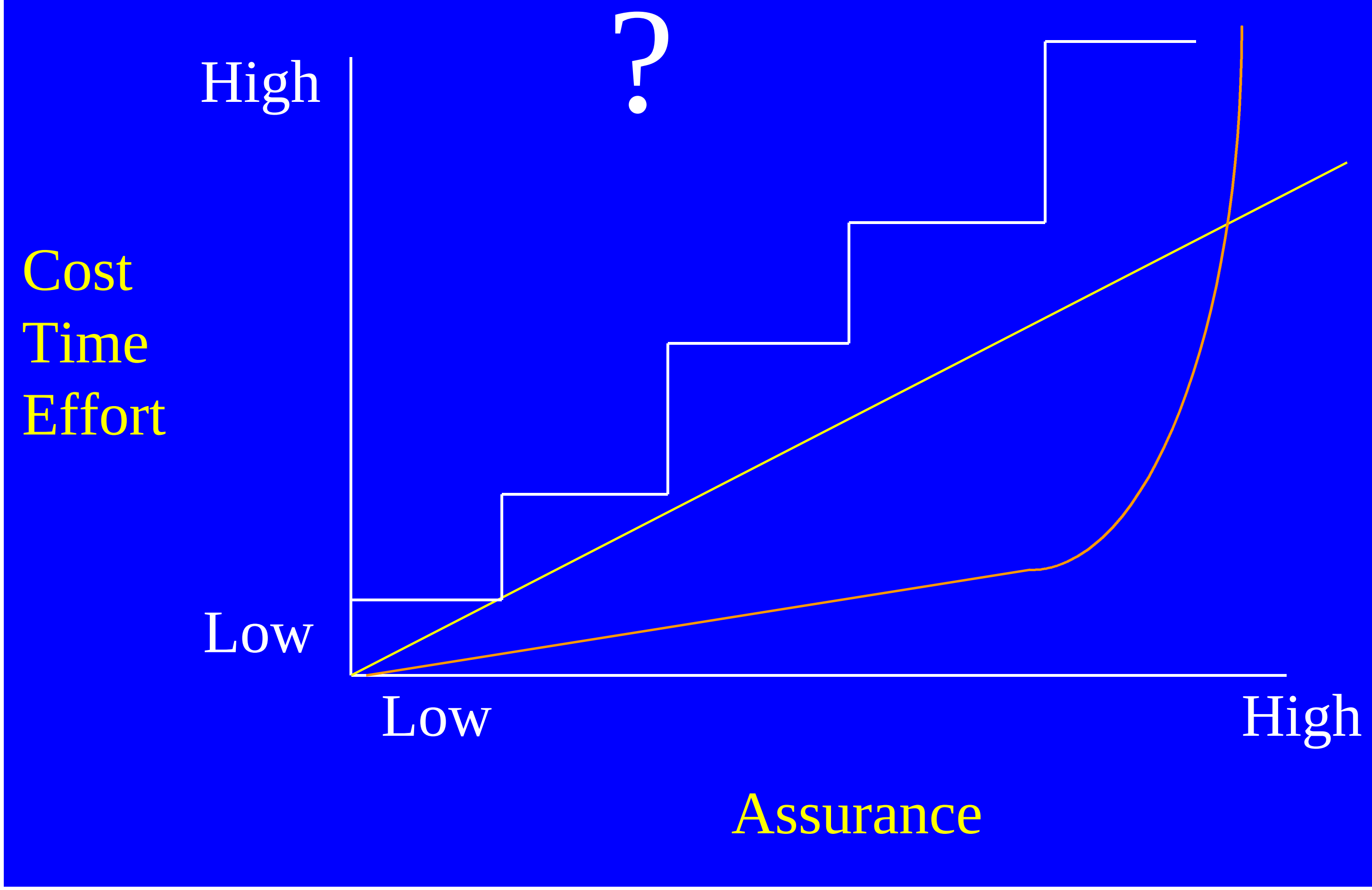


System or sub-system

Assurance Methods/Approaches

- Development methods & processes used
- Analysis of security architecture & design
- Testing
  - known vulnerability testing
  - penetration testing
  - test suites
- Vendor claim and warranty
- Vendor reputation & track record
- User experiences/recommendations

Assurance vs. Cost, Time & Effort



Who Makes Assurance Assessments?

- 1st Party: vendor
- 2nd Party: user/application owner
  - technical assessment
  - approval to operate
- 3rd Party
  - independent testing labs (e.g., NSTL)
  - gov’t approved testing labs (e.g., FIPS140-1)
  - other organizations that do testing (e.g., SRIC)

Assurance Indicators

- Certificate
  - government conformance test (e.g., DES)
  - government evaluations (e.g., Orange book)
  - government certification body w/international mutual recognition (e.g., FIPS 140-1)
  - organizational sponsor (e.g., ANSI, IEEE, IETF)
  - independent laboratory (e.g., ICSA)

Assurance Indicators (cont.)

- Mark or brand
  - OpenGroup
- Market popularity

Assurance Choices/Issues

- Is assurance important to you?
- Which methods/approaches are acceptable?
- Who would you like to see determine assurance?
- What proof of assurance is acceptable?
- How much extra would you pay for it?

NIST/NSA Security Testing/Evaluation (T/E) Initiatives

Stuart Katzke
Chief, Computer Security Division
National Institute of Standards and Technology
katzke@nist.gov

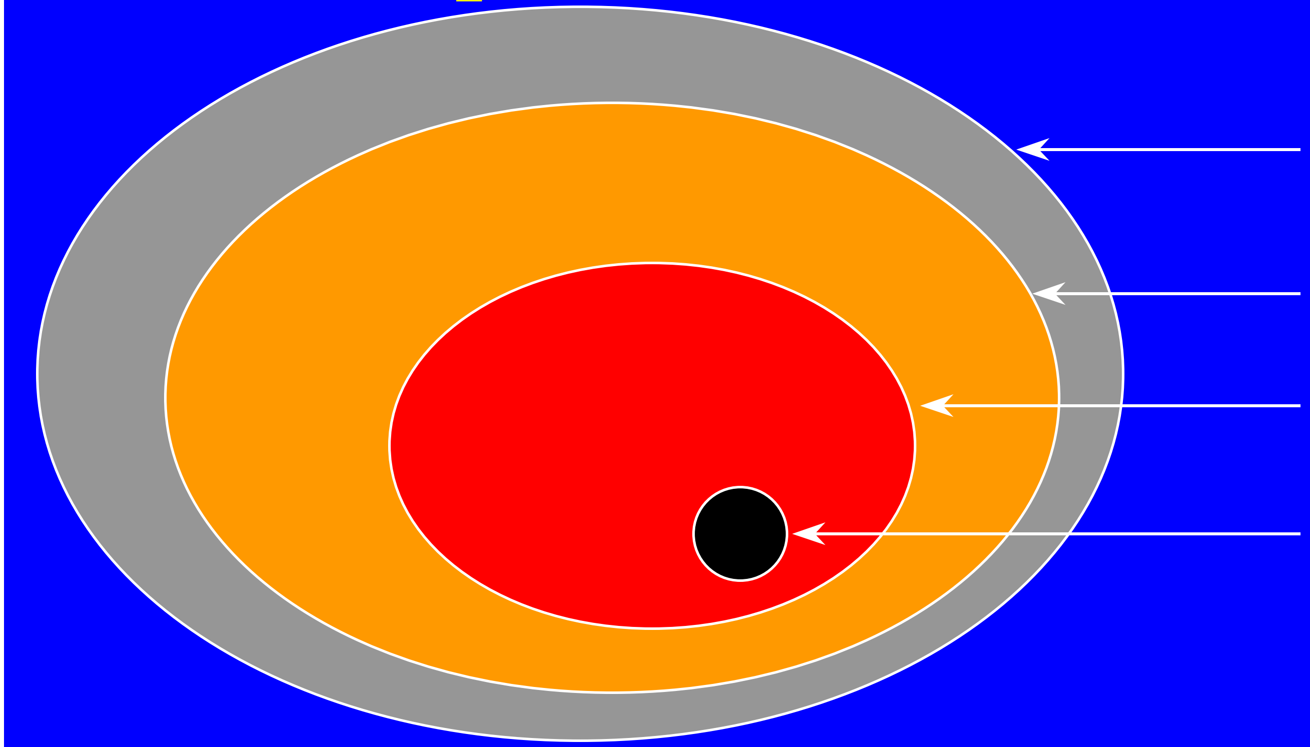
Lou Giles
Chief, Information Assurance Partnerships, Evaluations,
& Knowledge Management
National Security Agency
lgiles@radium.ncsc.mil

4/15/98

Overview

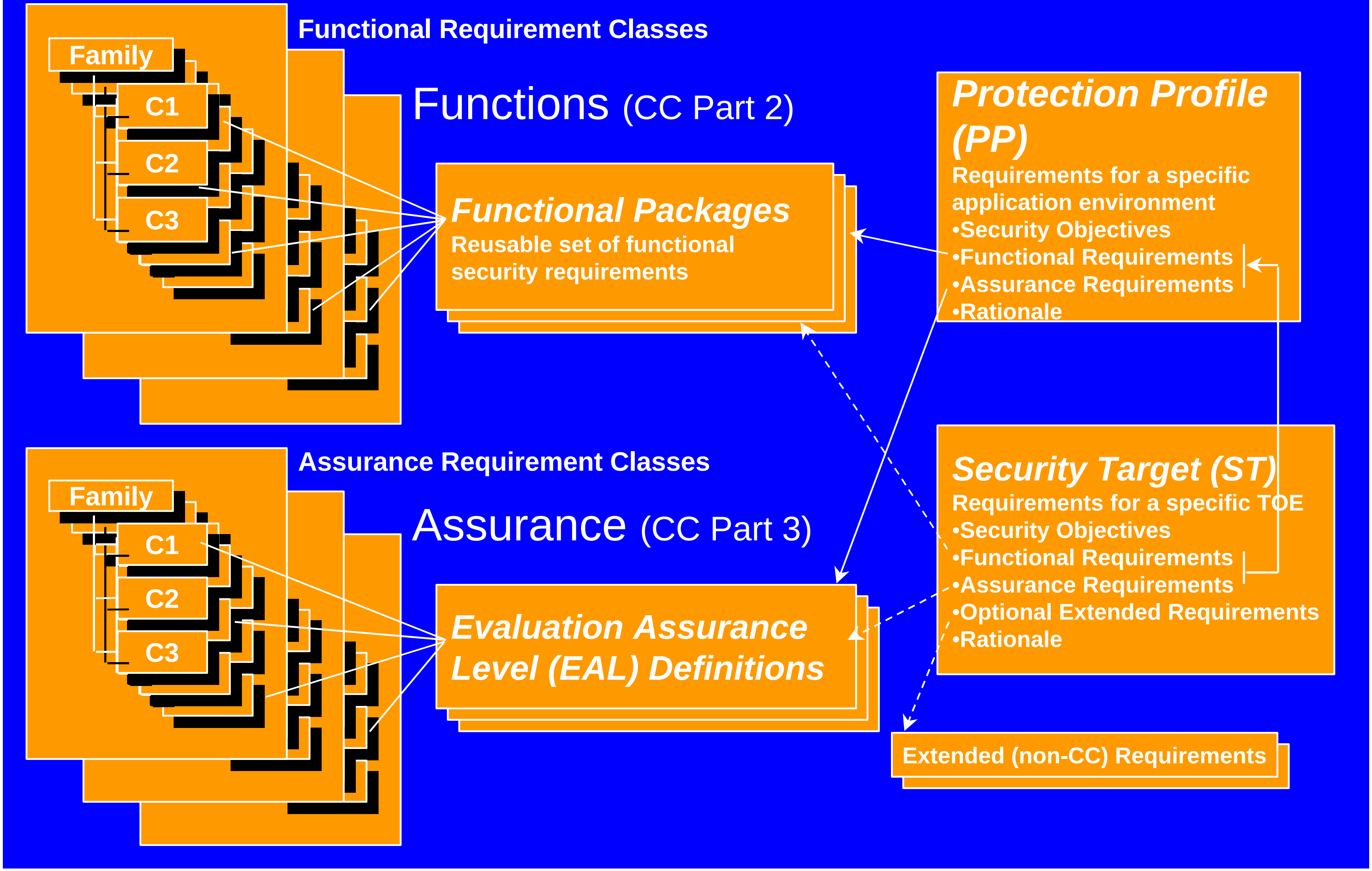
- Specification-Based Testing/Evaluation (T/E)
- Common Criteria (CC)
- Common Criteria Testing Program
- National Information Assurance Partnership
- Transition to CCTP
- TCSEC-CC Achievements
- TPEP and Its Future

Specification-Based T/E



Level	Example	Specification
Application/System	Air Traffic Control	CC, GSSP, ...
Product	Firewall , OS	Common Criteria (CC)
Security Module	Crypto Module	FIPS 140-1
Algorithm	DES	FIPS 46-2

Common Criteria Elements



Functional Requirement Classes

Family

C1

C2

C3

Functions (CC Part 2)

Functional Packages

Reusable set of functional security requirements

Protection Profile (PP)

Requirements for a specific application environment

- Security Objectives
- Functional Requirements
- Assurance Requirements
- Rationale

Assurance Requirement Classes

Family

C1

C2

C3

Assurance (CC Part 3)

Evaluation Assurance Level (EAL) Definitions

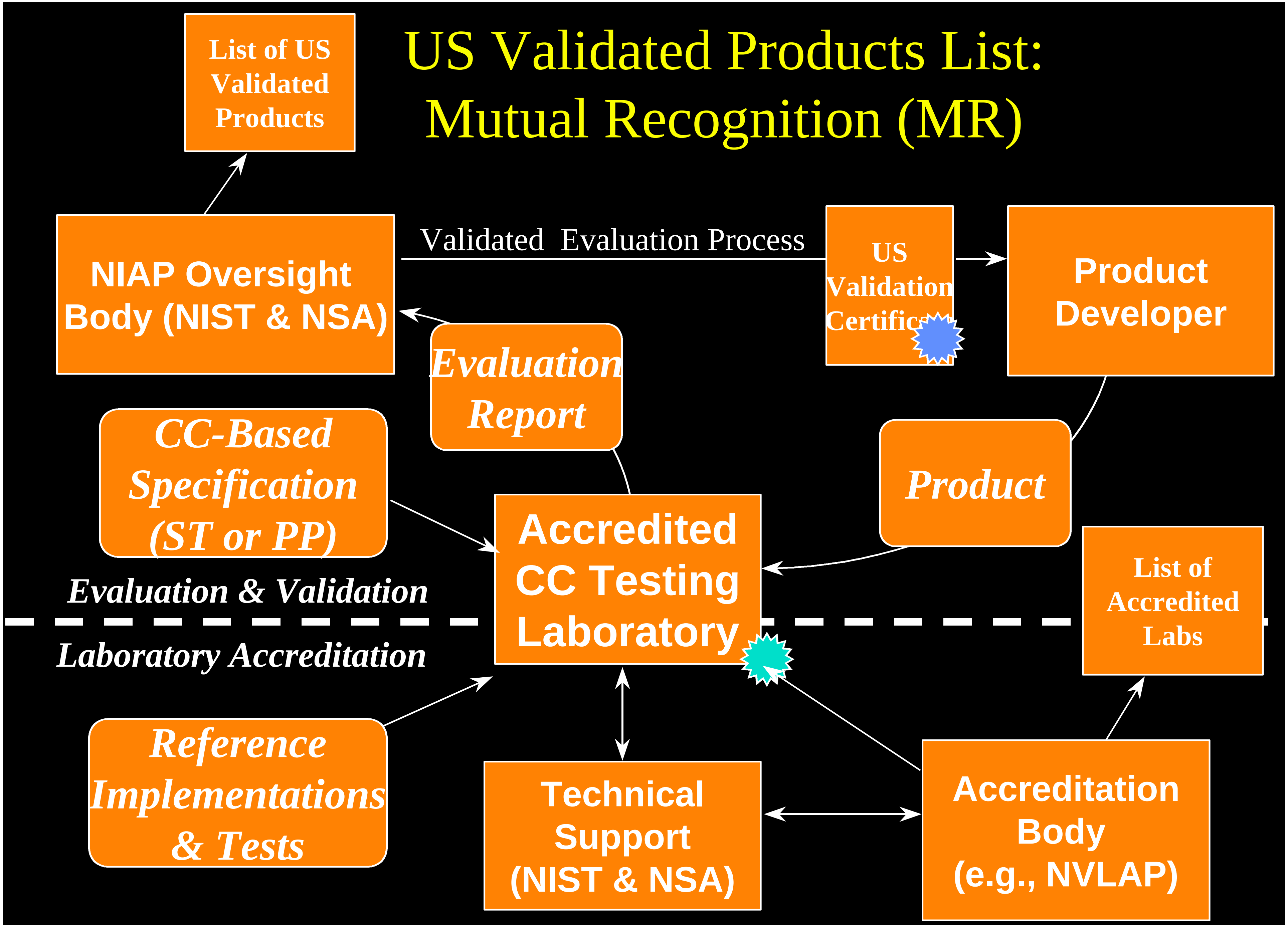
Security Target (ST)

Requirements for a specific TOE

- Security Objectives
- Functional Requirements
- Assurance Requirements
- Optional Extended Requirements
- Rationale

Extended (non-CC) Requirements

US Validated Products List: Mutual Recognition (MR)



List of US Validated Products

NIAP Oversight Body (NIST & NSA)

Validated Evaluation Process

US Validation Certificate

Product Developer

Evaluation Report

CC-Based Specification (ST or PP)

Product

Accredited CC Testing Laboratory

List of Accredited Labs

Evaluation & Validation

Laboratory Accreditation

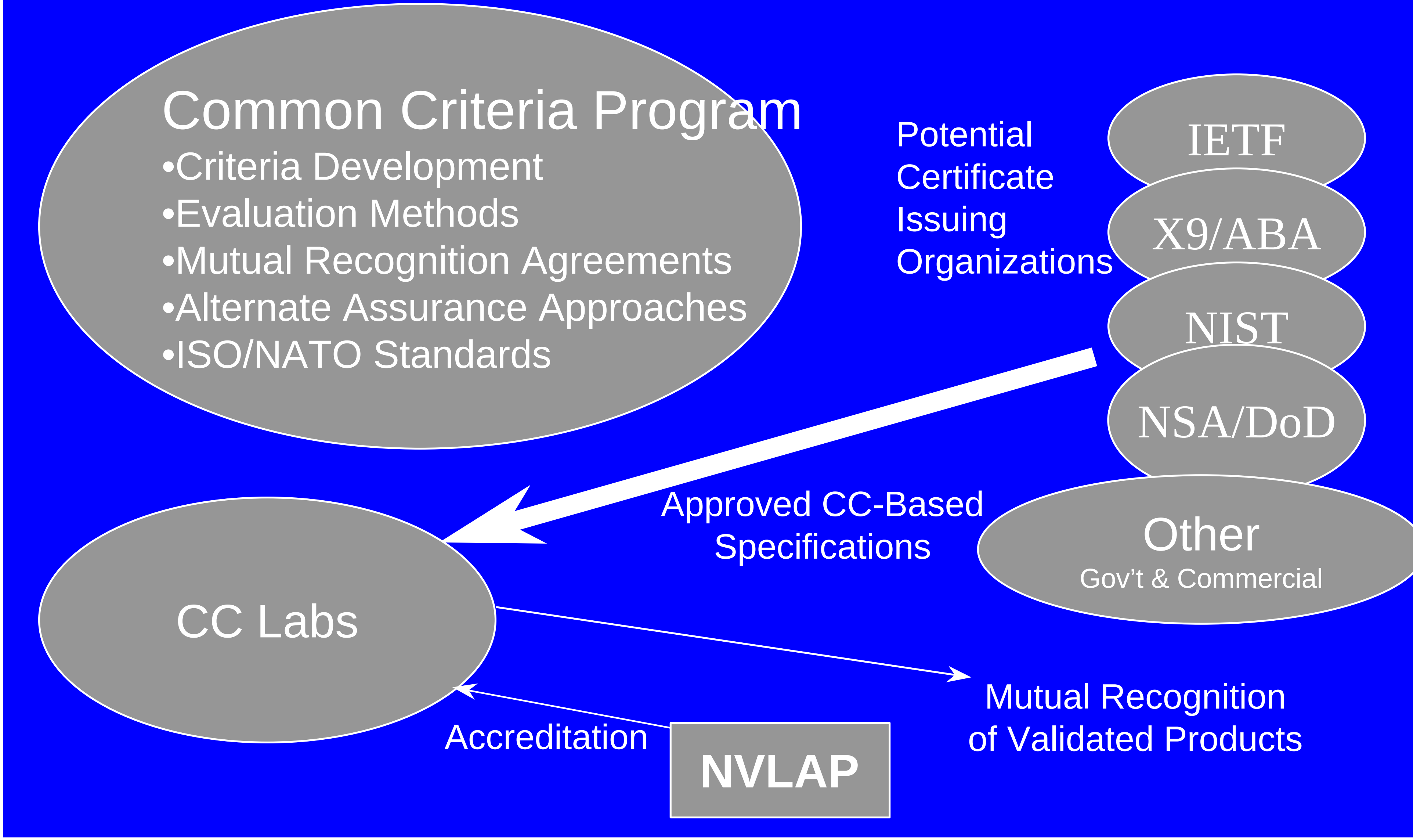
Reference Implementations & Tests

Technical Support (NIST & NSA)

Accreditation Body (e.g., NVLAP)

9/29/97

Role of the Common Criteria



Common Criteria Program

- •Criteria Development
- •Evaluation Methods
- •Mutual Recognition Agreements
- •Alternate Assurance Approaches
- •ISO/NATO Standards

Potential Certificate Issuing Organizations

IETF

X9/ABA

NIST

NSA/DoD

Other

Gov't & Commercial

Approved CC-Based Specifications

CC Labs

Mutual Recognition of Validated Products

Accreditation

NVLAP

Common Criteria Testing Program (CCTP)

- Successor to NSA (Orange Book) testing program
- Develops tests and methods
- Develops technical requirements for NVLAP accreditation criteria
- Supports NVLAP in accrediting commercial labs
- Results in NVLAP commercial labs
- NIST/NSA do NOT Perform Testing/Evaluation
- Requires an Oversight Body (National Information Assurance Partnership oversight role)

CCTP (continued)

- Developed Derived Test Requirements for EAL 1-3
- Developing national scheme documentation
- Developing laboratory proficiency tests
- Seeking NVLAP Accreditation of commercial labs
- Operational Q1 FY99 with multiple labs

National Information Assurance Partnership (NIAP) Oversight Role

- NIST/NSA oversight required due to subjectivity in evaluation process
- Supports and Maintains CC-Labs
  - lab accreditation/reaccreditation (NVLAP)
  - interpretations
  - validate lab evaluation report
  - quality control
  - develop tests for new requirements
- Member of International MR Group

Why the CC / CCTP?

- Evaluated components necessary (but not sufficient) for a secure infrastructure
- CC is widely recognized common language for developing and testing security specifications (ISO standard & FIPS)
- IT industry benefits by: one criteria; one evaluation; open market

Why the CC / CCTP? (cont.)

- Developed for government use
- Expectations: commercial sector will also use/require
- Foster US IT security testing/evaluation industry
- Focus on low cost, low end assurance for > 90 % of the commercial market

Support for the Common Criteria

- ISO standard
- Many other countries eager to join CC MRA (e.g., Japan, Australia, NZ, Korea, Sweden, Norway)
- Laboratory interest in accreditation
- Protection profile development activity
- Trail evaluations
- Guidance documents/automated support tools
- Evaluated products major component of DoD system security architecture

National Information Assurance Partnership (NIAP)

- Forum where US government & industry cooperatively:
  - develop security metrics, tests, test methods, tools, reference implementations, & “secure” protection profiles
  - conduct R & D in support of the above
- Supports commercial CC-based test laboratories

NIAP (continued)

- Establishes mutual recognition of CC-based evaluations
- Supports international development & recognition of PPs

NIAP (continued)

- Established joint NIST/NSA partnership Q4FY97
- Built lab facility for research and collaboration
- Recruited, hired, and staffed at about 20 FTEs (govt/contractors)
- Initiated Common Criteria Testing Program (CCTP)
- Initiated multiple projects: Firewall,Telecomm Switch, Automated Security Testing
- Started development of CC toolbox (tools, PP/ST registry, interpretations)

NIAP Goals

- Promote demand and investment in secure products
- Have trusted security products available at an affordable price and in a timely manner
- Transition operational security testing from government to commercial laboratories
- Foster a commercially viable security testing industry

CC Toolbox

- Develop automated tools for PP/ST preparation
- Describe the environment of a PP/ST
- Perform requirements mapping
- Perform consistency checking
- Capture interpretations
- Registration of PP/STs

Protection Profiles

- Firewall PPs
- Role Based Access Control (RBAC)
- Commercial Security (CS2)
- Extended Commercially Oriented Functionality Class (E-COFC)
- Telecomm & PBX Switch

Transition to the CCTP

- Trust Technology Assessment Program
  - Transfer of TPEP methodology to commercial evaluation facilities
  - Four labs approved for TCSEC C2 and B1
    - Two additional applications in process
  - Labs also approved to evaluate to Common Criteria using TPEP methodology
  - TTAP will migrate into CCTP

CC Achievements

- CC Protection Profile and Verification Requirements completed for TCSEC C2
  - Commercial facilities approved to evaluate
- Draft CC Protection Profile for TCSEC B1
- NIST/NSA Protection Profile for Firewalls and Routers
  - Commercial facilities approved to evaluate
- Labs report significant vendor interest

TPEP and Its Future

- Program initiated in 1986 to evaluate products to the Department of Defense Trusted Computer System Evaluation Criteria (Orange Book)
- Over 100 Products Have Obtained Ratings
- Program will continue to be used for high assurance Orange Book and for CC evaluations (EAL 5-7) if no commercial labs accredited
- NSA will migrate from Orange Book to Common Criteria Protection Profiles

Firewall PPs

- Developed Application Level & Traffic Filter Firewall PPs
- Minimal essential requirements for low risk environments
- EAL 2
- Delivered Q1FY98

RBAC

- Simplifies Access Control and Authorization Management over ACLs
- Allows specification & enforcement of enterprise specific security policy via roles
- Revised PP based on evaluation & public comment
- RBAC workshop industry participants (Tivoli, Cisco, Oracle, BDM, Schumann AG, Entrust)
- Due Q3 FY98

CS2

- Rooted in Minimum Security Functionality Requirements (MSFR)
- Developed for the Federal Criteria
- Updating to CC Version 2/EAL 2
- Balances cost of evaluation versus level of security provided
- Adding networking capability to PP
- Examining consolidation with E-COFC
- Due Q3 FY98

E-COFC

- ECMA work item (TC-36)
- Rooted in Minimum Security Functionality Requirements (MSFR)
- Baseline functionality for distributed commercial systems
- Develop a PP based on established commercial specifications
- Draft PP to ECMA Q3 FY98

Telecomm & PBX Switch PP

- Develop and publicly vet (with industry participants) EAL 2/3 PP
- Develop and vet suite of tests and procedures for the PP
- Due FY99

Oracle Trial Evaluation

- Oracle DBMS SQL Server 7.2
- Based on commercial DBMS (C-DBMS) PP/ST Developed By Logica/Oracle
- EAL 3/CCV 2.0
- Jointly evaluated by Cygnacom and NIST
- Gain experience and insight
- Due Q3 FY98

Security Assurance: Does Anybody Care?

— Consultant Viewpoint —

National Information Systems Security Conference
National Computer Security Center

Presented by

Douglas A. Webb, PhD
SRI Consulting

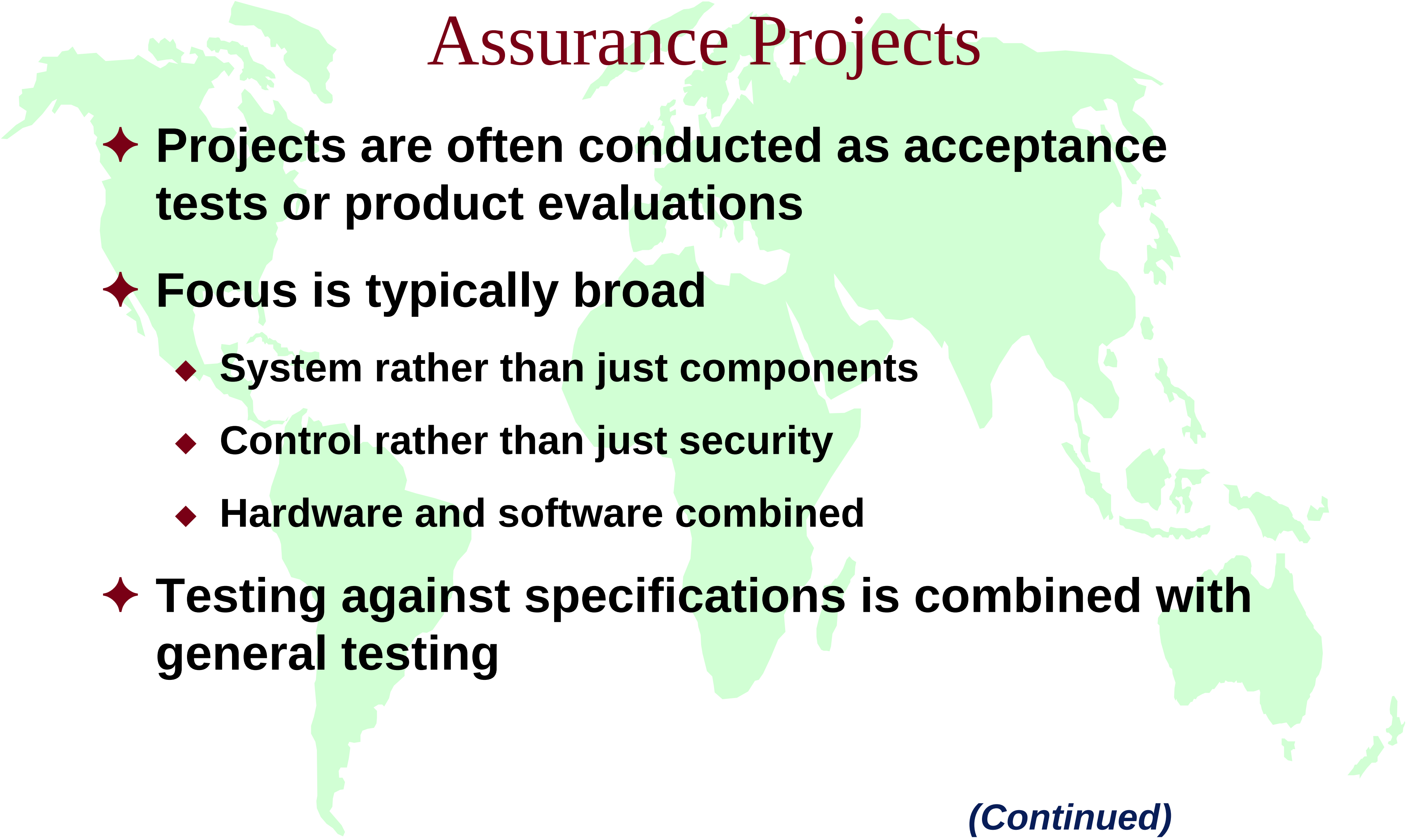
October 5-8, 1998

SRI CONSULTING
Subsidiary of SRI International

Agenda

- SRIC Security Assurance Projects
- NYCEP Project Overview
- Voting Machine Security Assurance Review
- Need or Desire for SA
- Alternative SA Approaches
- Assessing SA--Client’s View

SRIC Security Assurance Projects



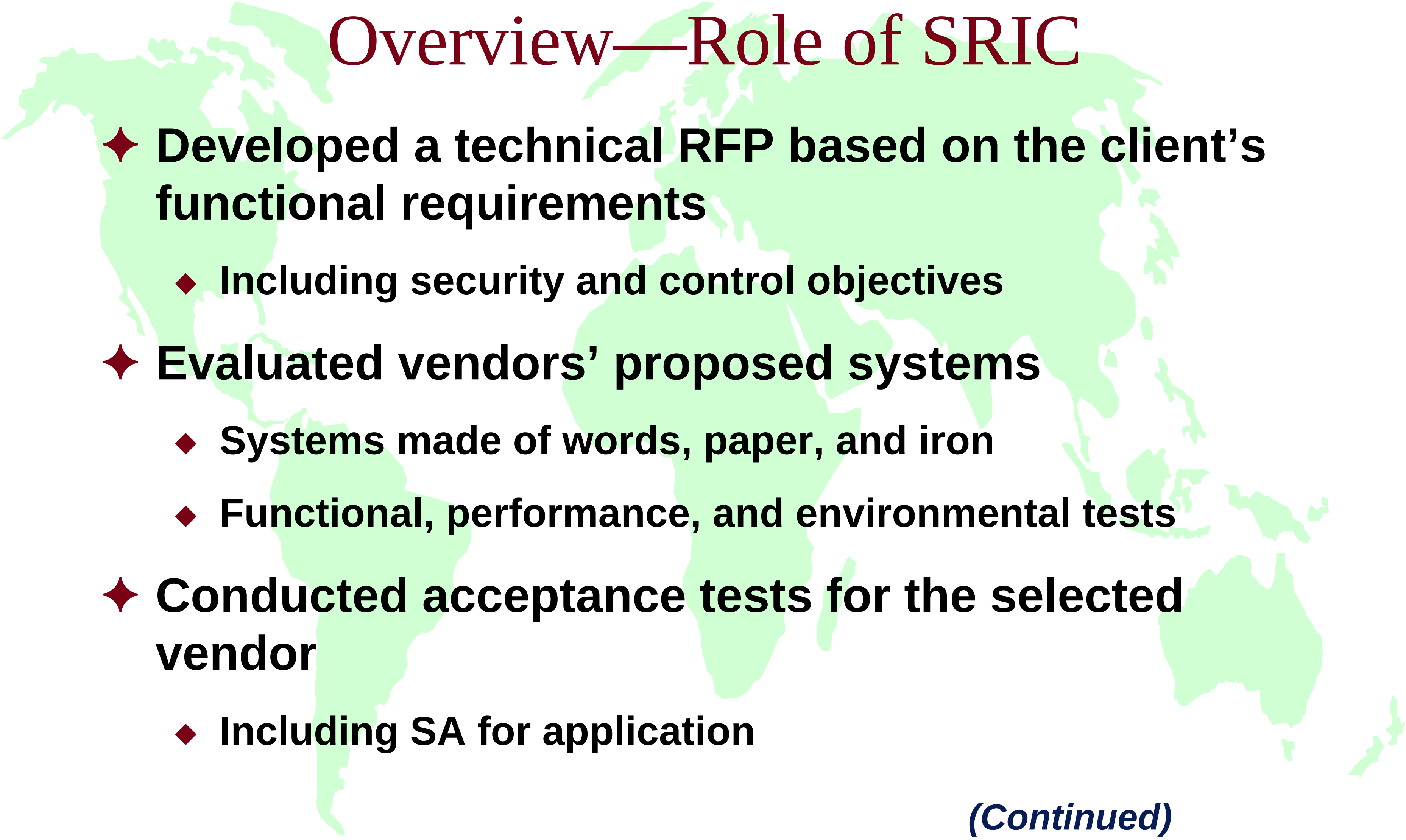
- ✦ Projects are often conducted as acceptance tests or product evaluations
- ✦ Focus is typically broad
  - System rather than just components
  - Control rather than just security
  - Hardware and software combined
- ✦ Testing against specifications is combined with general testing

(Continued)

SRIC Security Assurance Projects

- ✦ **Security requirements are combined with functional, performance, and environmental requirements**
- ✦ **Transforming security requirements into security specifications is not straightforward for one-of-a-kind products**

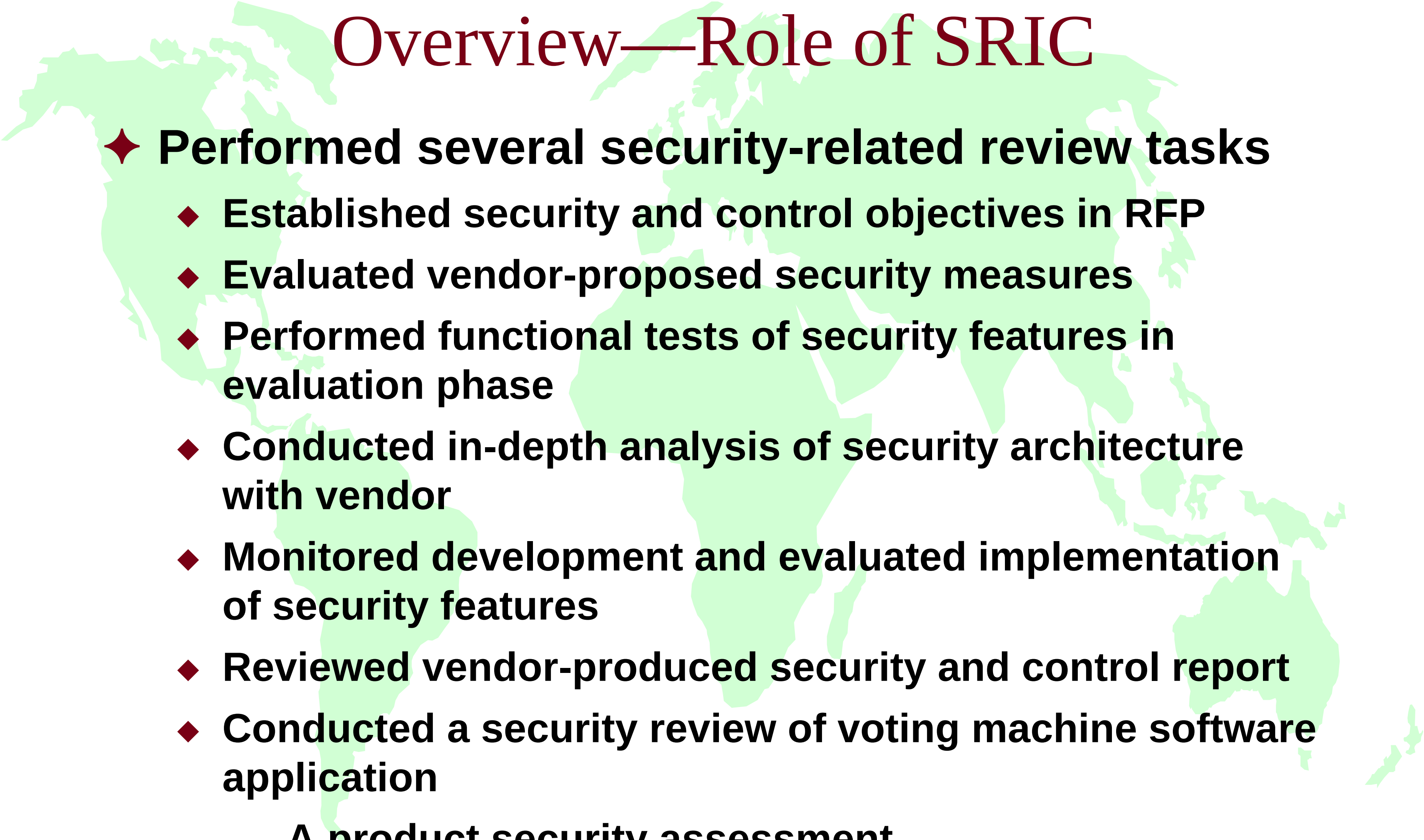
NYCEP Project Overview—Role of SRIC



- **Developed a technical RFP based on the client’s functional requirements**
  - **Including security and control objectives**
- **Evaluated vendors’ proposed systems**
  - **Systems made of words, paper, and iron**
  - **Functional, performance, and environmental tests**
- **Conducted acceptance tests for the selected vendor**
  - **Including SA for application**

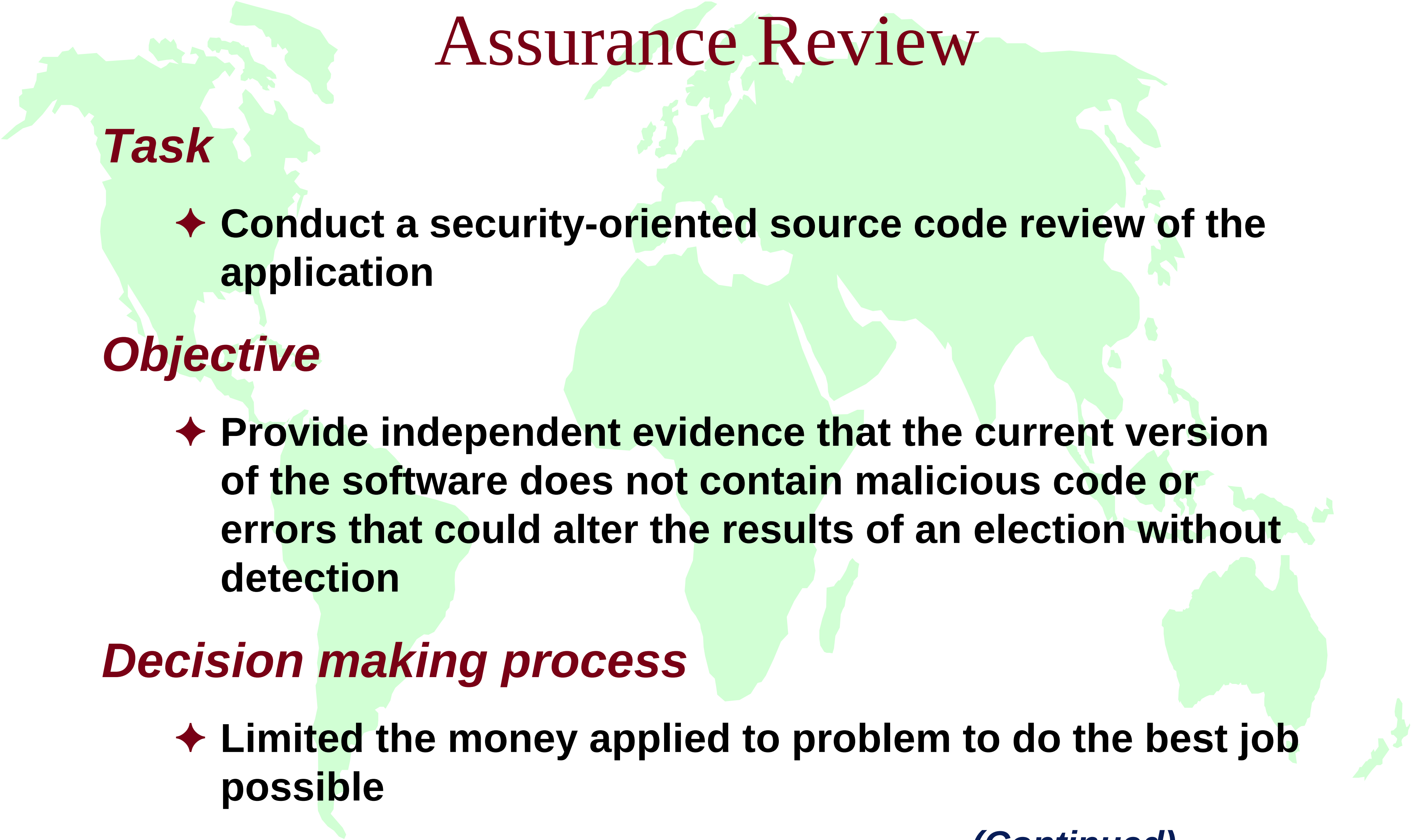
(Continued)

NYCEP Project Overview—Role of SRIC



- ✦ **Performed several security-related review tasks**
  - **Established security and control objectives in RFP**
  - **Evaluated vendor-proposed security measures**
  - **Performed functional tests of security features in evaluation phase**
  - **Conducted in-depth analysis of security architecture with vendor**
  - **Monitored development and evaluated implementation of security features**
  - **Reviewed vendor-produced security and control report**
  - **Conducted a security review of voting machine software application**
    - **– A product security assessment**

Voting Machine Security Assurance Review



Task

- ✦ Conduct a security-oriented source code review of the application

Objective

- ✦ Provide independent evidence that the current version of the software does not contain malicious code or errors that could alter the results of an election without detection

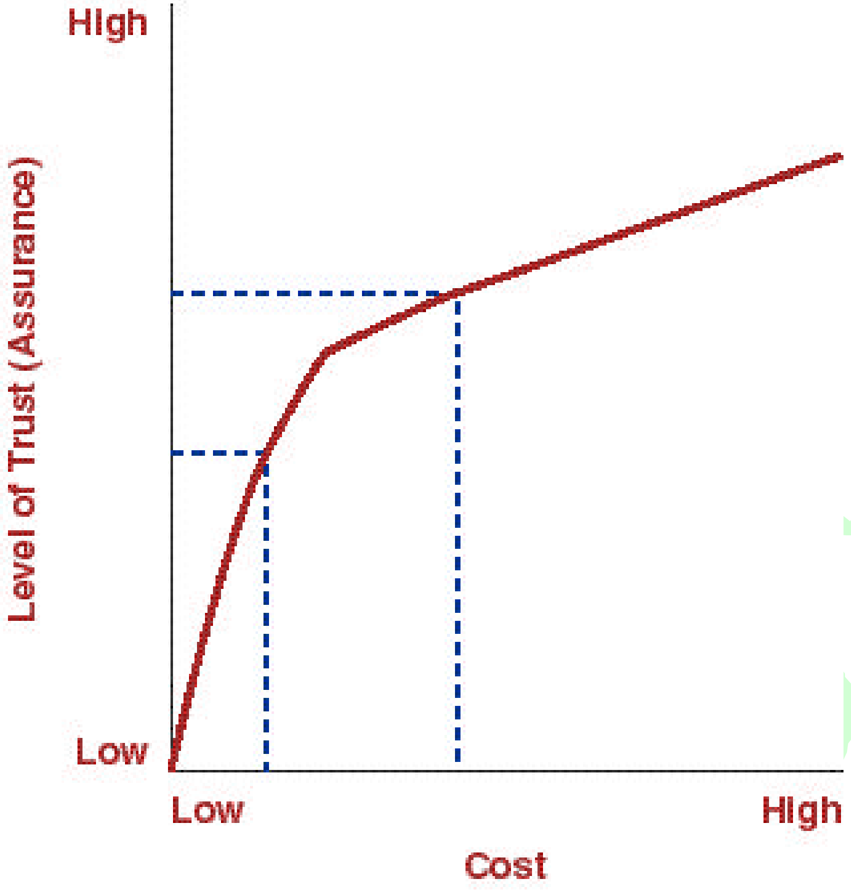
Decision making process

- ✦ Limited the money applied to problem to do the best job possible

(Continued)

Voting Machine Security Assurance Review

- Independent variable is cost, not assurance level
- Nonlinear relationship
- “Knee” is key point on curve



Need or Desire for SA

- Political (the good, the bad, and the ugly)
  - Each vote is a constitutional issue
  - Board would be embarrassed if a problem occurs (disruption may be worse than a limited security compromise)
  - Backroom pressures are intense
- Strong vendor competition
- Need to be clean and be seen as clean
- Bottom line
  - High need and desire for SA
  - Low need for any specific or formal certification

Alternative SA Approaches (Steps Considered by NYCEP)

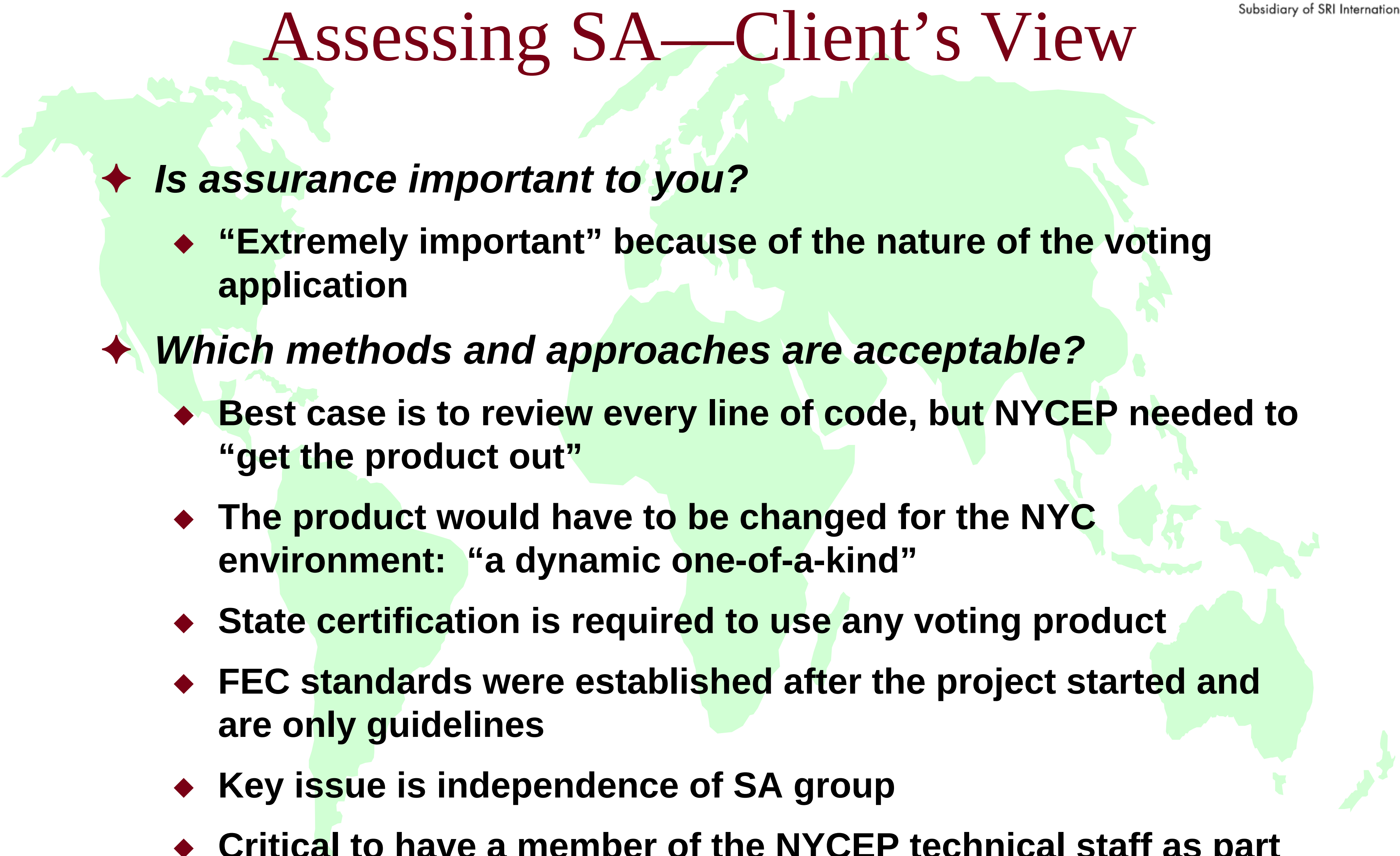
- ✦ **Accept the statements of the vendor**
- ✦ **Compare control points in the vendor's security model as contrasted to the SRIC-defined security model (control objectives)**
- ✦ **Discuss the security level with the vendor**
- ✦ **Perform functional and black-box testing against the specifications**

(Continued)

Alternative SA Approaches (Steps Considered by NYCEP)

- Conduct an in-depth team analysis with the client and vendor
- Conduct bread-board testing
- Conduct code review team discussion
- Require vendor to obtain state BOE certification
- Conduct code review by independent expert (i.e., product SA)
  - Formal review, evaluation, and report

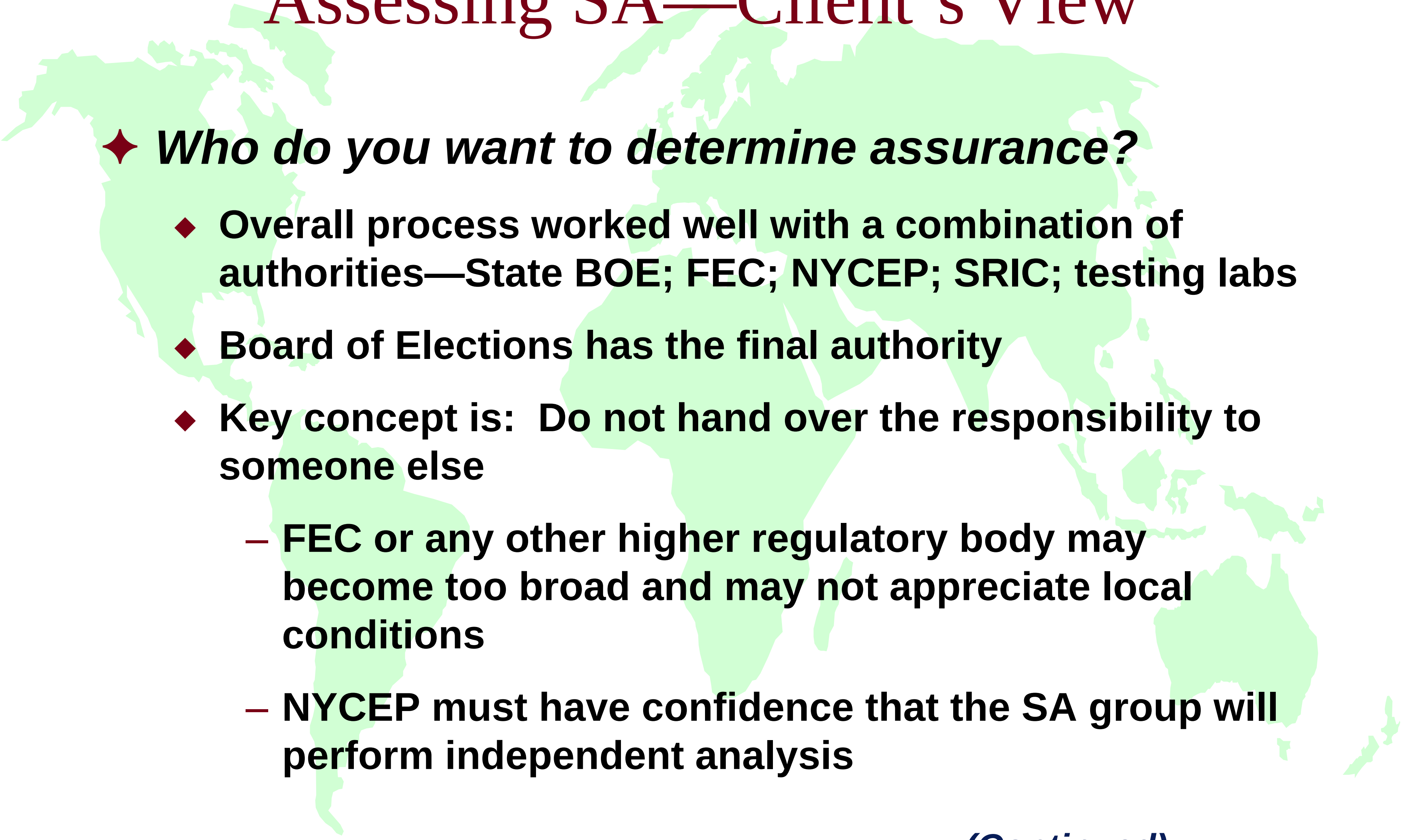
Assessing SA—Client’s View



- ***Is assurance important to you?***
  - **“Extremely important” because of the nature of the voting application**
- ***Which methods and approaches are acceptable?***
  - **Best case is to review every line of code, but NYCEP needed to “get the product out”**
  - **The product would have to be changed for the NYC environment: “a dynamic one-of-a-kind”**
  - **State certification is required to use any voting product**
  - **FEC standards were established after the project started and are only guidelines**
  - **Key issue is independence of SA group**
  - **Critical to have a member of the NYCEP technical staff as part of the SA process**

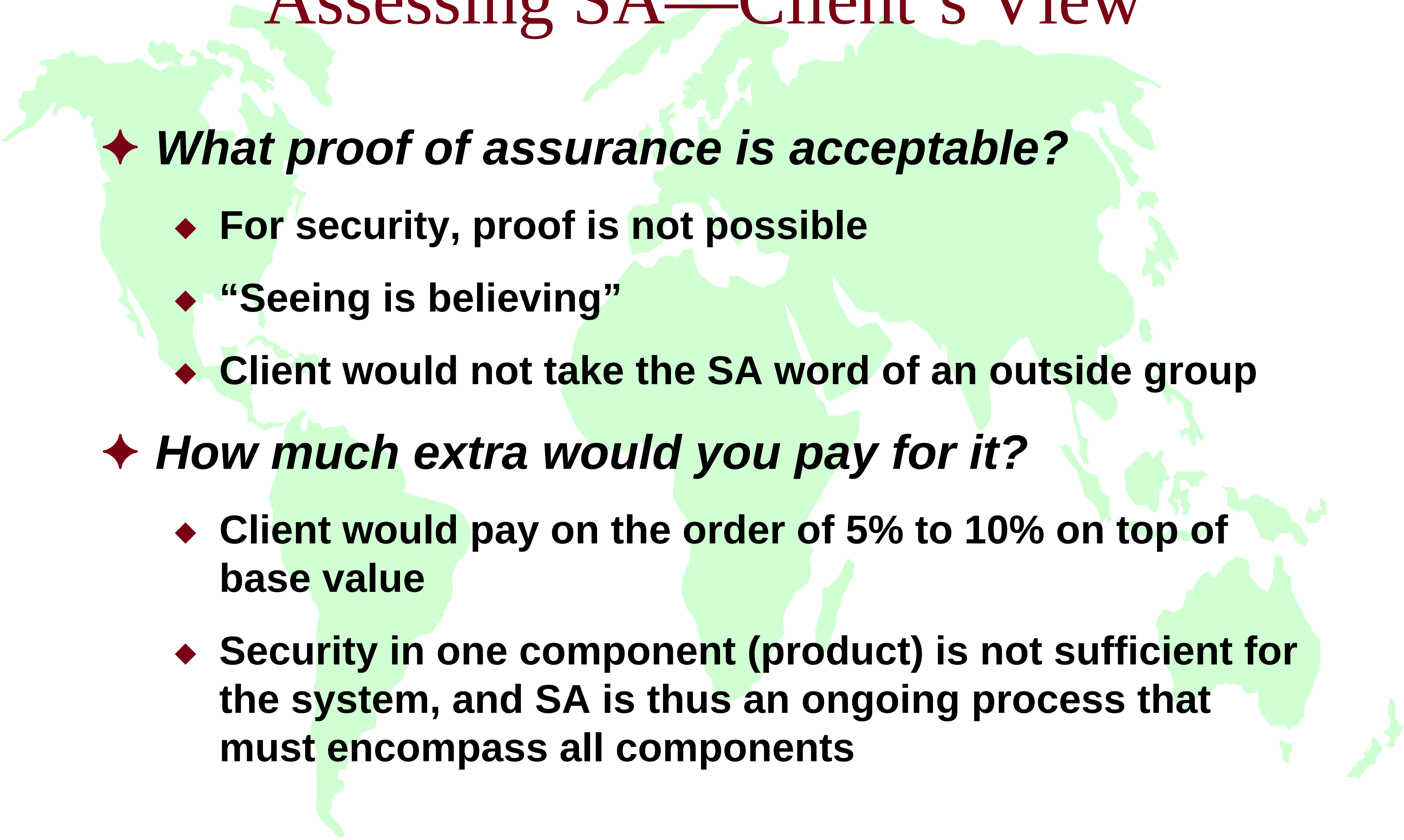
(Continued)

Assessing SA—Client’s View



- ***Who do you want to determine assurance?***
  - **Overall process worked well with a combination of authorities—State BOE; FEC; NYCEP; SRIC; testing labs**
  - **Board of Elections has the final authority**
  - **Key concept is: Do not hand over the responsibility to someone else**
    - **FEC or any other higher regulatory body may become too broad and may not appreciate local conditions**
    - **NYCEP must have confidence that the SA group will perform independent analysis**

(Continued)



Assessing SA—Client’s View

- ***What proof of assurance is acceptable?***
  - **For security, proof is not possible**
  - **“Seeing is believing”**
  - **Client would not take the SA word of an outside group**
- ***How much extra would you pay for it?***
  - **Client would pay on the order of 5% to 10% on top of base value**
  - **Security in one component (product) is not sufficient for the system, and SA is thus an ongoing process that must encompass all components**