Institute for Defense Analyses
4850 Mark Center Drive • Alexandria, Virginia 22311-1882

A Comprehensive Review of the National Information Assurance Partnership

Edward Schneider/William Simpson

Institute for Defense Analyses (IDA)

ACSAC 2005

Product Evaluation Case Study

Study undertaken by IDA of a US organization

- Probably also applies to other national Common Criteria (CC) bodies
- Comments on security evaluations

Agenda / Outline

- National Information Assurance Partnership (NIAP) Review
- Evaluation Context
- Analysis Approach
- Top-Level Findings
- Options

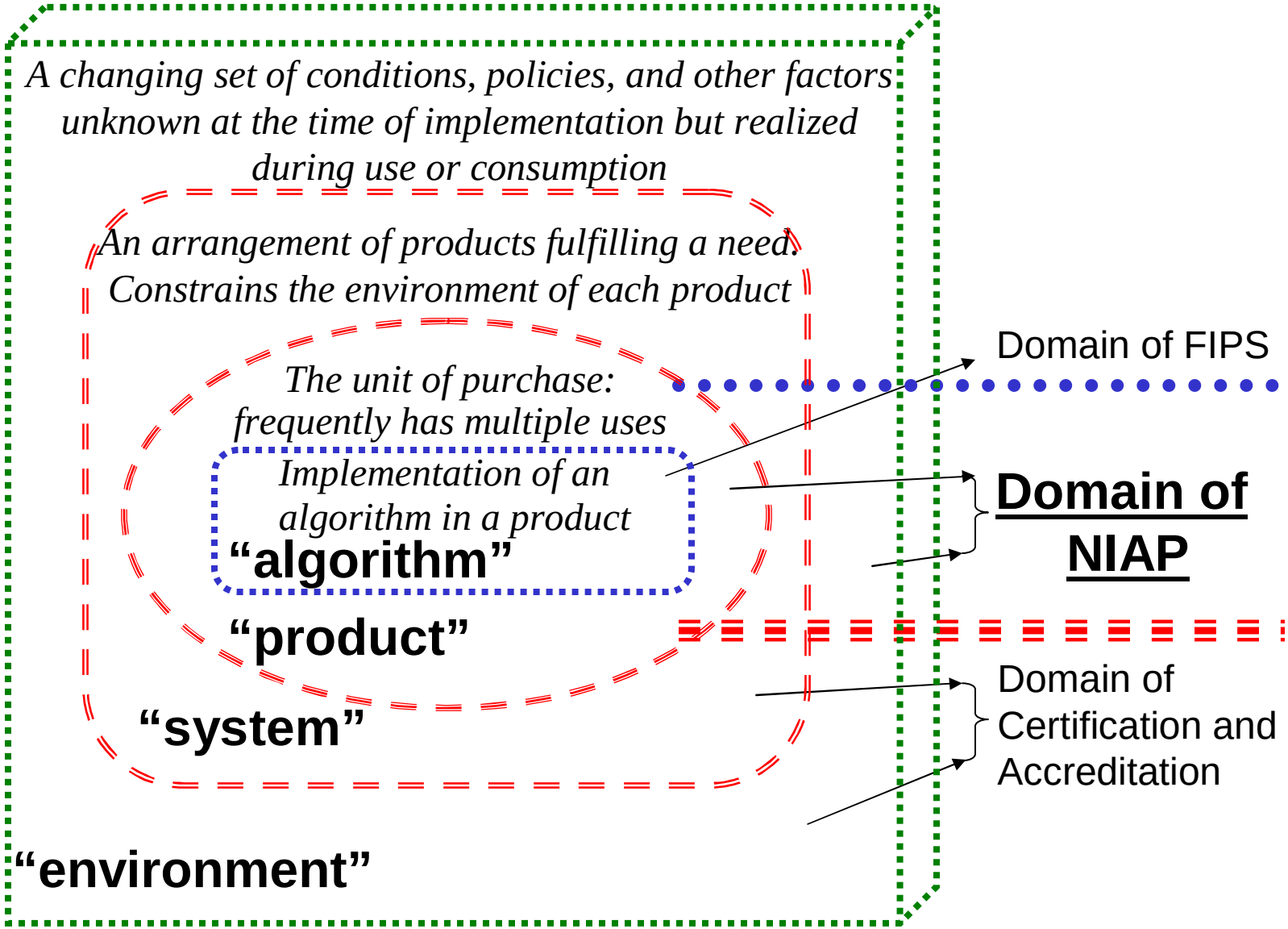
NIAP

- Information Assurance (Security) covers those areas of IT that protect data and IT resources from abuse, denial, misuse or misapplication.
- The US National Security Agency (NSA) has specific responsibilities for Information Assurance in the National Security Community including the Department of Defense.
- The US National Institute of Standards and Technology (NIST) has specific responsibilities for Information Assurance throughout government and Industry.
- There has been an explosive growth of IT industry and increasing reliance on and awareness of software for IA services and the complexity of the IA landscape has significantly grown.
- NIAP was formed as a partnership between NIST and NSA to combine efforts in these areas.

Scope of NIAP Review

- The US Department of Defense (DoD) and the US Department of Homeland Security (DHS) tasked IDA to conduct review of NIAP
  - Comprehensive review required by *The National Strategy to Secure Cyberspace*
- Scope
  - Recommendations should apply government-wide
  - Analysis should focus on particular DoD and DHS issues and concerns

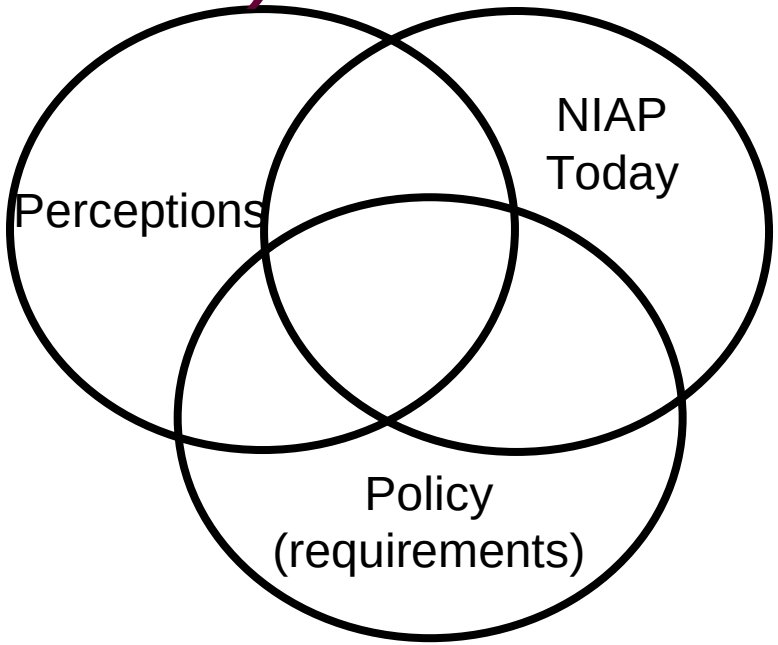
Evaluation Context



Approach

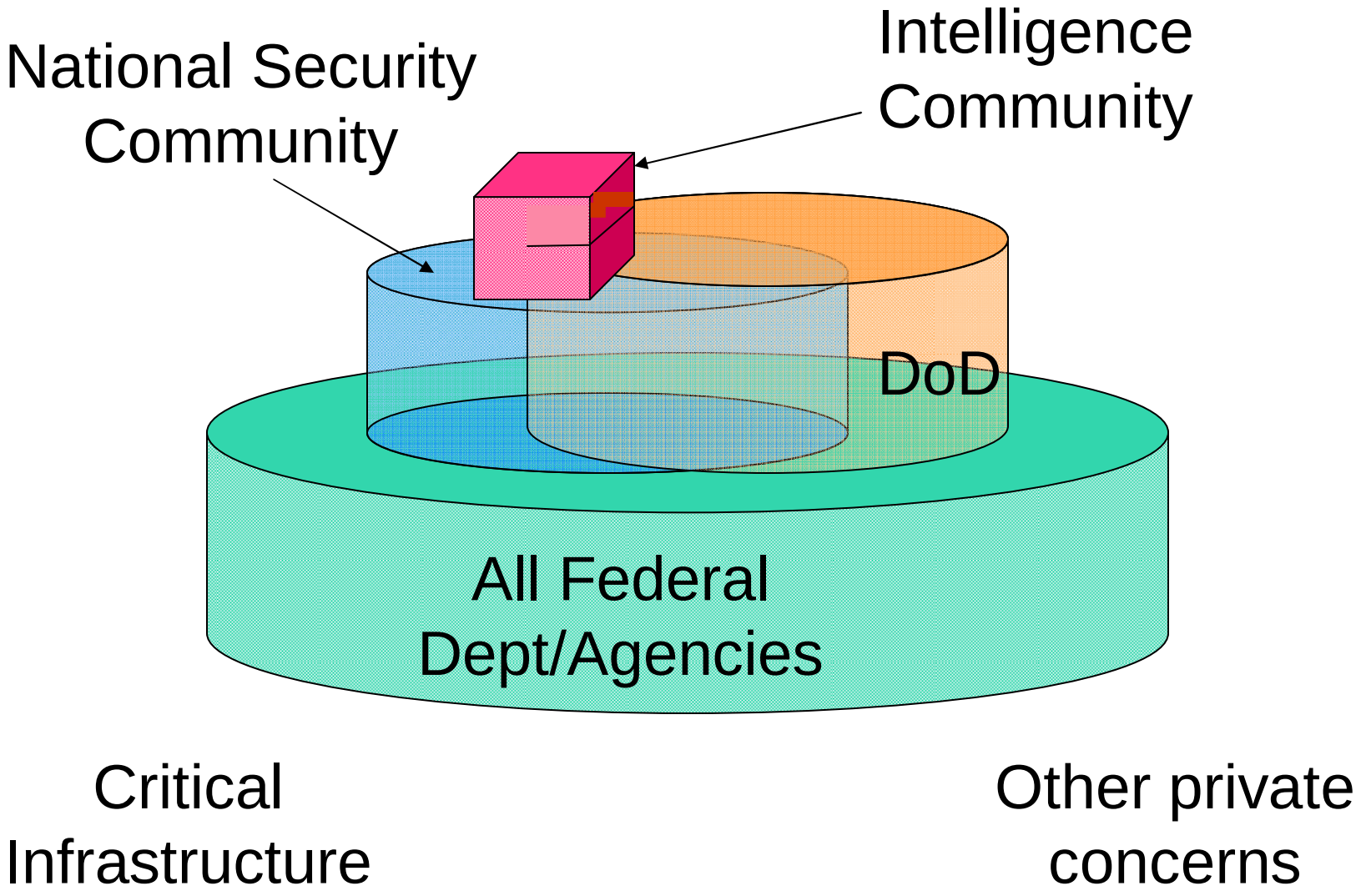
What do users expect and need?
(Desires, Expectations)

What requirements does NIAP meet and how are they met?
(Implementation Practices)

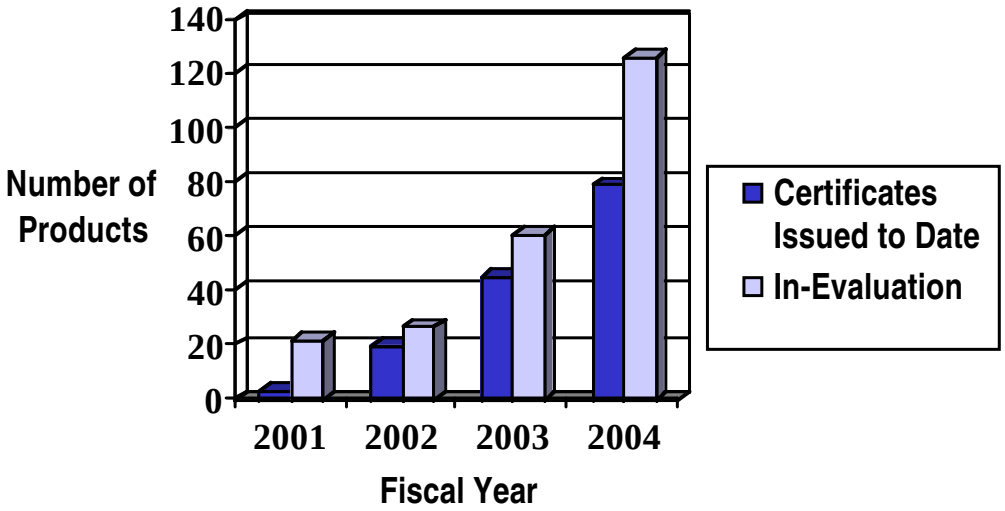


What requirements are derivable from DoD/DHS/U.S. Government documents (Legal, Regulatory, Policy)

The Policy Landscape



NIAP Today



- NIAP's principally active component is its product evaluation process, the Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS)
- Implicit assumptions built into CCEVS – derived from observing its current operations
  - Product developers are presumed to be trustworthy and disclose all known product testing and vulnerability information
  - Evaluation labs are presumed to be competent, competitive, and commercially viable

Perceptions

- Based upon:
  - Interviews
  - Literature
  - Forum
  - Solicitation

Numerous expectations that were surprising, conflicting, and some even expected

- Interpreting evaluation results should only require a general understanding of the concepts
- Conformance with a trusted PP should be required
- Source code review should be required at all levels

Top Level Findings

Summary Finding	Impact
NIAP has put together a flexible structure and gathered expertise to apply to cybersecurity problems	Flaws within NIAP are addressable and can be fixed with the proper application of resources
Policy and legal landscape extremely complex	Government developers have a difficult time figuring just what their requirements are and why they are needed
Education Training & Awareness programs have languished are incomplete and not current	Stakeholders have little appreciation for what a properly developed evaluation process does provide
Funding processes and priority shifts have moved NIAP away from its original charter	NIAP is basically a product evaluation organization.
Product Evaluation has not been integrated with Certification and Accreditation	C&A processes do not take full advantage of product evaluation
NIAP is basically a product evaluation organization.	Product Evaluation is less useful than it would be with education, research, tools, other functions.
The Cybersecurity landscape has shifted while NIAP has struggled to keep up with evaluation	Product Evaluation is not responsive in some areas
NIAP is focused on an individual part of an overall cybersecurity landscape	Product evaluation and its data are not used to help with other parts of the cybersecurity posture (C&A)
Common Criteria evaluations cost too much for low assurance products	Commercial market less than enthusiastic.

Options

- Stop product testing
- Maintain current focus on products
- Restore research, tool development, non-military PP development
- Modernize: Improve Common Criteria, low assurance evaluations; license evaluation personnel
- Expand to integrate with system evaluations (C&A)
- Replace with something new

Backup

Selected Community Perceptions

Consumer Knowledge and Understanding

Expectation: Evaluations should state in plain language what information assurance protection the product provides.

Evaluation Certificates

Expectation: Evaluation certificates should identify the degree of security provided and example applications for which the product is suitable.

Protection Profiles

Expectation: A collection of protection profiles covering core information assurance capabilities at more modest assurance levels should be developed.

Selected Community Perceptions (2)

Evaluation Personnel

Expectation: A credentialing program should be developed to ensure adequate training of evaluators and consistent evaluations across laboratories.

Commercial Viability

Expectation: Market forces would encourage developers and insurers to warrant NIAP-evaluated products and assume at least limited liability for information assurance breaches.

Selected Community Perceptions (3)

Testing

Expectation: NIAP should develop and make available a standard collection of automated security analysis tools, and require use of these or equivalent tools in evaluations.

Research

Expectation: NIAP should support research in information assurance metrics, the security of systems composed using standard building-block components, and other security issues.

Targets of Evaluation

Expectation: Whole products should be evaluated in their normal usage configuration and environment.

A Few Threads

Summary Data from each area provides some insights

- Money
  - Product Security area has been and continues to be under funded
    - ROM five or six times current funding probably needed for all requirements
  - Product evaluation costs too much for commercial enthusiasm
  - High cost evaluation processes probably only acceptable for high assurance products
- Education
  - Education activities have languished due to funding
  - A fully educated stakeholder at all levels is an unrealistic assumption
    - Re-target: Plain language and self evident meanings of evaluation
- Policy
  - Too complicated - Need to plan a clearinghouse function
- Common Security Flaws
  - The product evaluation should do something here - Tools appear to be a part of the answer
- Integration
  - Product evaluation that is independent of C&A is a pointless exercise (critical items repeated in C&A)
  - Product evaluation must be an integral part of the C&A scenario and the cybersecurity posture