

National Information Assurance Partnership®
NIAP 2000



Building More Secure Systems for the New MillenniumSM

NIAP[®] Roadmap



- Introduction
- Partnership Objectives
- Program Areas, Activities, and Services
- FY 2000 Projects
- NIAP Certification and Accreditation Initiatives
- Summary

Today's Climate

- Rapidly changing information technologies and compressed technology life cycles
- Growing complexity of IT products and systems
- Increasing connectivity among systems
- Dependence on commercial off-the-shelf IT products and systems
- Need for greater assurance in critical information infrastructures (both public and private sector)

Introducing NIAP

- NIAP is a partnership between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) to meet the security testing needs of information technology (IT) producers and consumers
- The long-term goal of NIAP is to increase the level of trust consumers have in their systems and networks through the use of cost-effective testing, evaluation, and validation programs

Partnership Objectives

- Promote the development and use of evaluated IT products and systems
- Champion the development and use of national and international standards for IT security
- Foster development of IT security requirements, test methods, tools, techniques, and assurance metrics
- Support a framework for international recognition and acceptance of IT security evaluation results
- Facilitate the development and growth of a commercial IT security testing industry within the U.S.

Activities and Services

- Promote government and industry forums for the development of IT security requirements and specifications
- Support information systems security testing, evaluation and assessment programs
- Provide a state-of-the-art, web-based repository of security requirements and testing information
- Sponsor IT security classes, conferences, and workshops for product developers, testing laboratories and consumers
- Collaborate with industry in the development of advanced tools, techniques, and methods for security testing

Program Areas

- Security Requirements Definition and Specification

How do we tell product and systems developers what types of IT security we want?

- Product and System Security Testing, Evaluation, and Assessment

How do we know if developers produced what we asked for?

- Information Assurance Research

How can we improve the ways we achieve assurance in our products and systems?

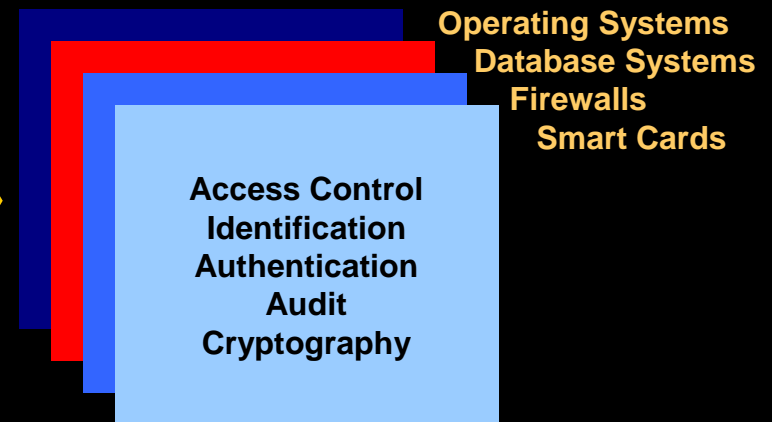
Defining Requirements

ISO Standard 15408



*A flexible, robust catalogue of
IT security requirements
(features and assurances)*

Protection Profiles



*Consumer-driven security
requirements in specific
information technology areas*

Industry Responds



Protection Profile

Security Targets

Firewall Security Requirements

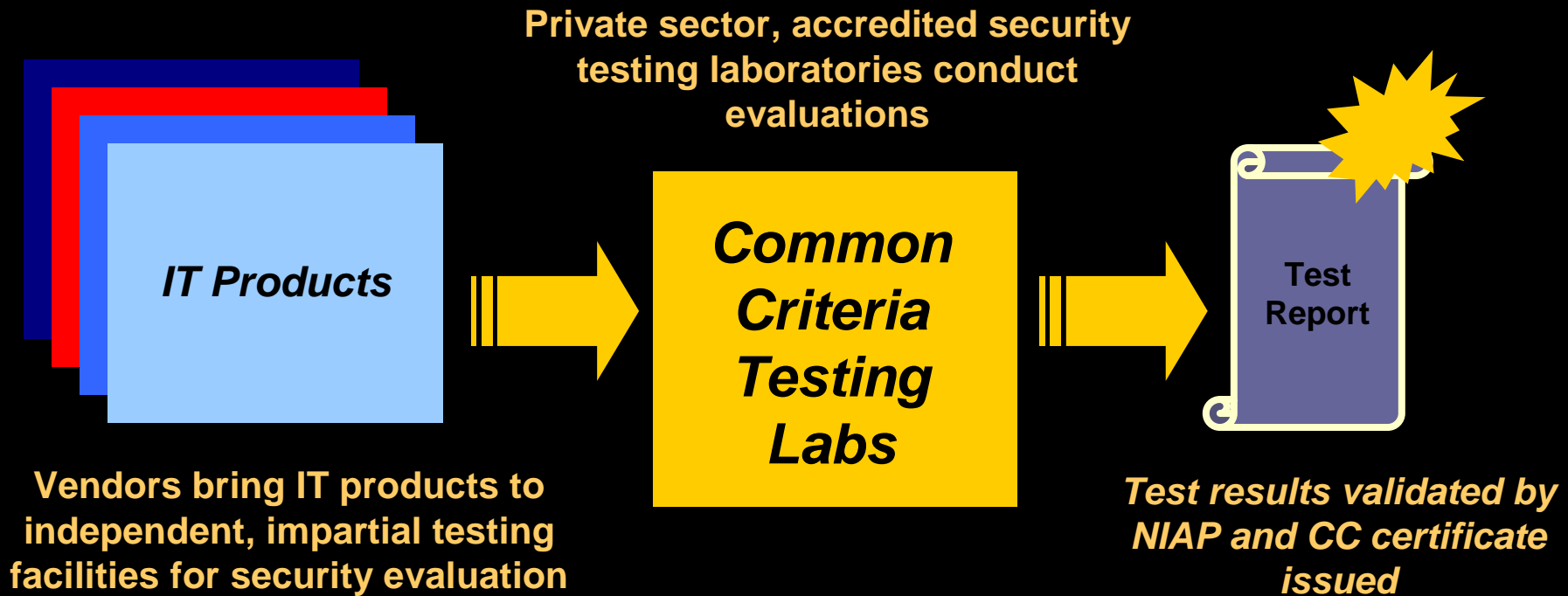
Security Features and Assurances

Firewall Product 4
Firewall Product 3
Firewall Product 2
Firewall Product 1

A consumer statement of security requirements to industry

Vendors statements of security claims for their IT products

Demonstrating Conformance



Mutual Recognition

NIAP, in conjunction with the U.S. State Department, negotiated a CC Recognition Arrangement that:

- Provides recognition of U.S. issued certificates by 13 nations:

Canada, United Kingdom, France, Germany, Australia, New Zealand, Greece, Norway, Finland, Italy, Spain, Netherlands, Israel

- Eliminates need for costly security evaluations in more than one country
- Offers excellent global market opportunities for U.S. IT industry

NIAP 2000 Projects

- Common Criteria Evaluation and Validation Scheme
- Cryptographic Module Protection Profile Development
- Healthcare Security Forum
- Smart Card Security Forum
- Telecommunications Security Forum
- Common Criteria Toolbox™
- Automated Security Testing
- Threat and Vulnerability Research
- INFOSEC Assessment Program / Certification & Accreditation

Certification & Accreditation Initiatives



- National Level C&A Policy - OMB A-130
- National Level C&A Implementation - FIPS-102
- Dept of Defense NIACAP - DITSCAP Programs
- Major Policy Drivers - Private Sector
 - HIPPA - Healthcare
 - Graham / Leach / Wiley - Banking and Finance
 - Insurance Industry - Cyber System Policies
 - Legal - ‘Due Diligence’
- C&A Certification Criteria ??
- Commercial Laboratory Assessments ??

NIAP - IATF 'Certification and Accreditation' Forum

- January 25 - NIST Red Conference Room
- Agenda
 - OMB
 - NIST
 - NIACAP-DITSCAP
 - Healthcare Views
 - Insurance Industry Views
 - Audit Industry Views
 - IT Industry Views
- Register Online - www.iatf.net - \$50 includes Lunch+ Breaks

Summary



NIAP is helping secure the critical information infrastructure (public and private sectors) by:

- Promoting the development of standard security requirements and specifications
- Increasing the security of IT systems through wider availability of evaluated products
- Providing IT industry with an opportunity to sell evaluated products in world-wide markets

Contact Information

**National Information Assurance Partnership
100 Bureau Drive Mailstop 8930
Gaithersburg, MD 20899-8930**

Director

Dr. Ron S. Ross
NIST-ITL
(301) 975-5390
ross@nist.gov

Deputy Director

Terrance Losonsky
NSA-V1
(301) 975-4060
tmloson@missi.ncsc.mil

Technical Advisor

R. Kris Britton
NSA-V1
(410) 854-4458
britton@radium.ncsc.mil

Email: niap-info@nist.gov

World Wide Web: <http://niap.nist.gov>

Today's Challenge

- Consumers have access to an increasing number of security-enhanced IT products with different capabilities and limitations
- Consumers must decide which products provide an appropriate degree of protection for their information systems
- *Impact: choice of products affects the security of systems in the critical information infrastructure*

What is Needed?

- Producers of IT products need to have a better understanding of consumer's information security requirements
- Consumers of IT products need to have better ways to:
 - ▣ specify desired security features
 - ▣ assess the security claims made by producers

Activities and Services

- Operate the Common Criteria Evaluation and Validation Scheme (CCEVSSM) for IT Security
- Issue Common Criteria certificates for IT products that have been successfully evaluated and validated
- Support the international Common Criteria Recognition Arrangement for IT security evaluations
- Maintain list of approved testing laboratories, validated products, and test methods
- Provide state-of-the-art automated tools and information sources for security requirements definition and testing

NIAP Testing Advantages

- Specification of security features and assurances based on an international standard
- Evaluation methodology based on an international standard---leading to comparability of test results
- Testing laboratory expertise assessed by NIST's National Voluntary Laboratory Accreditation Program---an internationally recognized program based on standards
- Quality technical oversight provided by NIST/NSA experts
- Testing results recognized by many nations

Education and Training

- International Common Criteria Conference
- Protection Profile Development Classes
- Common Evaluation Methodology Classes
- CC Evaluation and Validation Scheme
Technical Workshops
- Information Assurance Workshops

Automated Tools

Helping Consumers



IT Product
Security
Requirements

Helping Industry



IT Product
Security
Specifications

The screenshot shows a software interface with a menu bar (File, Report, Help) and a toolbar (New, Open, Save, Exit, Security Target, Protection Profile, MSA Status, EAL Value). Below the toolbar are tabs: Interactive, EAL, Contrast, Allocation, Elaboration, Report, User's Guide. The main area has a 'Prompt' section with the text 'Do you wish to describe the Security Functions of the TOE?' and 'Answer Options' with 'Yes' and 'No' radio buttons and an 'Accept' button. Below this is a table with columns for Assurance Classes, Assurance Families, Assurance Components by Evaluation Assurance Level (EAL1-EAL7), and Fragmenting Components.

Assurance Classes	Assurance Families	Assurance Components by Evaluation Assurance Level							Fragmenting Components
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7	
Configuration management	ACM_AUT				1	1	2	2	
	ACM_CAP	1	2	3	4	4	5	5	
	ACM_SCP			1	2	3	3	3	
Delivery and operation	ADO_DEL		1	1	2	2	3		
	ADO_OES	1	1	1	1	1	1	1	2
Development	ADV_FSP	1	1	1	2	3	3	4	
	ADV_HLD		1	2	2	3	4	5	
	ADV_IMP				1	2	3	3	
	ADV_INT					1	2	3	
	ADV_LLD				1	1	2	2	3