

Common Criteria

NSTISSP # 11

A National IA Acquisition Policy

Yanet Manzano

Florida State University

manzano@cs.fsu.edu



Outline

- Critical Definitions
 - NSTISSP
 - National Security System
 - IT Products
 - IT Enable Products
 - COTS Products
 - GOTS Products
 - Security Robustness
- NSTISSP #11
- NSTISSP #11 Content
- Why NSTISSP #11
- Supporting NSTISSP #11
- NSTISSP #11 Application Scope
- Product Evaluation under NSTISSP #11
- Conclusion

Critical Definitions



NSTISSC

- National Security Telecommunications and Information Systems Security Committee
- Responsible for developing and promulgating national policies applicable to the security of *national security telecommunications and information systems*
- Recently renamed the Committee on National Security Systems (CNSS).

3

Critical Definitions



National Security System

Telecommunications and information systems operated by the U.S. Government, its contractors, or agents that contain classified information, or involved:

- intelligence activities
- cryptologic activities related to national security
- command and control of military forces
- equipment that is an integral part of a weapon or weapons system
- equipment that is critical to the direct fulfillment of military or intelligence missions

4

Critical Definitions



National Security System

- A system is considered a national security system if any part of that system meets any one of the categories mentioned in the previous slide

- Includes networks that attempt to maintain separation between classified and unclassified enclaves but do allow for limited information transfer between those enclaves

5

Critical Definitions



IT Products

- IT product or technology whose primary purpose is to:
 - provide security services (e.g., confidentiality, authentication)
 - correct known vulnerabilities
 - provide layered defense against various categories of non-authorized and malicious penetrations of
- information systems or networks

Examples:

- data/network encryptors
- firewalls

6

Critical Definitions



IT Enable Products

- A product or technology whose primary role is not security, but provides security services as an associated feature of its intended operating capabilities.

7

Critical Definitions



□ COTS Products

- A Commercial Off The Shelf IT product
- Widely available
- Developed with general commercial applications in mind.
- Typically: little or no U.S. Government funding or influence

□ GOTS Products (For the context of NSTISSP #11)

- Government Off the Shelf IA or IA enabled products
- Often require special features and assurances not found in typical COTS products and they are:
 - usually developed with U.S. Government cooperation
 - results in products that contain domestic and/or

8

Critical Definitions



Security Robustness

- A qualitative metric determined by:
 - security functionality
 - e.g., encryption, access controls), plus
 - the strength of the implementing mechanism
 - e.g., 256 bit key length
 - security assurance
 - achieved through testing, evaluation, etc
- U.S. Government is developing *CC Protection Profiles*, that fall into one of three robustness levels

9

NSTISSP #11



- A national security community policy governing the acquisition of information assurance (IA) and IA enabled information technology products
- Issued by the Chairman of the National Security Telecommunications and Information Systems Security Committee (NSTISSC),
- 2/1/00
- Effective July 1st, 2002

10

Affect all departments and agencies within the

NSTISSP Content (1)



- Mandates that all commercial off-the-shelf products (COT) or cryptomodules acquire for use on national security systems, must have been validates by:
 - National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme or
 - National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptomodule Validation Program

11

NSTISSP Content (2)



- Non-national security systems, also subject to policy and guidance
- Departments and agencies may wish to also consider:
 - validated COTS products for use in information systems associated with the operation of critical infrastructures
 - Note: critical infrastructures as defined in the Presidential Decision Directive on Critical

12

Why NSTISSP #11?



□ **U.S. Government:**

- **Initially:** exclusive use of Government Off-the-Shelf (GOTS) products
- **Today:** to a mix of COTS and GOTS products for the protection of information within our national security systems

- **COTS IA and IA-enabled IT products acquired:**
 - should be subject to a standardized evaluation process
 - to provide validation that products perform as

13

Supporting NSTISSP #11



- To achieve this objective, the policy requires COTS products be evaluated and validated

- To Support NSTISSP #11, the NSA and NIST created:
 - The National Information Assurance Partnership's (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) Program and,

 - NIST's Federal Information Processing Standard (FIPS) Cryptographic Module Validation Program₁₄ (CMVP)

Importance of NSTISSP



- NSTISSP #11 is:
 - a critical policy component of the U.S. Government's overall Information Assurance (IA) strategy
 - a binding, national policy requirement
 - design to establish policies and processes to:
 - validate the performance claims of marketed IA products
 - ensure that products are responsive to the security needs of the intended user
- Acquirers, users and vendors of IA products are encouraged to:
 1. Familiarize themselves with the policy and its associated processes,
 2. Ensure, effective 1 July 2002, full compliance with its documented requirements

15

NSTISSP #11 Application



scope

- Applies to all IA and IA enabled IT products in a given solution
- IA/IA enabled IT components:
 - Recognized part of the security policy and
 - Makes security decisions or
 - Implements security services
 - Availability | Integrity | Confidentiality
 - Authentication | Non-repudiation

Note: Labeling a component as an IA/IA enabled IT component is heavily dependent on the nature of the architecture where the component is being placed

16

Example



- Consider one solution architecture where an operating system may be required to enforce an access control policy because it is being used to separate multiple users from each other.
- OS considered an IA/IA Enabled IT component
- Because
 - it must enforce isolation with access control decisions

17

Product Evaluation under NSTISSP



- IA or IA enabled products must be evaluated
- COTS products must be evaluated and validated by accredited labs under:
 - U.S. NIAP Evaluation and Validation Program
 - Common Criteria Mutual Recognition Arrangements
 - The NIST FIPS validation program
- GOTS products must be evaluated by the NSA or in accordance with NSA-approved processes

18

Conclusion



- **Advantages of testing in accordance with International standards such as the Common Criteria**
 - Commercial vendors (domestic or foreign) not limited to having their products tested within their own countries.
 - Any commercial testing laboratory accredited as compliant with the CC Recognition Arrangement (CCRA) can perform evaluations up to and including evaluations at the EAL 4 level.

19

Conclusion



- CCRA signed in October of 1998, original members:
 - USA | Canada | France | Germany
 - the Netherlands | UK
- Additional members since then:
 - Australia | New Zealand | Finland | Greece
 - Israel | Norway | Spain | Sweden
- Programs in place to evaluate IT products against the CC:
 - USA | Canada | France | Germany | The UK
 - Australia/New Zealand (combined).
- Remaining nations agreed to accept certificates produced by nations that have evaluation

20