National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) Briefing to IAPB

23 March 2006

Audrey M. Dale

Director, NIAP CCEVS

Agenda

- A Historical Perspective
- Governing Policies
- Terminology
- NIAP/CCEVS in a Nutshell
- Where we are Today – Organization, CCRA, Products, Labs, Validators
- Issues – IDA Study, GAO Audit
- Other Actions

A Historical Perspective

- 1983- 1997 NSA's National Computer Security Center (NCSC) used DoD TCSEC (Orange Book or DoD 5200.28-STD) criteria within the Trusted Product Evaluation Program (TPEP) (totally government funded - using gov & FFRDC evaluators)
- 1997 – NIST & NSA Implemented Trusted Technology Assessment Program (TTAP) using Orange Book, Common Criteria & evaluations by approved commercial labs with NSA oversight.
- 1997 – Letter of partnership signed between NIST & NSA establishing the National Information Assurance Partnership (NIAP).

A Historical Perspective

- 1998 – International Common Criteria Version 2.0 published
- 1999 – CC V2.0 adopted as ISO Standard 15408
- 2000 – NIAP/CCEVS program implemented using Common Criteria & evaluations by accredited commercial labs with government oversight/validation
- 2003 – NSA begins assumes total responsibility for resourcing and running the CCEVS

Governing Policies

- **NSTISSP 11 -** National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products that protect national security information. Mandated all these types of products be evaluated by CC, NIAP or FIPS beginning in Jul 2002
- **DoD Directive 8500.1, Oct 2002 –** DoD policy mandating compliance with NSTISSP 11, requiring products to be evaluated or in evaluation (with successful evaluation a condition of the purchase)
- **DoD Instruction 8500.2, Feb 2003 –** DoD policy mandating product being evaluated also conform to a Government Protection Profiles (whenever one exits)

Terminology

- Evaluation Assurance Level (EAL)
- Protection Profile (PP)
- Security Target (ST)
- Target of Evaluation (TOE)
- Evaluators
- Validators
- Evaluation Technical Report (ETR)
- Evaluated Products List (EPL)
- Common Criteria Testing Methodology (CCTL)

Terminology

Evaluation Assurance Levels

- ***EAL 1*** *– Functionally tested. The product has been functionally tested using available off-the-shelf vendor documentation. Doesn't require vendor cooperation. NIAP no longer performs EAL 1 evaluations.*
- ***EAL 2*** *– Structurally tested. The product has been functionally tested using available off-the-shelf vendor documentation as well as some vendor design documentation to support more complete functional testing. Requires vendor co-operation with delivery of design information.*
- ***EAL 3*** *– Methodically tested and checked. The product has been functionally tested with more insight into the design and more test coverage.*
- *Developer must provide evidence of a search for obvious flaws.*
- ***EAL 4*** *– Methodically designed, tested and reviewed. The product has been functionally tested with even more insight into the design and more comprehensive test coverage. Testing supported by independent search for obvious vulnerabilities (accomplished by NIAP lab and vendor)*
- *(NOTE: EAL 4 is the highest level that is mutually recognized by the Common Criteria Recognition Arrangement (CCRA).)*
- ***EAL 5*** *– Semiformally designed and tested. In addition to more evidence provided by the vendor, the product must also have been developed with a rigorous development approach. Beginnings of use of formal methods and covert channel analysis and modular design. Independent search for vulnerabilities by attacker with moderate attack potential is accomplished by NSA.*
- ***EAL 6*** *– Semiformally verified design and tested. Formal methods and systematic covert channel analysis required. Product must be modular and layered in design. Independent search for vulnerabilities by attacker with high attack potential is accomplished by NSA.*
- ***EAL 7*** *– Formally verified design and tested. More formal methods and systematic covert channel analysis required. Product must be modular and layered in design. Independent search for vulnerabilities by attacker with high attack potential is accomplished by NSA. The complexity of the products design must be minimized. Complete independent confirmation of developer test results.*

NIAP in a Nutshell

National Information Assurance Partnership

NIST

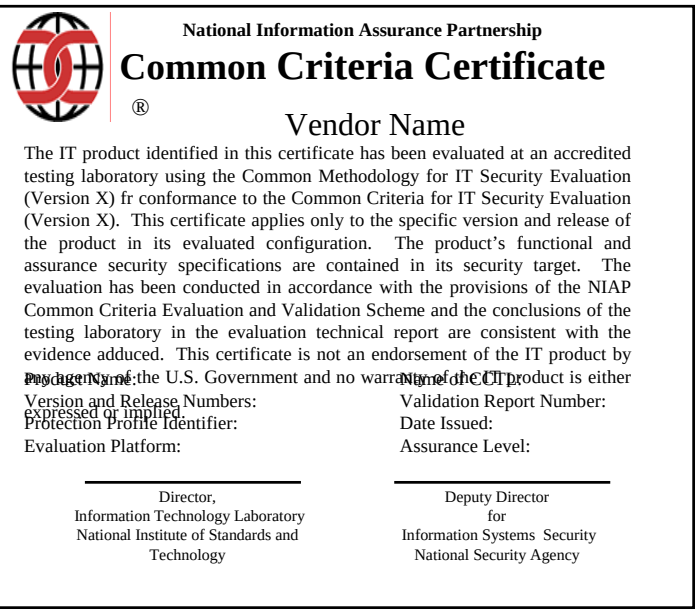
NATIONAL SECURITY AGENCY
UNITED STATES OF AMERICA

NIAP

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

CCEVS in a Nutshell

- Evaluations performed by NVLAP accredited labs
- Vendors negotiate evaluation costs with accredited labs
- NSA provides penetration testing support to EAL4+ and above evaluations (government personnel only)
- Validation/oversight performed by NIAP government & NIAP funded FFRDC personnel
- Product evaluated against vendor written Security Target (ST) and/or Government Protection Profile (PP)
- NIAP issues CC certificate to vendor upon successful completion of evaluation



National Information Assurance Partnership

Common Criteria Certificate

®

Vendor Name

The IT product identified in this certificate has been evaluated at an accredited testing laboratory using the Common Methodology for IT Security Evaluation (Version X) fr conformance to the Common Criteria for IT Security Evaluation (Version X). This certificate applies only to the specific version and release of the product in its evaluated configuration. The product's functional and assurance security specifications are contained in its security target. The evaluation has been conducted in accordance with the provisions of the NIAP Common Criteria Evaluation and Validation Scheme and the conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence adduced. This certificate is not an endorsement of the IT product by any agency of the U.S. Government and no warranty of the IT product is either expressed or implied.

Product Name:
Version and Release Numbers:
Protection Profile Identifier:
Evaluation Platform:

Name of CCTL:
Validation Report Number:
Date Issued:
Assurance Level:

Director,
Information Technology Laboratory
National Institute of Standards and Technology

Deputy Director
for
Information Systems Security
National Security Agency

CCEVS Process Summary

Government Protection Profiles identify sets of security and assurance requirements for specific technology types

Vendor submits Security Target, IA or IA-enabled product and required documentation to NIAP Lab for evaluation

Performed by Government funded FFRDC & contractor personnel

VALIDATION

- Oversee
- Review
- Validate
- Report

N I A P

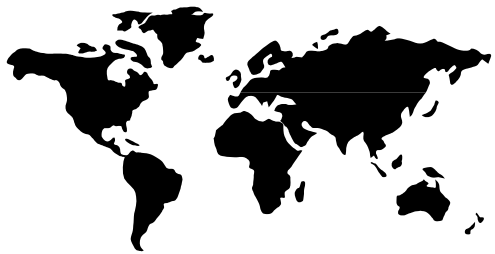
EVALUATION

Commercial Evaluation Facility

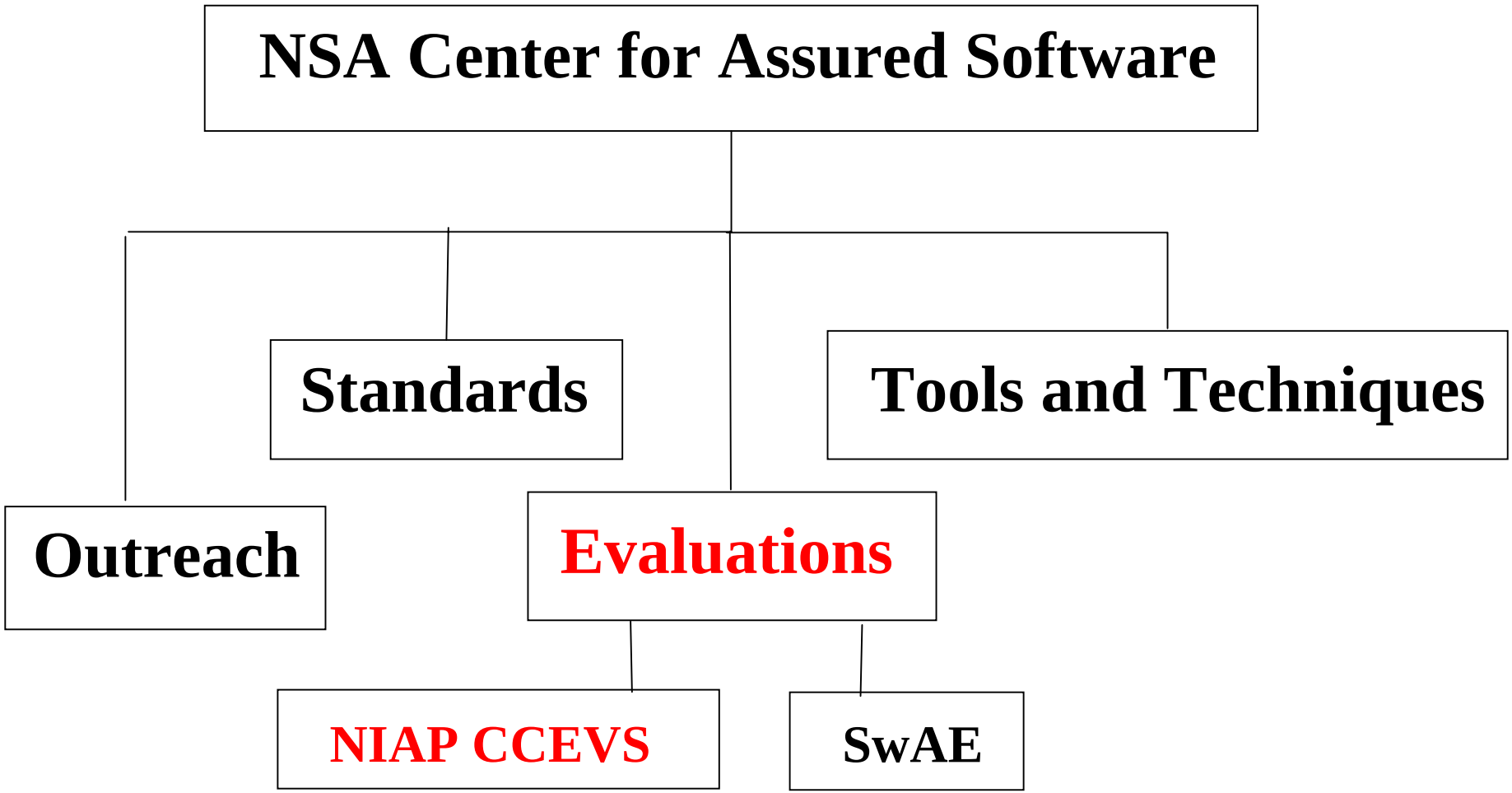
- Analyze
- Test
- Document
- Report

For EAL4+ and above evaluations, product is brought into NSA for vulnerability assessment evaluation

10 NIAP Accredited Labs



Where We Are Today - Organization



Common Criteria Recognition Arrangement (CCRA)

Certificate Producers

US

Canada

UK

Germany

France

Netherlands

Norway

Japan

Australia/New Zealand

Denmark

Finland

Greece

Italy

Spain

Israel

Sweden

Austria

Turkey

Hungary

Czech Republic

Singapore

India

Certificate Consumers

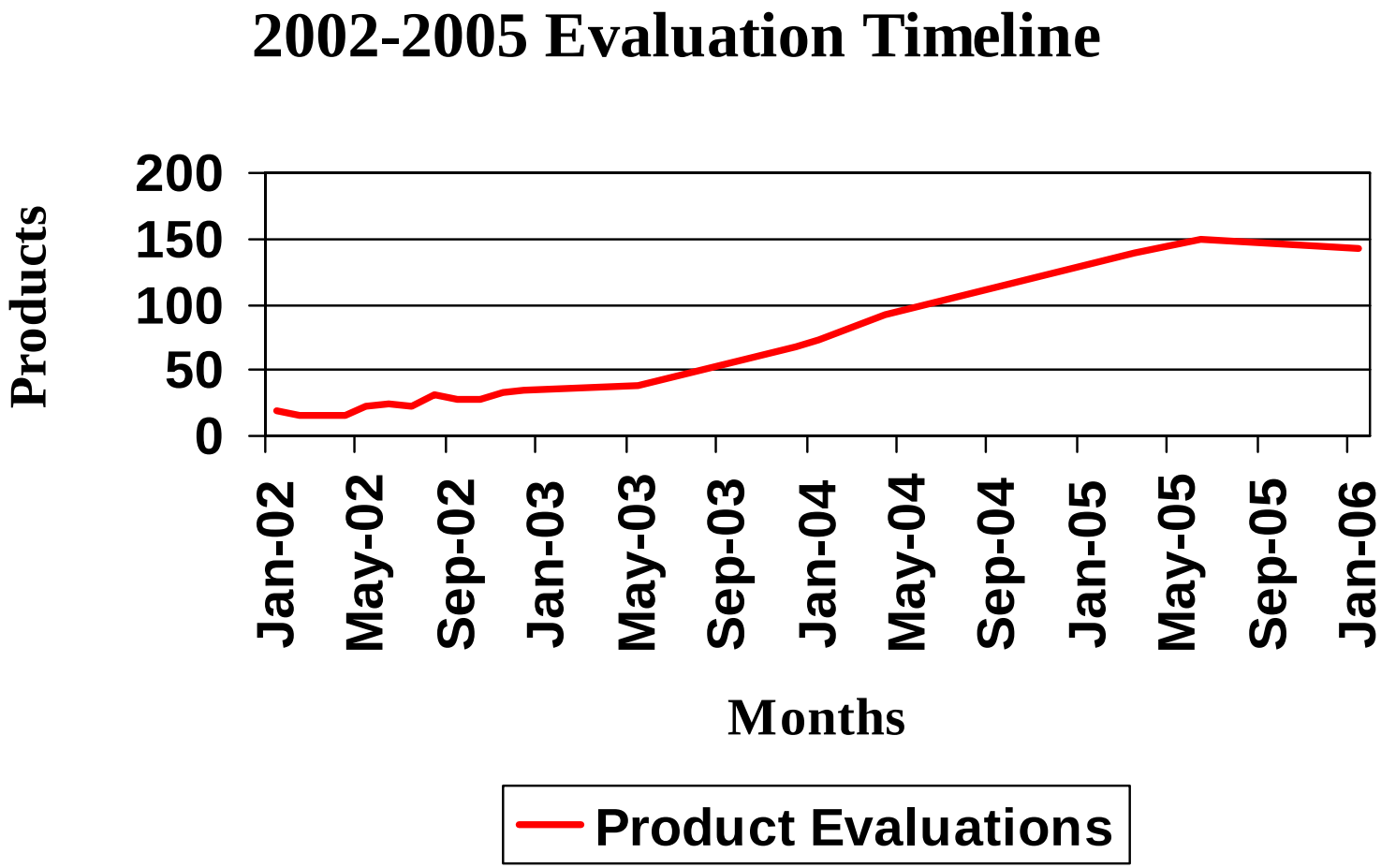
International Common Criteria Mutual Recognition Arrangement

- Mutually recognizes evaluations up through EAL 4
- CC Recognition Arrangement (CCRA) – now up to 23 signatories
  - 3 more nations have formally applied to become certificate producers: Sweden, South Korea*, Spain
  - Italy planning to formally apply
  - Singapore, India and Denmark added in 2005/2006 as certificate consuming nations
  - Inquiries made from China, Russia and Iran
- CCv3.0 put out for public comment on CC website on 4 Jul 2005, expect CCv3.X to be published in Jul 2006

Snapshots During 2000, 2003 & 2005

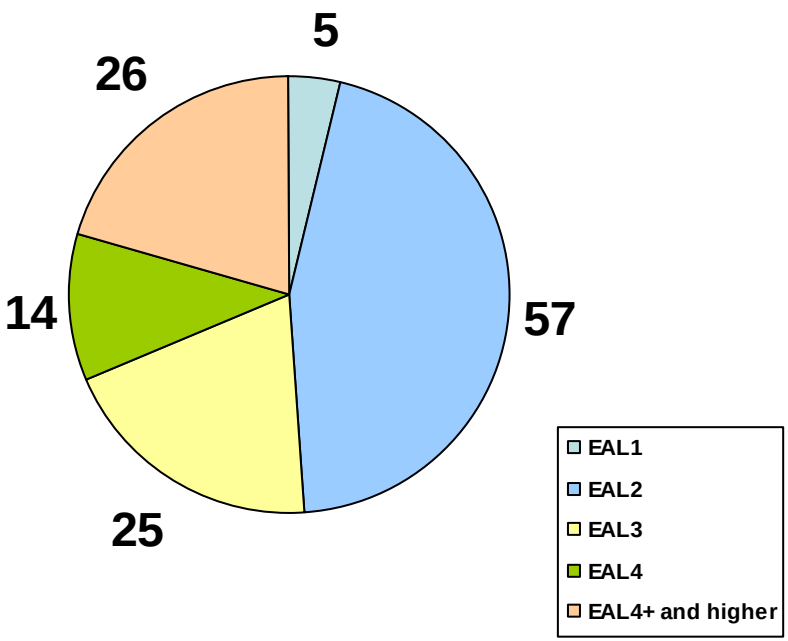
Oct 2000	Jun 2002	July 2005
4 CCTLs	6 CCTLs	10 CCTLs
2 Products in Evaluation	40 Products in Evaluation	154 Products in Evaluation
$3.0M	$3.2M	$6.38M

Where we are Today - Products

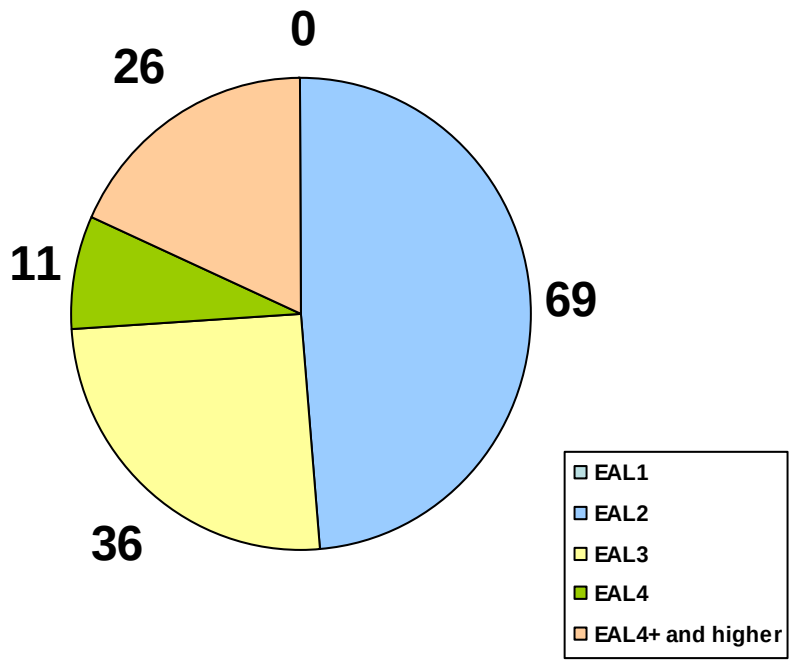


Where We Are Today - Products

127 Completed Product Evaluations
(approx 3-4 completed each month)



142 Product Evaluations in Progress
(approx 5-7 new entries each month)



EAL 1 - 4 = Basic

EAL 4+ - 7 = Medium/High

Accredited Testing Laboratories - CCTLs

1.	**Booz Allen Hamilton**	Linthicum, Maryland
2.	**Arca**	Sterling, Virginia
3.	**atsec**	Austin, Texas
4.	**COACT, Inc.**	Columbia, Maryland
5.	**Computer Sciences Corp.**	Annapolis Junction, MD
6.	**Criterian Independent Labs**	Fairmont, West Virginia
7.	**CygnaCom Solutions, Inc.**	McLean, Virginia
8.	**InfoGard Laboratories, Inc.**	San Luis Obispo, CA
9.	**Science Applications Int'l Corp.**	Columbia, MD
10.	**Lockheed Martin**	Hanover, MD

Plus 4 Candidate Labs (Ashton, BKP, BT, DIAL)

CCTL Evaluation Facts

- Prices and Evaluation Time for *typical* evaluations:
  - EAL 2 (e.g. IDS,Firewall,Router,Switch) ~$100-170K, 4-6 months
  - EAL 3 (e.g. Firewall, IDS – PP Compliant) ~$130 -225K, 6-9 months
  - Simple EAL 4 (e.g. IDS, Firewall, Router, Switch) ~$175K- $300K, 7-12 months
  - Complex EAL 4 (e.g. Operating System – PP Compliant) ~$300K-750K, 12-24 months
- Consulting & document prep costs can easily add $25K-200K to an evaluation

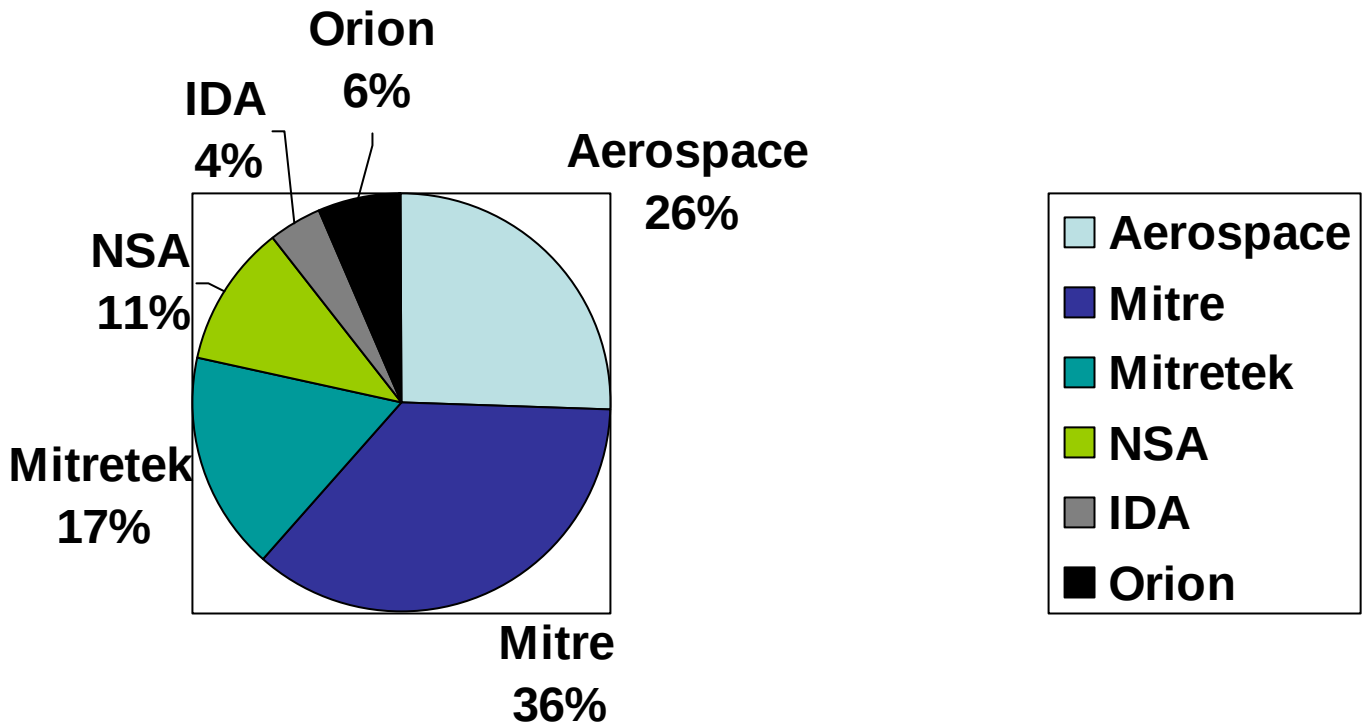
CCTL Evaluation Findings & Fixes

- Average of 2 to 3 fixes per product
- Bugs found in nearly all products – even mainstream large company products
- Examples of findings & fixes:
  - Bugs in password mechanism
  - Bugs in audit mechanism
  - Access control flaws
  - Management function feature bugs
  - Document (ST) findings/corrections

Validator Resources

- Aerospace - FFRDC
- Mitre - FFRDC
- IDA - FFRDC
- Mitretek – Not for Profit
- Orion – SETA Contractor
- NSA - Government

Validator Resource Breakdown



IDA Draft Report Findings

- **Report recommends continuing and improving NIAP**
- NIAP accomplishing nearly all of its goals; limited funding puts its future in jeopardy
- Deficiencies exist in NIAP relative to
  - Development and use of Protection Profiles
  - Fixing/strengthening Common Criteria requirements and deliverables
  - Training
  - Development of tools to aid in evaluation
  - Linkage between evaluation and the Certification and Accreditation process
- Provided 6 Options to DoD and DHS for NIAP's Future

IDA Draft Report Findings Relative to Criteria, Protection Profiles (PP) and Security Targets (ST)

- All relevant IA functions of the product must be in ST Target Of Evaluation (TOE) (not always the case today) – policy published in Feb 06
- All PPs and STs should include Flaw Remediation and Assurance Maintenance Requirements – being considered
- Additional PP's need to be developed at the basic assurance levels to support general use (Vendors would like nested PP's from basic to high) – participating in DoD PP Strategy
- Criteria needs to be updated – CCv3.X due out in Jul 06

IDA Draft Report
Other Issue Areas Identified

- Education of Stakeholders – on-going but limited due to resources
- Research Areas that should be pursued
  - Tools – will be addressed via re-alignment under CAS
  - Alternate Forms of Assurance – being investigated
- Critical Infrastructure (Banking, Electric, Water Systems) – cannot pursue due to resource constraints – looking to partner with DHS & other government agencies
- Product Evaluation Relationship to Certification and Accreditation of systems – researching but to a limited degree due to resource constraints

GAO Audit Report Goals

- Identify the government-wide benefits of NIAP evaluation process on national security systems
  - Independent testing & evaluation of products giving agencies confidence that products will perform as advertised
  - International recognition
  - Discovery of software flaws
  - Improvements in vendor development processes
- Identify the potential benefits and challenges of expanding the requirement for NIAP to non-national security systems including sensitive but unclassified systems
  - Expanding NIAP requirement to non national security benefits may yield many of the same benefits and challenges but could exacerbate resource constraints

GAO Audit Report Recommendations

- Develop training & awareness workshops for program participants in coordination with vendors, labs and industry associations – plan to work with vendors, labs and industry associations (such as the CC Vendor's Forum) to find creative, low-cost ways to provide training and awareness to the community
- Consider collecting, analyzing, and reporting metrics on the effectiveness of NIAP tests and evaluations; such metrics could include summary information on the number of findings, flaws, and associated fixes – planning has already begun for gathering these metrics during and at the end of the evaluations

Actions Taken to Improve NIAP CCEVS

- Policies:
  - TOE Policy – mandates "reasonable" TOEs so the small portions or products will no longer be accepted into evaluation – published Feb 06
  - Letter of Intent Policy – mandates vendors give us information/rationale for obtaining NIAP evaluation – published Feb 06
  - Testing Policy – will establish minimum standards for NIAP labs for vulnerability assessments and testing – being written
- Other Actions:
  - Developing templates for NIAP labs to report all important evaluation finding & fixes
  - Working with ICSA to determine how we can "partner" with them and give vendors who obtain ICSA certifications "credit" within NIAP evaluations
  - Researching how we can incorporate NIAP results into C&A processes
  - Partnering with NSA Information Systems Security Engineers in supporting the security needs of their customers (i.e. major DoD programs)

Questions ?

Important Web Sites

NIAP CCEVS: http://niap.nist.gov/cc-scheme

CC Portal: http://www.commoncriteriaportal.org

Protection Profiles: http://niap.nist.gov/pp/index.html

Validated Products:

http://niap.nist.gov/cc-scheme/Validated Products.html

Contact Information

Audrey M. Dale
National Security Agency
9800 Savage Road, STE 6740
Fort George G. Meade, MD 20755-6740

amdale@missi.ncsc.mil **phone: (410) 854-4458**
http://niap.nist.gov/cc-scheme **fax: (410) 854-6615**