INFORMATION ASSURANCE DIRECTORATE

"INFORMATION ASSURANCE LEADERSHIP FOR THE NATION"

COMMITTEE ON NATIONAL SECURITY SYSTEMS

FREQUENTLY ASKED QUESTIONS

24 MARCH 2005

NATIONAL POLICY REGARDING THE EVALUATION OF COMMERCIAL PRODUCTS

WHAT IS IT?

WHY IS IT IMPORTANT?

HOW THE PROCESS WORKS

WHAT IS THE IMPORTANCE OF COMPLIANCE?

INFORMATION ASSURANCE DIRECTORATE

This FAQ is designed to answer common questions about the Committee on National Security Systems (CNSS) policy governing the acquisition of trusted products (i.e., NSTISSP #11). We have attempted to be as clear, precise and accurate as possible. Comments and questions on the FAQ may be directed at to the NSA IA Service Center (NIASC) at 1-800-688-6115 option 3.

Contents

(I) General

1. What is NSTISSP #11?
2. Why is there a need for a national IA acquisition policy like NSTISSP #11?
3. What is the objective of NSTISSP #11?
4. How should NSTISSP #11 be viewed?
5. Why is NSTISSP #11 so important?
6. What are the advantages of testing in accordance with International Standards such as the Common Criteria?

(II) Policy Information and Guidance

1. Is there any acquisition guidance for COTS products under NSTISSP #11?
2. To whom does NSTISSP #11 apply?
3. To what products does NSTISSP #11 apply?
4. Are all systems processing classified information considered National Security Systems?
5. Does NSTISSP #11 validation of products replace system certification testing?
6. What guidance is available regarding "the appropriate combinations and implementation of GOTS, COTS IA and IA-enabled products"?
7. Does NSTISSP #11 apply to all components of a large system?
8. What other related NSTISSP #11 documents exist?
9. How can I find out what products have already been tested by NIST's FIPS 140 Cryptographic Module Validation Program (CMVP) or by the NIAP?
10. What do I do if the commercial product I want to purchase is not on the NIAP or NIST validated products list?

11. Do products validated in the United States receive preferential treatment over products validated elsewhere?

12. Is there an NSTISSP #11 waiver process?

13. I have already purchased a COTS product, but it is not yet validated or fielded. Do I need to have it evaluated by NIAP CCEVS?

14. I have purchased a service agreement with my COTS product which gives me updates and patches over the lifetime of the product. Do each one of these updates/patches need to be tested by NIAP CCEVS?

15. I have a number of COTS products in an already fielded and accredited system. How does NSTISSP #11 apply to me?

16. My organization negotiates indefinite delivery/indefinite quantity (ID/IQ) agreements with vendors. How does NSTISSP #11 COTS testing requirements apply to these types of arrangements?

17. I am a government product program manager building a system comprising numerous IA/IA-enabled COTS products that will be purchased by government customers for use in their systems. How does NSTISSP #11 apply to my program?

(III) Definitions

1. What is the NSTISSC (recently renamed to the CNSS)?

2. What is a National Security System?

3. What are IA products? How do they differ from IA-enabled products?

4. What is a COTS product?

5. What is the nature of a GOTS product?

6. Is the evaluation different for COTS and GOTS products?

7. What is security robustness?

(IV) NIAP and the Common Criteria

1. What is the NIAP?

2. What is CCEVS? What is its purpose?

3. What is the CMVP?

4. What is the Common Criteria?

5. What is a Protection Profile (PP)?
6. Do any Protection Profiles exist? Where?
7. Can I write a Protection Profile?
8. What is a Security Target (ST)?
9. How can I find out what products have been CCEVS validated?
10. Is a NIAP/NIST validated product secure?
11. What are Evaluation Assurance Levels (EALs)?
12. Can I get Common Criteria training?
13. What is the Common Criteria Mutual Recognition List?
14. What is the relationship of NIAP's CCEVS and NIST's Cryptographic Module Validation Program (CMVP)?
15. What U.S. laboratories have been approved to perform CC and PP evaluations?

(V) Developers and NSTISSP #11

1. What are Protection Profile compliant products? Should I attempt to make my product compliant?
2. Should I attempt to get my product evaluated before a prospective customer requests one?
3. How do I get a GOTS product validated?
4. How much does an evaluation cost?
5. What do I do to start a Common Criteria evaluation? How does the process work?
6. I have a product which contains a cryptographic module along with other mechanisms to implement separate security features. Do I need two evaluations? Why? What is the relationship between the CCEVS and the CMVP?

(VI) NSTISSP #11 and National Security System Product Testing Programs

1. Do products for which NSA has produced Configuration Guidance meet NSTISSP #11 validation requirements?
2. Do SABI/TSABI approved COTS IA/IA-enabled products qualify as "validated" under NSTISSP #11?
3. What is the difference between NIAP CCEVS evaluated products and NSA approved products?

(I) General

1. What is NSTISSP #11

NSTISSP #11 is a national security community policy governing the acquisition of information assurance (IA) and IA enabled information technology products. The policy was issued by the Chairman of the National Security Telecommunications and Information Systems Security Committee (NSTISSC), now known as the Committee on National Security Systems (CNSS) in January 2000 and revised in June 2003. . The policy mandates, effective 1 July 2002, that departments and agencies within the Executive Branch shall acquire, for use on national security systems, only those COTS products or cryptographic modules that have been validated with the International Common Criteria for Information Technology Security Evaluation, the National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS), or by the National Institute of Standards and Technology (NIST) Federal Information Processing Standards (FIPS) Cryptographic Module Validation Program. Additionally, subject to policy and guidance for non-national security systems, NSTISSP # 11 notes that departments and agencies may wish to consider the acquisition of validated COTS products for use in information systems that may be associated with the operation of critical infrastructures as defined in the Presidential Decision Directive on Critical Infrastructure Protection (PDD-63).
The revised NSTISSP #11 added the Deferred Compliance Authorization (DCA) that states, "No blanket or open-ended waiver to NSTISSP No.11 will be authorized, but a DCA[1] may be granted on a case-by-case basis." Departments and agencies electing to pursue a DCA from the policy requirement of NSTISSP #11 shall use the guidelines and procedures provided in NSTISSP No. 11, Revised Fact Sheet (July 2003) .

2. Why is there a need for a national IA acquisition policy like NSTISSP #11?

The technology advances and threats of the past decade have drastically changed thinking and approaches to protecting national security systems and information. The U.S. Government has migrated from the exclusive use of Government Off-the-Shelf (GOTS) products to a mix of Commercial Off-the-Shelf (COTS) and GOTS products for the protection of information within our national security systems. The proliferation of COTS information assurance (IA) products such as firewalls and Intrusion Detection Systems, as well as IA-Enabled products such as operating systems and database management systems with security attributes, has provided the community of users with a multitude of security products to choose from. All of the products come with their own specific claims relative to the security robustness they provide. In this context, it is important that COTS IA and IA-enabled IT products acquired by the U.S. Government Departments and Agencies be subject to a standardized evaluation process that will provide some validation that these products perform as advertised.

3. What is the objective of NSTISSP #11?

The objective of NSTISSP #11 is to ensure that COTS IA and IA-enabled IT products acquired by the U.S. Government for use in national security systems perform as advertised by their respective manufacturers, or satisfy the security requirements of the intended user. To achieve this objective, the

[1] A Deferred Compliance Authorization (DCA) is a formal approval by an authorized official to defer compliance with the requirement of a national IA policy for a specified period of time, normally not to exceed more than one calendar year.

policy requires COTS products be evaluated and validated in accordance with either the International Common Criteria for Information Technology Security Evaluation, or the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2. Supportive of the intent and implementation of NSTISSP #11, the NSA and NIST have collaborated to establish the following two evaluation and validation programs: The National Information Assurance Partnership's (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) Program and the NIST Federal Information Processing Standard (FIPS) Cryptographic Module Validation Program (CMVP) each which target different, but complementary, areas.

4. How should NSTISSP #11 be viewed?

NSTISSP #11 should be viewed as a tool for evaluating the security functionality provided by COTS IA and IA-enabled IT products at various robustness levels. A comprehensive risk management program must be considered from the outset in the design, acquisition and operation of all Information Technology (IT) systems. During the initial design phase of any information system, security considerations must be included. However, compliance with the policy in its most simplistic form (i.e., feel comfortable that a properly evaluated product has been acquired), should not be viewed as an "end result" IA solution in and by itself. The use of properly evaluated products certainly contributes toward the security and assurance of the overall system where they are employed and should be an important factor in IT procurement decisions. From an overall security perspective, however a properly evaluated product is only a part of the security solution. Other complementary controls are needed including sound operating procedures, adequate training, overall system certification and accreditation, sound security policies and well-designed system architectures.

5. Why is NSTISSP #11 so important?

NSTISSP #11 is a critical policy component of the U.S. Government's overall Information Assurance (IA) strategy. A wide variety of products are available to satisfy a diversity of security requirements to include providing confidentiality for data, as well as authenticating the identities of individuals or organizations exchanging sensitive information. In terms of design, quality and performance, these products run the gamut from "terrific to terrible". It is imperative that policies and processes be established to validate the performance claims of marketed IA products, and to ensure that these products are responsive to the security needs of the intended user. In the context of national security systems and information, these requirements take on added significance and importance. NSTISSP #11 is a binding, national policy requirement. Acquirers, users and vendors of IA products are encouraged to familiarize themselves with the policy and its associated processes, and to ensure, effective 1 July 2002, full compliance with its documented requirements.

6. What are the advantages of testing in accordance with International standards such as the Common Criteria?

The advantages of using international standards are that commercial vendors (either domestic or foreign) are not limited to having their products tested within their own countries. Any commercial testing laboratory accredited as compliant with the Common Criteria Recognition Arrangement (CCRA) can perform evaluations up to and including evaluations at the EAL 4 level. This arrangement ensures that

accredited laboratories, regardless of their geographic location or national affiliation, will test products against the same criteria and use the same testing methodology.

The United States, Canada, France, Germany, the Netherlands and the United Kingdom are all charter members of the Common Criteria Recognition Arrangement that was signed in October of 1998. Since that time, Australia, New Zealand, Finland, Greece, Israel, Norway, Spain, Italy, Hungary, Turkey, Republic of Singapore and Sweden have also become members. Of these nations, the United States, Canada, France, Germany, the United Kingdom Australia/New Zealand (combined) and Japan have programs in place to evaluate COTS IA and IA-enabled IT products against the Common Criteria. The remaining nations do not have evaluation programs, but have agreed to accept the certificates produced by those nations that do have evaluation programs.

Based on the need for good security products, as well as the plethora of products and services available on the commercial market, consistency and efficiency are desirable objectives. The use of recognized, common standards within the structure of NIAP and NIST provide the mechanisms for accomplishing those objectives. Specifically:

- The evaluations of IT products and protection profiles are performed against high and consistent standards that are seen as contributing significantly to the confidence in the security of those products and profiles;

- The framework of the Common Criteria increases the availability of evaluated, security-enhanced IT products and profiles for national implications;

- Duplicative evaluations of IT products and protection profiles are eliminated; and

- Continuous improvements in the efficiency and cost-effectiveness of security evaluations and the certification/validation processes for IT products and protection profiles are achieved.

(II) Policy Information and Guidance Contents

1. Is there any acquisition guidance for COTS products under NSTISSP #11?

Acquisition guidance for COTS products that contain cryptographic modules used by the U.S. Government to protect UNCLASSIFIED information within computer and telecommunications systems has not changed. NSTISSAM INFOSEC/1-00, dated 8 FEB 2000, is the Advisory Memorandum for the Use of FIPS 140 Validated Cryptographic Modules in Protecting Unclassified National Security Systems. FIPS 140 is applicable to all Federal agencies that use cryptographic-based security systems to protect sensitive information in computer and telecommunication systems (including voice systems) as defined in Section 5131 of the Information Technology Management Reform Act of 1996, Public Law 104-106. This standard shall be used in designing and implementing cryptographic modules that Federal departments and agencies operate or are operated for them under contract. Cryptographic modules that have been approved for classified use may be used in lieu of modules that have been validated against this standard. For FIPS compliant cryptographic modules, products from the NIST CMVP Validation List should be selected.
The recommended acquisition approach for products containing non-cryptographic IA or IA-enabled features is as follows. First, choose a product from the NIAP CCEVS Validated Products List that is compliant with the requirements of a government sponsored protection profile for the desired technology (e.g., firewalls). In the absence of any products that are compliant with a government sponsored protection profile, or where there is no government sponsored protection profile for that particular technology, the consumer should choose from the CCEVS Validated Products List an evaluated product from the desired technology that has met its security target requirements. Lastly, where no evaluated or validated product is on the CCEVS Validated Products List, the consumer should check the CCEVS Products and Protection Profiles In Evaluation List for a potential product. All proposed contracts for acquisition of IA or IA-enabled IT products should contain language that very specifically documents the requirement for NSTISSP #11 validated products. This can be accomplished in two ways:

1. If an approved U.S. Government protection profile exists for a particular technology area, but no validated products that conform to the protection profile are available for use, the acquiring organization must require, prior to purchase, that vendors submit their products for evaluation and validation by a NIAP laboratory or CCRA laboratory to a security target written against the approved protection profile or acquire other U.S.-recognized products that have been evaluated under the sponsorship of other signatories to the CCRA

2. If no U.S. Government protection profile exists for a particular technology area and the acquiring organization chooses not to acquire products that have been evaluated by the NIAP CCEVS or CCRA laboratories, then the acquiring organization must require, prior to purchase, that vendors provide a security target that describes the security attributes of their products, and that vendors submit their products for evaluation and validation at a DAA-approved EAL. Robustness requirements, mission, and customer needs will together enable an experienced information systems security engineer to recommend a specific EAL for a particular product to the DAA. In addition, the organization should file the necessary for a DCA (see FAQ #12 under Policy information and Guidance).

The recommended acquisition approach for products containing both cryptographic modules and IA or IA-enabled features is as follows. Apply the procedures for non-cryptographic IA or IA-enabled features as described above and ensure that any cryptographic modules included in the product meets the FIPS criteria described above. If there are no products that meet the FIPS and NIAP criteria, apply the rules outlined in 1 and 2 above and apply for DCA noted in #2 above for non-cryptographic IA or IA-enabled features and the waiver process outlined in the FIPS 140-2 standard for cryptographic modules.

2. To whom does NSTISSP #11 apply?

All departments and agencies in the Executive Branch that acquire COTS products for use in national security systems. Departments and agencies associated with the operation of critical infrastructures as defined in the Presidential Decision Directive on Critical Infrastructure Protection (PDD-63), may wish to consider the acquisition of validated COTS products for use in 'critical' information systems.

3. To what products does NSTISSP #11 apply?

NSTISSP # 11 applies to products being acquired for national security systems used to enter, process, store, display, or transmit national security information. The policy applies only to departments and agencies within the Executive Branch of the U.S. Government. Departments and agencies responsible for governing non-national security systems but considered part of the of critical infrastructure as defined in the Presidential Decision Directive on Critical Infrastructure Protection (PDD-63), may wish to consider this policy in their implementation IA procurement strategy.

4. Are all systems processing classified information considered National Security Systems?

Yes. See E.O. 12958.

5. Does NSTISSP #11 validation of products replace system certification testing?

No. For national security systems, composite system level certification analysis and testing is still required per the local Designated Accrediting Authority requirements (e.g., DITSCAP, NIACAP). The hope is that using validated products will aid in increasing security of systems in development by allowing organizations to make more informed security decisions before procurement, and decrease the effort required for composite system testing before Accreditation.

6. What guidance is available regarding "the appropriate combinations and implementation of GOTS, COTS IA and IA-enabled products"?

The National Security Agency, as well as numerous support contractors offer Information System Security Engineering services that provide guidance on secure architectures, risk management and risk mitigation. To receive such services from NSA, call the NSA Information Assurance Service Center at 1-800-688-6115 option 3 or (410) 854-7661 for more information.

7. Does NSTISSP #11 apply to all components of a large system?

NSTISSP #11 applies to all IA and IA-enabled IT products in a given solution. Whether a component is considered an IA/IA-enabled IT component depends heavily on the nature of the architecture in which it is being placed. If the component is not "cognizant" of the security policy and has no security policy enforcement responsibilities (i.e. it is not required to make policy enforcement decisions or implement a security feature), it is not considered to be an IA/IA-enabled IT component and hence will not need to be validated. On the other hand, if the component is "cognizant" of the security policy and makes security decisions or implements security features, it is considered to be an IA/IA-enabled IT component and must be validated. To illustrate this, consider an 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. In this case, the operating system is considered to be an IA-enabled IT component because it must enforce isolation with access control decisions. For another architecture, the same operating system may not be responsible for enforcing or implementing separation of users (i.e. it is being used only as a dumb terminal) because the architecture calls for it to be a "single user" system which is connected to a network where all security services are implemented on a network server. In this architecture, the operating system would not be considered an IA-enabled IT component, and hence not require CC evaluation/validation.

8. What other related NSTISSP #11 documents exist?

There are numerous Department of Defense and Civilian policy documents that reference or are related to NSTISSP #11. NIAP has selected policy and guidance documents. The U.S. Department of Defense maintains the DoD issuances web site where DoD Directive 8500.1 mandates NSTISSP # 11 compliance. NIST Special Publication 800-23 "Guidelines to Federal Organizations in Security Assurance and Acquisition/Use of Tested/Validated Products" references NSTISSP #11. Information Technology Management Act (Clinger/Cohen Act) defines national security systems and national security information.

9. How can I find out what products have already been tested by NIST's FIPS 140 Cryptographic Module Validation Program (CMVP) or by the NIAP?

Validated Cryptographic Modules can be found on the CMVP Validated Modules List. Products that have been evaluated against the International Common Criteria for Information Technology Security Evaluation can be located on the CCEVS NIAP Validated Products List or the Common Criteria Validated Products.

10. What do I do if the commercial product I want to purchase is not on the NIAP or NIST validated products list?

If the product contains a cryptographic module and that cryptographic module is not on the CMVP Validated Modules List, then the product cannot be purchased. If the product contains non-cryptographic IA or IA-enabled features and is not on the CCEVS or Common Criteria Validated Products List, the acquisition contract must require Common Criteria evaluation/validation as a condition of purchase. See question 12 on the Deferred Compliance Authorization.

11. Do products validated in the United States receive preferential treatment over products validated elsewhere?

Cryptographic COTS products used by the U.S. Government must be validated by the NIST Cryptographic Module Validation Program (CMVP). The CMVP was established by NIST and the Communications Security Establishment (CSE) of the Government of Canada in July 1995. All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). There are currently nine CMT laboratories located in the U.S., Canada, and UK. Testing at any laboratory is recognized by the CMVP and upon successful testing, cryptographic modules, which are validated are added to the CMVP Validated Modules List.
For non-cryptographic COTS IA/IA-enabled IT products evaluated at EAL1- EAL4, evaluations may be performed at one of the U.S. accredited Common Criteria Testing Laboratories (CCTLs) or an accredited CCTL recognized under the Common Criteria Recognition Arrangement. Products whose evaluations have assurance components above EAL 4 must be evaluated in the U.S., for that portion that is above EAL 4, before they are placed on the CCEVS Validated Products List.

12. Is there an NSTISSP #11 waiver process?

No blanket or open-ended waivers to NSTISSP No. 11 will be authorized, but a Deferred Compliance Authorization (DCA)[2] may be granted on a case-by-case basis. See NSTISSP No. 11, Revised Fact Sheet (July 2003) for details.

13. I have already purchased a COTS product, but it is not yet validated or fielded. Do I need to have it evaluated by NIAP CCEVS?

If the product contains a cryptographic module, NSTISSAM INFOSEC 1/00 requires that the cryptographic module must undergo FIPS testing prior to being used to protect UNCLASSIFIED information. If the product does not contain a cryptographic module, the answer is no. Although this may seem counter-intuitive, NSTISSP #11 is an acquisition policy, and as such it is invoked as part of the initial procurement activity and does not apply to IA/IA-enabled products that have already been acquired, the DAA (Designated Accrediting Authority) makes the "use" decision. The key to whether NSTISSP #11 Common Criteria testing applies is based on when the contract was signed. If the procurement agreement is signed prior to July 1, 2002, COTS IA/IA-enabled testing through an accredited Common Criteria Testing Laboratory (CCTL) is not required. If it is signed after July 1, 2002, COTS IA/IA-enabled testing through a CCTL is required.

14. I have purchased a service agreement with my COTS product, which gives me updates and patches over the lifetime of the product. Do each one of these updates/patches need to be tested by NIAP CCEVS?

[2] A **Deferred Compliance Authorization** (DCA) is a formal approval by an authorized official to defer compliance with the requirements of a national IA policy for a specified period of time, normally not to exceed more than one calendar year.

In the context of NSTISSP #11, whether or not COTS IA/IA-enabled testing is required will be based upon when two parties legally agree upon a price and a product. When funds actually change hands or when the product is actually obtained is irrelevant to whether NSTISSP #11 COTS testing is required or not. Specifically for the DoD community, the following policy words apply:

> Acquiring DoD organizations that anticipate using the IA functionality of subsequent versions of an evaluated product shall specify in the original contract that product validation will be kept current through vendors submitting the next version of their products for evaluation or through participation in the NIAP Assurance Maintenance Program or the CCRA Assurance Maintenance Program.
>
> Products that are available under multiple-award schedule contracts or non-DoD Government-Wide Acquisition Contracts awarded before July 1, 2002, must be evaluated when and if a version release of the product is made available under the contract.
>
> Implementation of security-related software patches directed through the DoD IAVA program shall not be delayed pending evaluation of changes that may result from the patches.

15. I have a number of COTS products in an already fielded and accredited system. How does NSTISSP #11 apply to me?

As an acquisition policy, NSTISSP #11 testing applies only to the acquisition of new products. NSTISSP #11 does not require testing of COTS products that are already fielded.

16. My organization negotiates indefinite delivery/indefinite quantity (ID/IQ) agreements with vendors. How does NSTISSP #11 COTS testing requirements apply to these types of arrangements?

For the purposes of determining whether NSTISSP #11 COTS testing is required or not, an agreement is considered to be a "contract" when two parties legally agree upon a price and a product. When funds actually change hands or when the product is obtained is irrelevant to whether NSTISSP #11 COTS testing is required or not. Therefore, if the IDIQ agreement notes an agreed upon price and product (with funds changing hands at a future date) and it is signed before July 1, 2002, COTS testing is not required for "buys" against that agreement. However, once the agreement is renegotiated (after July 1, 2002), it must include a provision for COTS tested products.

17. I am a government product program manager building a system comprising numerous IA/IA-enabled COTS products that will be purchased by government customers for use in their systems. How does NSTISSP #11 apply to my program?

How NSTISSP #11 applies depends heavily on whether the resultant system is considered a COTS or GOTS product. GOTS products must be evaluated by NSA or in accordance to an NSA-approved process. However if it is a COTS oriented solution, much depends on how it is going to be distributed.

1. If distribution is through a single office that negotiates price and product (e.g., an ID/IQ

agreement), whether NSTISSP #11 COTS testing is required will be based on when price and product are agreed upon. If it is agreed upon before July 1, 2002, no NSTISSP #11 COTS testing is required. If it is agreed upon after July 1, 2002, NSTISSP #11 COTS testing is required.

2. If distribution is through a contractor that deals directly with each customer (with the contractor in control of price and distribution), whether NSTISSP #11 COTS testing required will be based upon when the price and product is agreed upon by each individual customer attempting to purchase the product. Products sold before July 1, 2002 will not require NSTISSP #11 COTS testing. Products sold after July 1, 2002 will require NSTISSP #11 COTS testing.

In general, it may be reasonable for the program office to have the product Common Criteria evaluated before it is distributed so that multiple evaluations of the same product would not be pursued over the course of the product.

(III) Definitions

1. What is the NSTISSC (recently renamed to the CNSS)?

The National Security Telecommunications and Information Systems Security Committee (NSTISSC) was established by National Security Directive (NSD) No. 42, dated July 1990, and is responsible for developing and promulgating national policies applicable to the security of national security telecommunications and information systems. The NSTISSC has been recently renamed the Committee on National Security Systems (CNSS).

2. What is a National Security System?

This term means those telecommunications and information systems operated by the U.S. Government, its contractors, or agents that

a. contain classified information; or that
b. involve intelligence activities,
c. involve cryptologic activities related to national security (national defense or foreign relations matters of the United States),
d. involve command and control of military forces,
e. involve equipment that is an integral part of a weapon or weapons system, or
f. involve equipment that is critical to the direct fulfillment of military or intelligence missions.

A system is considered a national security system if any part of that system meets any one of the categories above. This includes networks that attempt to maintain separation between classified and unclassified enclaves but do allow for limited information transfer between those enclaves.

3. What are IA Products? How do they differ from IA Enabled Products?

An IA product is an IT product or technology whose primary purpose is to provide security services (e.g., confidentiality, authentication, integrity, access control and non-repudiation of data); correct known vulnerabilities; provide layered defense against various categories of non-authorized and malicious penetrations of information systems or networks. Examples include such products as data/network encryptors, firewalls and intrusion detection devices.

An IA-enabled product is a product or technology whose primary role is not security, but which provides security services as an associated feature of its intended operating capabilities. To meet the intent of NSTISSP #11, acquired IA-enabled products must be evaluated if the IA features are going to be used to perform one of the security services (availability, integrity, confidentiality, authentication, or non-repudiation). Therefore, the determination of whether an IA-enabled product must be evaluated will be dependent upon how that particular product will be used within the consumer's system architecture. Examples include such products as security-enabled web browsers, screening routers, and security-enabled messaging systems. Although NSTISSP #11 uses both terms, the policy as stated applies equally to both types of products.

4. What is a COTS Product?

A Commercial Off The Shelf (COTS) IT product is widely available is developed with general commercial applications in mind. Such products typically have little or no U.S. Government funding or influence.

5. What is the nature of a GOTS Product?

For the context of NSTISSP #11, Government Off-the-Shelf (GOTS) IA or IA-enabled products are those products that often require special features and assurances that are not found in typical COTS products. These additional features and assurances are usually developed with U.S. Government cooperation and results in products that contain domestic and/or international restrictions.

6. Is the evaluation different for COTS and GOTS products?

The NSTISSP #11 policy states that all IA or IA-enabled products must be evaluated and validated regardless of whether the product is categorized as COTS or GOTS. Furthermore, COTS products must be evaluated and validated by accredited labs under the U.S. NIAPCCEVS, the International Common Criteria for Information Security Technology Evaluation Mutual Recognition Arrangements, and/or the NIST FIPS validation program. GOTS products must be evaluated by the NSA or in accordance with NSA-approved processes. If a consumer or vendor needs clarification of which process should be used, contact NSA/ IA Services Center, 1-800-688-6115 option 3 or (410) 854-7661, for information.
Some government departments and agencies may require additional testing or evaluation of products prior to operational use depending upon the architecture or environment that these products will be used in; however, those additional requirements are outside of the scope of NSTISSP #11.

7. What is security robustness?

Security robustness is 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), plus security assurance (achieved through testing, evaluation, etc). The U.S. Government is developing CC Protection Profiles that fall into one of three robustness levels; basic, medium, and high. Protection profiles in development and NIAP validated can be found at the CCEVS web pages.

(IV) NIAP and the Common Criteria

1. What is the NIAP?

The National Information Assurance Partnership (NIAP) is a U.S. Government initiative designed to meet the security testing, evaluation, and assessment needs of both information technology (IT) producers and consumers. NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) in fulfilling their respective responsibilities under the Computer Security Act of 1987. The partnership, originated in 1997, combines the extensive security experience of both agencies to promote the development of technically sound security requirements for IT products and systems and appropriate metrics for evaluating those products and systems. The long-term goal of NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and assessment programs. NIAP continues to build important relationships with government agencies and industry in a variety of areas to help meet current and future IT security challenges affecting the nation's critical information infrastructure.

2. What is CCEVS? What is its purpose?

The Common Criteria Evaluation and Validation Scheme (CCEVS) is a program under the NIAP to meet the security evaluation needs of both IT/IA product producers and users. Its purpose is to evaluate COTS IA and IA-enabled products (e.g., a firewall or an operating system) in accordance with the "International Common Criteria for Information Technology Security Evaluation" (generally referred to as the Common Criteria). It accomplishes this through the use of U.S. Government accredited Common Criteria testing laboratories.

3. What is the CMVP?

The Cryptographic Module Validation Program (CMVP) was established by NIST and the Communications Security Establishment (CSE) of the Government of Canada in July 1995. All of the tests under the CMVP are handled by third-party laboratories that are accredited as Cryptographic Module Testing (CMT) laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). There are currently nine laboratories located in the U.S., Canada, and United Kingdom. More information about the CMVP can be obtained at http://www.nist.gov/cmvp.

4. What is the Common Criteria?

The Common Criteria for Information Technology Security Evaluation (CC), ISO/IEC 15408 Standard, defines general concepts and principles of IT security evaluation and presents a general model of evaluation. It presents constructs for expressing IT security objectives, for selecting and defining IT security requirements, and for writing high-level specifications for products and systems. It specifies information security functional requirements and seven predefined assurance packages, known as Evaluated Assurance Levels (EALs), against which products' functions are tested and evaluated. NSTISSP #11 does not require testing against any specific function or EAL. The seven EALs provide both the vendor and user with flexibility to define functional and assurance requirements that are unique

to their operating environments and to obtain an evaluated product best suited to those needs. Two very important specification documents associated with the CC (and hence CCEVS) are Protection Profiles and Security Targets.

5. What is a Protection Profile (PP)?

A protection profile is the specification document used by a consumer, consumer group, vendor, or any consortium to specify what functional requirements they would like to have in a commercial IA or IA-enabled products, and to document to what assurance level(s) they would like to have the product tested. Protection Profiles for IA and IA-enabled products can be developed by anyone ranging from a commercial producer to an intended government user of those products. Protection Profiles serve two purposes:

· Provide customers with the ability to specify security requirements for their given environment (levels of concern/robustness); and
· Serve to identify, for vendors, known markets for products that meet specified customer requirements.

6. Do any Protection Profiles exist? Where?

NSA and NIST are jointly developing and issuing a series of technology-based protection profiles that will address both specific technologies (e.g., firewalls), as well as levels of security robustness. Draft and NIAP Evaluated U.S. Government protection profiles can be seen at the CCEVS web site.

7. Can I write a Protection Profile?

Anyone can write a Protection Profile. When looking for protection profiles to build or for a TOE that meets a given protection profile, it is important to know who created the profile and who (if anyone) is planning to use it in procurements. For a protection profile to be acknowledged as a U.S. Government Protection Profile, it must undergo coordination and approval by NIST and NSA and be developed in accordance with the Consistency Instruction Manual appropriate for the required robustness.

8. What is a Security Target (ST)?

A security target is a specification document that a vendor would use to make security functionality claims about its product. To have a product evaluated, the vendor must develop a security target. As part of the security target development process, the vendor can claim conformance to a protection profile, but is not required to do so. The evaluation and testing methodologies are the same for the evaluation of a security target regardless of whether or not it claims conformance to a protection profile. The security target requirements in the security target describe the product's security functionality claims, as well as the desired level of evaluation (i.e., the EALs mentioned above) that the vendor desires a Common Criteria Testing Laboratory to test against. Every validated product will have a publicly available Security Target that describes the threats, objectives and requirements against which a product has been tested. The intent is for consumers to review and compare vendors Security Targets prior to making an acquisition decision to understand what the security functionality of the product will and will not provide.

9. How can I find out what products have been CCEVS validated?

CCEVS maintains a Validated Products List that contains all products that have been validated, as well as a list of products that are "In-Evaluation". If the Common Criteria evaluation is taking place in a non-U.S. accredited laboratory, information concerning that particular evaluation may be obtained from that nation's common criteria web site

10. Is a Common Criteria evaluated/validated product secure?

The fact that a product appears on the Validated Product List does not by itself mean that it is secure. A product's listing on any Common Criteria validated products list means that the product was evaluated against its security claims and that it has met those claims. The security claims are provided in a document called the product security target (which is available on the Validated Products List). In the security target, the vendor (or the sponsor of the evaluation) documents the security functionalities the product contains and the level of evaluation rigor (assurance) performed to determine if the product meets its claims. It is up to the purchaser to review the security target to determine if the security provided by the product is the appropriate level for the targeted application or system. For some technologies (e.g., firewalls, operating systems), NSA and NIST have collaborated to draft U.S. Government protection profiles. These U.S. Government protection profiles provide information to purchasers and vendors regarding the appropriate security functionality and level of testing (assurance) which NSA and NIST believe are appropriate for described IT environments. Products on the Validated Products List, which claim compliance with the U.S. Government protection profiles, meet the minimum security levels deemed appropriate by NIST and NSA and should generally be preferred over products which make no such claims.

11. What are Evaluation Assurance Levels (EALs)?

Evaluation Assurance Levels (EALs) are predefined assurance packages selected by the authors of the Common Criteria to represent points on the CC assurance scale. These predefined levels go from EAL1, the lowest level of assurance, to EAL 7, which is the highest. In general, the U.S. Department of Defense uses robustness, which not only includes assurances but also functionality. Theses robustness definitions are included in the Consistency Instruction Manuals. In general, basic robustness included basic functionality and an EAL that exceeds EAL2. Medium robustness includes medium functionality and an EAL that exceeds EAL4. High robustness includes high functionality and an EAL level that exceeds EAL6. Reliance on EALs alone does not provide a method for determining the "security robustness" of a product. The EAL merely provides a convenient reference for the amount of analysis and testing performed on the product. Users are encouraged to read both the security functionalities as well as the EAL specified in the security target to determine the whether the "security robustness" of the product is appropriate for their environment. Some Departments (e.g., U.S. Department of Defense) offer guidance as to appropriate assurance levels for given threat environments.

12. Can I get Common Criteria training?

Numerous vendors offer such training. Also, all members of U.S. Department of Defense and of the National Security Community who have a requirement to use the CC are eligible for training conducted

by the National Cryptologic School (NCS). Currently there are two courses available at the NCS, IAEC 3283 (Designing Protection Profile fundamentals, 1 day) and IAEC 3284 (Designing a Protection Profile, 3 days). Contact the NCS Registrar at (410) 854-6867 for more information.

13. What is the Common Criteria Mutual Recognition List?

Following the development of the Common Criteria, the National Institute of Standards and Technology and the National Security Agency, in cooperation and collaboration with the U.S. State Department, worked closely with their partners in the CC Project to produce a mutual recognition arrangement for IT security evaluations that use the Common Criteria. In October 1998, after two years of intense negotiations, government organizations from the United States, Canada, France, Germany, and the United Kingdom signed this historic recognition arrangement for Common Criteria-based IT security evaluations. The Arrangement is officially known as the Arrangement on the Mutual Recognition of Common Criteria Certificates in the field of IT Security. It states that each Participant will recognize evaluations performed using the Common Criteria evaluation methodology where product certificates have been issued by the Mutually Recognized producing nations for EAL1 to EAL4 evaluations. (Note: Evaluation Assurance components found in EAL5-EAL7 are not part of the mutual recognition arrangement.) Since October 1998, an additional eleven nations have joined the Arrangement. The list of product validations that have been mutually recognized by the United States Government can be found on the CCEVS Validated Products List.

14. What is the relationship of NIAP's CCEVS and NIST's Cryptographic Module Validation Program? (CMVP)

Both the Common Criteria Evaluation Validation Scheme (CCEVS) and the Cryptographic Module Validation Program (CMVP) are intended to evaluate the robustness levels provided by individual COTS IA products. While both programs are used to evaluate robustness levels with COTS IA and IA-enabled products, they each focus on different aspects of the product and use different criteria. The CMVP program provides customers with confidence that commercial cryptographic modules meet one of the four security specification levels documented in FIPS 140-2, Security Requirements for Cryptographic Modules, and that the FIPS-approved algorithms are properly implemented. Conversely, the CCEVS focuses more on confidence that the non-cryptographic security functions of an IA or IA-enabled IT product meets one of the seven robustness levels (i.e. EALs) documented in the CC. Products are encouraged to be evaluated under both programs if the product encompasses both cryptographic and non-cryptographic security modules.

15. What U.S. laboratories have been approved to perform CC and FIPS 140 evaluations?

An up to date list of NIAP CCEVS and FIPS 140 accredited testing laboratories can be found on their respective web sites:

- CCEVS Accredited Laboratories
- FIPS 140 Cryptographic Module Validation Program

(V) Developers and NSTISSP #11

1. What are Protection Profile compliant products? Should I attempt to make my product compliant?

The difference between products compliant with a protection profile and products that are not compliant is based on a determination as to whose requirements are being met (i.e. is it the vendor's or the customer's). For products claiming compliance to a specific protection profile, the requirements are set and the vendor must include in the product's security target all of the requirements stated in the protection profile. If, during the evaluation, it is determined that the product has difficulty in satisfying a requirement, the vendor must either fix the product, or drop their claim of conformance to the protection profile. For products not claiming compliance to a protection profile, the vendor only has to include in its security target those requirements for which they desire an evaluation. If, during the evaluation, the product has trouble satisfying a particular requirement, the vendor has the option to remove the requirement (i.e. the claim) from the security target and proceed with the evaluation. Products that are compliant with a protection profile provide the consumer with confidence that all of the necessary requirements for the technology operating within the defined level of concern or robustness (e.g. Basic, Medium or High) have been satisfied. For products that do not claim compliance with a protection profile, the consumer must ensure that the security target for the evaluation includes all of the necessary requirements for the particular level of concern or robustness where they plan to use the product. Whether developers should pursue compliance of a given protection profile relates directly to the market they are attempting to obtain. If a significant portion of a vendor's targeted market is the National Security Community, specifically the Department of Defense, and the DoD states that products conforming to a U.S. Government protection profile will get preferential treatment, then that vendor may make a business decision to have their product evaluated against the protection profile. If a vendor's targeted market is largely non-DoD, then the vendor may determine that the business case is not strong enough to warrant undergoing evaluation and will choose to not market to the DoD or National Security Community. However, it is often the case that many other communities, in the absence of any other industry security guidance, take advantage of National Security Community policies and programs to their own end. The bottom line is that developer's need to have a sense of what market they are attempting to satisfy and understand there may be secondary markets that are influenced by policy statements and standards made by the National Security Community. A developer should consider this carefully when determining whether to initiate a profile compliant evaluation without a specific customer or procurement in mind.

2. Should I attempt to get my product evaluated before a prospective customer requests one?

If it is likely that your product will be used to enforce a security policy, you should probably consider an evaluation. IA products (e.g., firewalls) will always be purchased to enforce a security policy and fall into this category. For IA-enabled products, it is not quite as clear. Whether you will be required to pursue evaluation depends heavily on how your product is to be used. If, as part of its other functions, it is likely that it will be enforcing some piece of a customer's security policy, the functions that are most likely to be used for this enforcement should be evaluated. However, if the functions are not likely to be used, it may be prudent to wait for an evaluation to be requested by a prospective customer. Some IA-enabled products (e.g., operating systems) are almost always an integral part of the security policy enforcement solution. Developers of these products should consider evaluation.

3. How do I get a GOTS product validated?

NSA has a number of programs to evaluate and validate GOTS IA products. Contact NSA's Information Assurance Business Affairs Office at 410-854-6091.

4. How much does an evaluation cost?

Costs will vary depending on the complexity of the product. Vendors are encouraged to contact multiple NIAP CCEVS accredited laboratories to compare expertise, experience, and costs. Costs of evaluations are negotiated between the vendor or sponsor of the evaluation and the evaluation laboratory. NIAP is not involved in these negotiations. The goal established for low assurance products (i.e., EAL 1) is 30-90 days of evaluation time and will cost less that higher assurance (e.g., EAL4) evaluations. All of the NIAP CCEVS accredited labs offer consultancy services to help the vendor determine what will be required prior to formally entering the evaluation process.

5. What do I do to start a Common Criteria evaluation? How does the process work?

The CCEVS evaluation process requires that a vendor first develop a document called the security target, which makes security functionality claims about the product. The next step in the evaluation process is for the vendor to take its security target to one of the NIAP accredited Common Criteria Testing Laboratories (CCTLs) for formal evaluation. The CCTL will evaluate the security target for completeness, consistency and conformance. Once this is successfully completed, the CCTL will evaluate and validate how the product satisfies its security target. At the conclusion of the evaluation, if the product has satisfied all requirements, CCEVS will issue a certificate validating the products' evaluation, place the product on the Validated Products List; and make a Validation Report available to the public. After a product has successfully completed an evaluation, the vendor has two options for maintaining the validity of the evaluation as the product evolves from one version to the next:

1. Request a re-evaluation of the next version of the product, or
2. Participate in Assurance Continuity.
    - The purpose of Assurance Continuity is to enable developers to provide assured products to the IT consumer community in a timely and efficient manner.
    - The awarding of a Common Criteria evaluation certificate signifies that all necessary evaluation work has been performed to convince the evaluation authority that the TOE meets all the defined assurance requirements as grounds for confidence that an IT product or system meets its security objectives.
    - Assurance Continuity recognizes that as changes are made to a certified TOE or its environment, evaluation work previously performed need not be repeated in all circumstances. Assurance Continuity therefore defines an approach to minimizing redundancy in IT Security evaluation, allowing a determination to be made as to whether independent evaluator actions need to be re-performed.

6. I have a product, which contains a cryptographic module along with other mechanisms to implement separate security features. Do I need two evaluations? Why? What is the relationship between the CCEVS and the CMVP?

Depending upon the IA or IA-enabled features of the product, both CCEVS and CMVP evaluations may be necessary for system certification and accreditation. Depending on user applications, the CMVP may be sufficient for validating the robustness level of a COTS product and providing the basis for implementation and commencement of operational use. However, in most cases, the evaluated COTS IA or IA-enabled IT products are often integrated into broader IT systems that address more than one security requirement. For example, tested cryptographic modules are often integrated into other commercial IT products with additional non-cryptographic functions. The confidence provided by CMVP testing does not imply an overall confidence with regard to the other aspects of the IT product or system into which the module may be integrated. In such cases, a separate CCEVS evaluation process should be used to complement the CMVP certification process with the objective of ensuring that the overall system configuration is adequately addressing all of the desired security requirements. As a general rule, the CMVP should be viewed as sufficient for the evaluation of products where encryption is the only security requirement (e.g. standalone encryption applications or Virtual Private Networks (VPNs)). Products that integrate basic data encryption with other IA functions (e.g, firewall access controls) require evaluation of the cryptographic components (in accordance with the CMVP), as well as the evaluation of the other IA system components in accordance with the requirements of the Common Criteria.

(VI) NSTISSP #11 and National Security System Product Testing Programs

1. Do products for which NSA has produced Configuration Guidance meet NSTISSP #11 validation requirements?

The existence of NSA-produced Configuration Guidance for a product does not mean that the product meets NSTISSP #11 validation requirements. When available, NSA-produced Configuration Guidance is used to complement the results of NSTISSP #11 validation. These are two related, but separate activities. The reason for this is that, configuration guidance captures (in the form of specific configuration settings, file permissions, security rule set up etc) the tradeoffs between prudent security behavior and useful "operations". An evaluation/validation offers a rigorous analysis of the product implementation and behavior in its secure configuration.

2. Do SABI/TSABI approved COTS IA/IA-enabled IT products qualify as "validated" under NSTISSP #11?

Generally not. However, much of the information that is created in the context of preparing a product for use in a SABI/TSABI environment will contribute greatly to a NIAP COTS testing activity and vice versa. As noted in Policy Information and Guidance Question 15, if the COTS product has already been procured and fielded, it need not retroactively go through a NIAP testing activity. However, if a COTS IA/IA-enabled IT product resides on the SABI/TSABI list and is being purchased after July 1, 2002, it is subject to NSTISSP #11 COTS IA testing.

3. What is the difference between NIAP CCEVS evaluated products and NSA approved products?

Products found on the NIAP Validated Products List (VPL) have been tested and shown to meet the security requirements articulated in their associated security targets. Residing on the VPL, by itself, is not grounds for NSA or NIST endorsement of the product. It is only an acknowledgement that the product's security claims have been tested using a Common Evaluation Methodology and that those claims have been shown to be true to a certain level of confidence (i.e., It does not make a statement that the claims that were made were indeed the right ones to make.) However, some products on the NIAP VPL will be approved by NSA. Specifically, products that meet one of NSA's approved Protection Profiles that have been written for various technologies (e.g., operating systems, firewalls) fall into this category. The NIAP Validated Products List clearly annotates those products that are compliant to NSA approved Protection Profiles. In addition to products that meet approved NSA protection profiles, NSA maintains a Products and Services Catalog that contains other GOTS products that have been approved by NSA for use. Contact the NSA Information Assurance Service Center for more information at 1-800-688-6115.