

Protecting Federal Information Systems and Networks

*A Standards-based Security Certification Program
for Operational Environments*

Dr. Ron Ross

Today's Climate

- Highly interactive environment of powerful computing devices and interconnected systems of systems across global networks
- Federal agencies routinely interact with industry, private citizens, state and local governments, and the governments of other nations
- The complexity of today's information systems presents great security challenges for both producers and consumers of information technology

Today's Challenge

- Need for greater confidence in the security of enterprise information systems
- Need for consistency in the approaches used to assess the capabilities and limitations of information systems in Federal agencies
- Need for competent personnel with requisite skill sets to conduct information system assessments

Assurance in Information Systems

Building more secure systems requires --

- Well defined system-level security requirements and security specifications
- Well designed component products
- Sound systems security engineering practices
- Competent systems security engineers
- Appropriate metrics for product/system testing, evaluation, and assessment
- Comprehensive system security planning and life cycle management

Supporting Tools and Programs

Building more secure systems is enhanced by --

- Standardized Security Requirements and Specifications
 - ✓ **Common Criteria protection profile development project**
 - ✓ **Private sector protection profile contributions**
- Component-level Product Testing and Evaluation Programs
 - ✓ **Common Criteria Evaluation and Validation Scheme**
 - ✓ **Cryptographic Module Validation Program**
- Security Implementation Guidance
 - ✓ **Security Technical Implementation Guides**
 - ✓ **Security Reference Guides**
- System Certification and Accreditation

The Security Chain



Links in the Chain

(Non-technology based examples)

- ✓ Physical security
- ✓ Personnel security
- ✓ Procedural security
- ✓ Risk management
- ✓ Security policies
- ✓ Security planning
- ✓ Contingency planning

Links in the Chain

(Technology based examples)

- ✓ Access control mechanisms
- ✓ Identification and authentication devices
- ✓ Audit mechanisms
- ✓ Encryption mechanisms
- ✓ Firewalls
- ✓ Smart cards
- ✓ Biometrics

Adversaries attack the weakest link...where is yours?

National Policy

Office of Management and Budget Circular A-130, *Management of Federal Information Resources* requires Federal agencies to:

- Plan for security
- Ensure that appropriate officials are assigned security responsibility
- Authorize system processing prior to operations and periodically, thereafter.

Achieving Adequate Security

- OMB Circular A-130 defines *adequate security* as security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information
- Adequate security emphasizes the risk-based policy for cost-effective security established by Public Law 107-347, the Federal Information Security Management Act of 2002

System Accreditation

“An official management decision to authorize operation of an information system. This authorization, given by a senior agency official, is applicable to a particular environment of operation, and explicitly accepts the level of risk to agency operations (including mission, functions, image or reputation), agency assets, or individuals, remaining after the implementation of an agreed upon set of security controls...”

Security Certification

“A comprehensive evaluation of the management, operational, and technical security controls in an information system. This evaluation, made in support of the security accreditation process, determines the effectiveness of these security controls in a particular environment of operation and the remaining vulnerabilities in the information system after the implementation of such controls...”

Program Objectives

Phase I

- To develop standardized guidelines for conducting security certifications and accreditations of Federal information systems

Phase II

- To create a national network of accredited organizations capable of providing cost effective, quality security certification services based on the standardized guidelines

PHASE I

Development of Guidance

- NIST Special Publication 800-37
Guidelines for the Security Certification and Accreditation of Federal Information Information Systems
- NIST Special Publication 800-53
Minimum Security Controls for Federal Information Systems
- NIST Special Publication 800-53A
Procedures for the Verification of Security Controls in Federal Information Systems

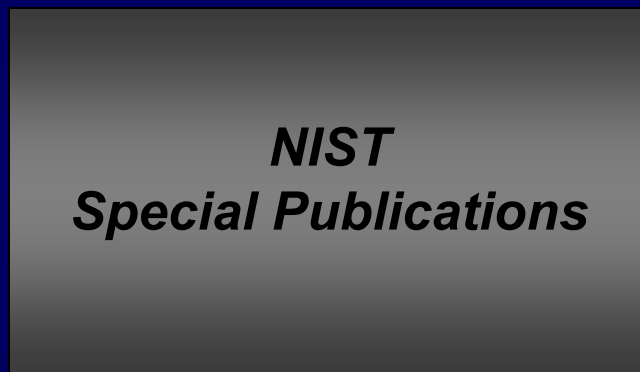
PHASE II

Development of Capability

- Create criteria for accrediting public and private sector organizations to conduct security certifications in accordance with NIST Special Publications 800-37, 800-53, 800-53A
- Develop associated proficiency tests to demonstrate assessment organization competence
- Accredite public and private sector enterprises to conduct security certifications by Fall 2005

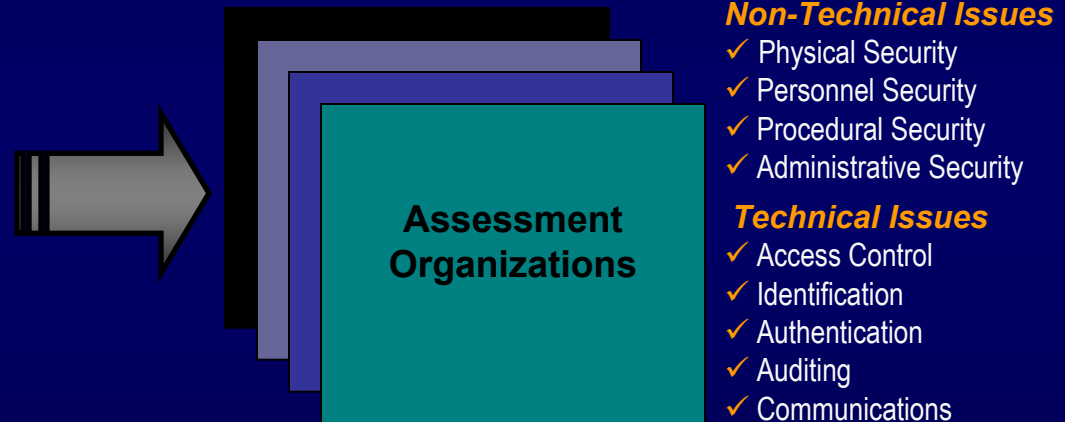
Comprehensive Security Program

Standardized Guidelines for Certification and Accreditation



A flexible, tailorable, and robust security certification process for federal agencies

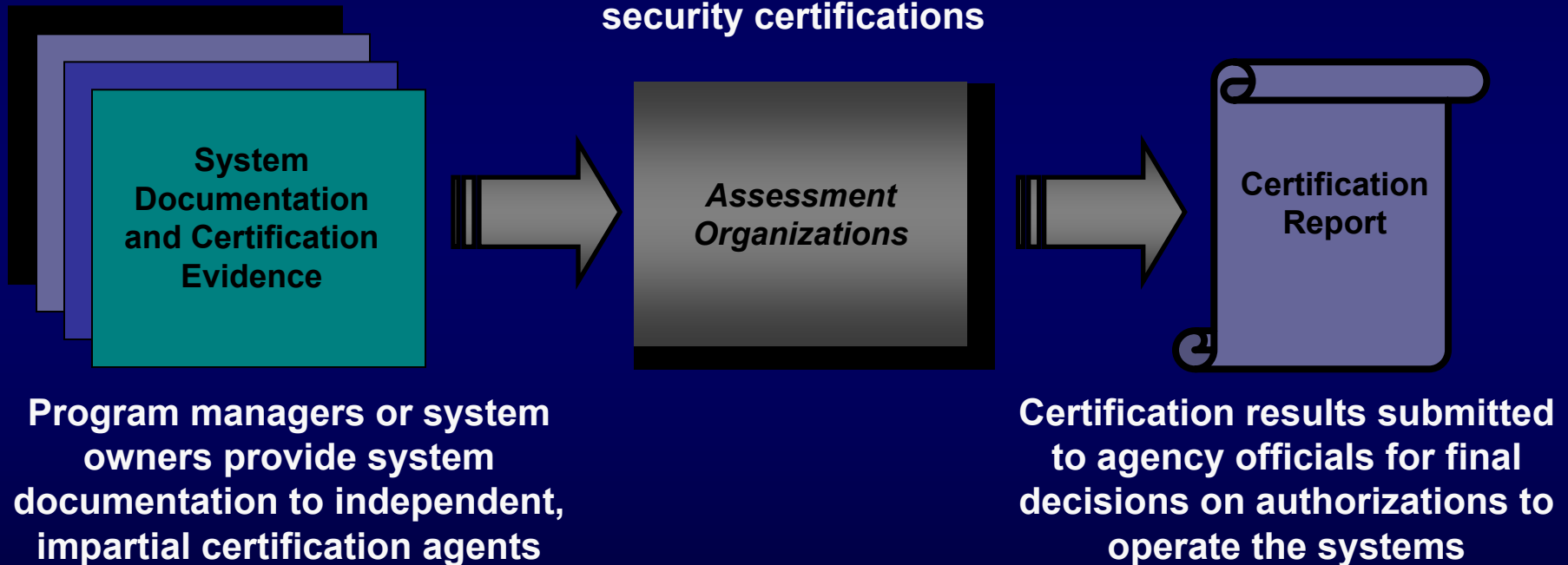
Network of Accredited Assessment Organizations



Competent providers of security assessment services

Assessing System Security

Public and private sector, accredited assessment organizations conduct security certifications



Significant Features

- Employs a standardized process for the certification and accreditation of information systems
- Integrates the use of standardized security controls and standardized verification procedures
- Minimizes documentation required and produced during the certification and accreditation process
- Maximizes the cost-effective production of essential evidence to support informed, risk-based accreditation decisions by senior agency officials

Significant Benefits

- More consistent, comparable, and repeatable system-level evaluations or system certifications of Federal information systems
- More complete, reliable technical information for information system accreditation authorities—leading to better understanding of complex systems and associated risks and vulnerabilities
- Greater availability of competent certification services for public and private sector customers

Special Publication 800-37

Guidelines for the Security Certification and Accreditation of Federal Information Systems

- Establishes a standard process, general tasks and specific subtasks to certify and accredit information systems supporting the executive branch of the Federal government
- Applicable to non-national security information systems; can also be applied to national security or intelligence systems, if so directed by appropriate authorities
- Replaces NIST Federal Information Processing Standards (FIPS) Publication 102

Special Publication 800-53

Minimum Security Controls for Federal Information Systems

- Provides standardized security controls for confidentiality, integrity, and availability
- Arrays controls in a standard package of basic controls for low risk systems
- Offers optional controls in agency-defined supplemental package for moderate and high risk systems
- Integrates security controls from many sources—policies, directives, and guidelines (e.g., NIST SP 800-26, DoD 8500, D/CID 6-3, ISO/IEC 17799, and GAO FISCAM)

Note: Projected publication June 2003.

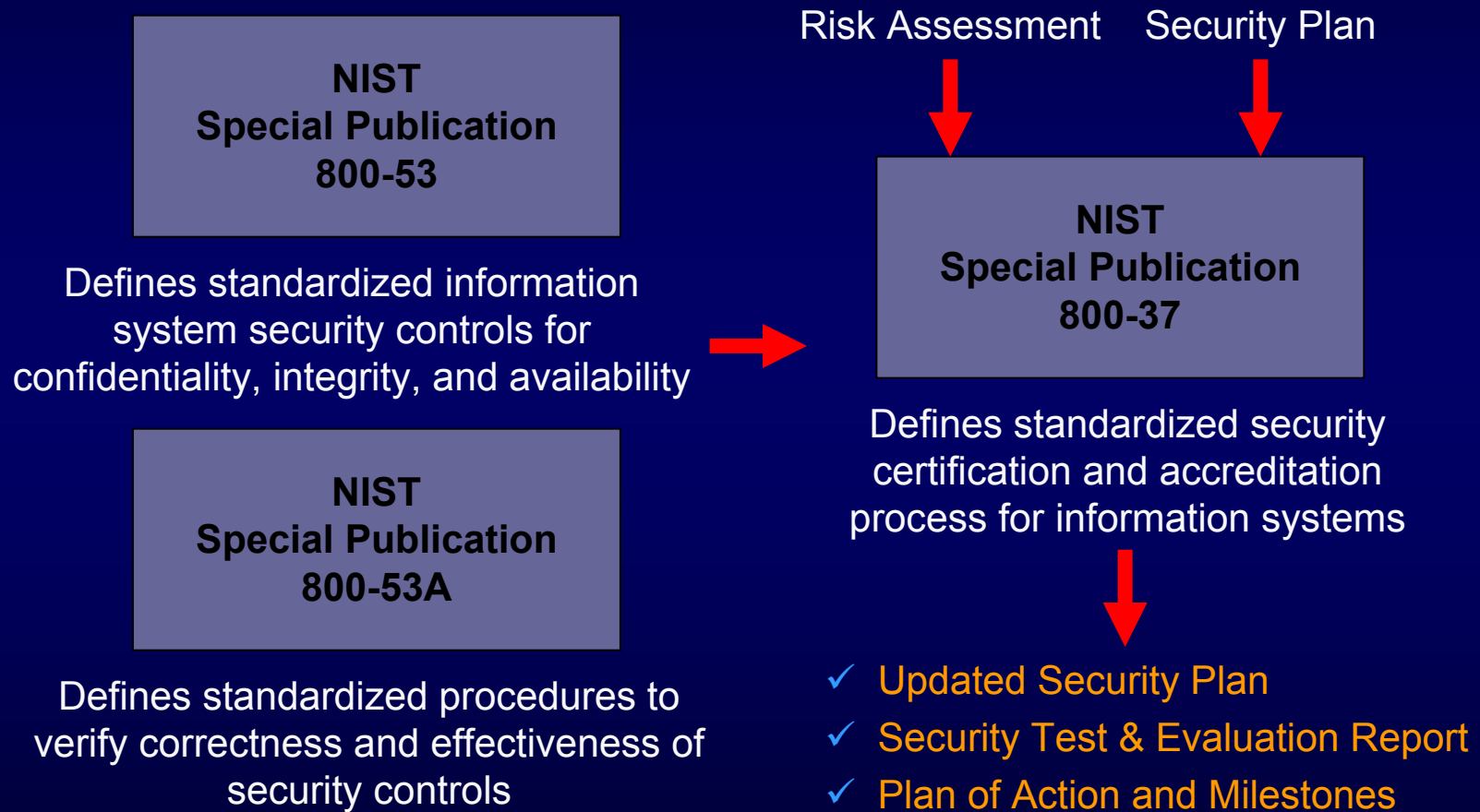
Special Publication 800-53A

Procedures for the Verification of Security Controls in Federal Information Systems

- Provides standardized verification procedures for security controls in SP 800-53
- Associates verification procedures with the level of rigor applied to the security test and evaluation activities
- Specifies certifier actions necessary to demonstrate correct and effective implementation of security controls in SP 800-53

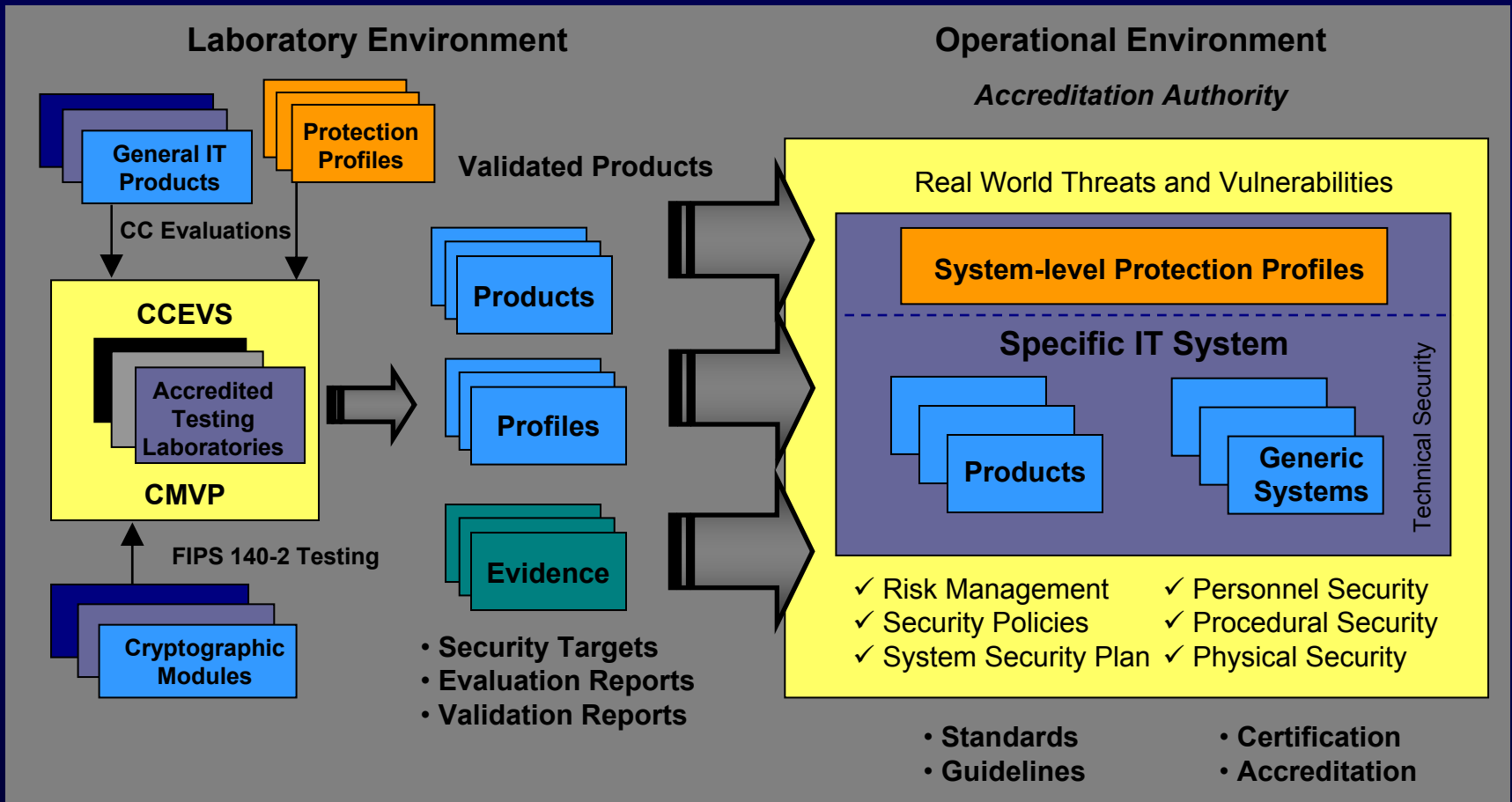
Note: Projected publication June 2003.

Security Accreditation Model



A Comprehensive Approach

Linking Critical Assessment Activities



Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

Program Manager

Dr. Ron S. Ross
(301) 975-5390
rross@nist.gov

Special Publications

Marianne Swanson
(301) 975-3293
marianne.swanson@nist.gov

Gov't and Industry Outreach

Dr. Stu Katzke
(301) 975-4768
skatzke@nist.gov

Assessment Scheme

Arnold Johnson
(301) 975-3247
arnold.johnson@nist.gov

Organization Accreditations

Patricia Toth
(301) 975-5140
patricia.toth@nist.gov

Technical Advisor

Gary Stoneburner
(301) 975-5394
gary.stoneburner@nist.gov

Comments to: sec-cert@nist.gov

World Wide Web: <http://csrc.nist.gov/sec-cert>