Statement of

Edward Roback

Chief, Computer Security Division
National Institute of Standards and Technology

U.S. Department of Commerce

Before the

Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

"Exploring Common Criteria: Can it Ensure that the Federal Government Gets Needed Security in Software?"

September 17, 2003

Chairman Putnam, Representative Clay, and Members of the Subcommittee, thank you for this opportunity to testify today. The Computer Security Division at the National Institute of Standards (NIST) has direct responsibility for NIST's activities associated with Common Criteria and the National Information Assurance Partnership. In response to the issues raised in the letter of invitation, I would like to first discuss what security assurance is and the role it plays in overall cyber security. I then will turn to the role that security testing, and specifically the Common Criteria (CC) and the NIST-National Security Agency (NSA) National Information Assurance Partnership (NIAP), play in helping to bring about security assurance. Finally, I would like to leave with you some ideas as to what else the cyber security research community could do to improve the trust and confidence we have in the proper, correct, and secure functioning of information systems.

Security Assurance

Assurance is the basis we need for overall trust and confidence in the correct *and* secure operation of information systems. The overall question of assurance tries to address two important questions: Does a system do what it is supposed to do? And, does the system do anything that is unintended? Within this context, *security assurance*, simply put, is the degree of confidence one has that the security measures of a system work as intended; it is *not* an absolute guarantee that security is achieved. We need to keep this in mind when discussing the NIAP, or any other security testing program. Today I will be speaking primarily to the question of security assurance, within this overall context.

Why is security assurance important? The risks we decide to take with regard to systems are based upon the system vulnerabilities and an assessment of potential losses if such vulnerabilities become manifest. (There are formal definitions of "risk levels" in the security community, but I am using the term in a more general sense here.) This can be clearly seen with life-critical systems. We generally are not willing to accept the potential losses from failure of a life-critical system! Rather, a high degree of confidence is required in the correct and secure operation of a system that could result in a loss of life. If we have good reasons to be confident in the security of a system, we can reasonably be expected to rely upon the system for more important tasks and the processing of more sensitive information. In the Federal context, security assurance is an important input to the security accreditation process, namely the decision by a management official to place a system into operation.

How is security assurance obtained? There is no single way. One can gain *some degree* of confidence in the security of a system (or component, etc.) by looking at the process of how the system is built. If a rigorous methodology of requirements definition, design specification, and conformance or acceptance testing is in place, one would generally have more confidence in the resulting system than one developed haphazardly. Similarly, use of advanced software engineering techniques can provide assurance. The past experience of use of a particular system is another means by which one can gain *some degree* of assurance. If a system is used by a hundred organizations without security incidents (which, by the way, can be most difficult to ascertain), one can make a

reasonable leap-of-faith that it will also operate securely in the hundred-and-first. Manufacturers' warranties or lack thereof is another means to have *some degree* of security assurance. Ensuring the continued security of a system once in operation is also important. Scanning tools can be (and should be) used to help ensure that important security settings are maintained and that known vulnerabilities are located and patched. There are many other means as well to help obtain and maintain security assurance. Of course, last but not least, is the use of independent security testing and evaluation to help achieve security assurance.

Security Testing and Evaluation

Security testing can be achieved through a range of means from the straightforward and repeatable through more complex and time consuming processes.

When a standard specification exists, such as an encryption algorithm, it is a reasonably straightforward (but not necessarily easy) process to determine whether the algorithm is correctly implemented. In this case, the specification is exact, and the tests can be correspondingly precise. NIST refers to this process as conformance testing and *validation.* I should note here that the Cryptographic Module Validation Program operated by NIST and the Communications Security Establishment of the Government of Canada provides such algorithm and related testing.

On the other hand, as we look at more complex and diverse information technology (IT) products lacking common/standard specifications, we are often confronted with products containing millions of lines of software code for which a standard bits-and-bytes level specification does not exist. Testing such products necessarily involves human subjectivity; NIST refers to such testing as *evaluation*. That is not to say evaluation cannot be and is not rigorous; it certainly can and probably should be more rigorous than current practices (depending upon the level of effort and time one wishes to expend.) What I am saying is that such testing is considerably removed from more straightforward, "black-box", yes/no testing. Although there is promise for the use of formal methods here, today the use of such techniques is considered by vendors to be expensive. Formal methods are of particular note as they can both be used to increase the quality of software and to facilitate the automatic generation of tests, including expected outputs, from formal specifications. A 2002 NIST commissioned study of the economic impact of software quality showed that software bugs, or errors, are so prevalent and so detrimental that they cost the U.S. economy an estimated $59.5 billion annually, or about 0.6 percent of the gross domestic product. Findings of the 309-page report are intended to identify the infrastructure needs that NIST can meet through its research programs. Though assurance programs can be built by various sectors NIST's programs address assurance, trust and confidence in general.

Next, let me turn more specifically to the NIST-NSA NIAP program, which provides security evaluation of IT products and is built upon the use of the CC.

Common Criteria

Development of the CC began in 1993 in response to efforts by a range of nations to develop IT security evaluation criteria. Efforts were underway in Canada, the U.K. and the E.U. to develop such criteria at the same time the US was considering a revision to the 1985 Department of Defense evaluation criteria commonly known as the "Orange Book." The development of different sets of criteria, which were not harmonized, presented costly potential conflicts to the IT industry. Vendors were going to be faced with the need to undergo multiple security evaluations in multiple countries. The likelihood of non-tariff barriers to trade loomed large. For this reason, security experts from NIST and NSA partnered with the U.K., Canada, Germany, France and the Netherlands and set a goal of developing a single set of criteria under which security evaluations could take place.

In May of 1998, the CC was completed. The 800-plus page document is known formally as ISO/IEC 15408: Common Criteria for Information Technology Security Evaluation. It is intended for use for either the specification of security requirements (i.e., properties) of a product (e.g., a specification for the security capabilities in a firewall), as the basis for security evaluation of security requirements of IT products and systems, or both.

As a security requirements specification language, the CC enables user communities (e.g. health care, financial, SCADA) to state to technology providers what security capabilities they desire in products they wish to buy. In addition, developers of specific products can use the CC to tell potential customers exactly what security capabilities are contained in the product.

As the basis for the evaluation of security requirements, the CC permits comparability between the results of independent security evaluations. It does so by providing a common taxonomy of security functional requirements for describing IT products and systems and of assurance measures that are applied during development and evaluation of the products/systems. The evaluation process establishes a level of confidence that the products and systems conform to their stated security functional and assurance requirements, which have been specified using the CC. The evaluation results are intended to help consumers determine whether the IT product is secure enough for their intended application and whether the security risks are acceptable.

The great potential of the CC is both in (1) its use to express "good sets of requirements" and (2) to provide assurance, through evaluation, that products comply with these requirements. Examples of how various user communities have and are using the CC to state its security requirements are given later. Unfortunately, the use of the CC as a requirements specification language has been under-utilized.

Common Criteria Mutual Recognition Arrangement

The completion of the CC was followed by the signing of the CC Recognition Arrangement (CCRA), now including 17 signatory nations, in order to reduce the cost of multiple evaluations to vendors. In October 1998, Government organizations from the United States, Canada, France, Germany, Netherlands, and the United Kingdom signed an historic mutual recognition arrangement for Common Criteria-based evaluations. The Arrangement, officially known as the *Arrangement on the Recognition of Common Criteria Certificates in the field of Information Security*, was a significant step forward for Government and industry in the area of IT product security evaluations. The partners in the Arrangement share the following objectives in the area of Common Criteria-based evaluations of IT products:

- To ensure that evaluations of IT products are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products;
- To increase the availability of evaluated, security-enhanced IT products for national use;
- To eliminate the need for redundant evaluations of IT products; and
- To continuously improve the efficiency and cost-effectiveness of security evaluations and the validation process for IT products.

The purpose of this Arrangement is to advance those objectives by bringing about a situation in which security-enhanced IT products that earn a Common Criteria certificate can be procured or used without the need for them to be evaluated and validated again. It seeks to provide grounds for confidence in the reliability of the judgments on which the original certificate was based by declaring that the Validation Body associated with a Participant to the Arrangement shall meet high and consistent standards. The Arrangement specifies the conditions by which each Participant will accept or recognize results of IT security evaluations and the associated validations conducted by other Participants and to provide for other related cooperative activities.

Since it original signing, Australia, New Zealand, Greece, Finland, Israel, Italy, Spain, Norway, Austria and Sweden have signed the arrangement. In addition, a number of countries such as Japan, Russia, and Korea have indicated their intent to accede to the arrangement.

National Information Assurance Partnership

As the CC was nearing completion, NIAP was created in 1997 by NIST and NSA to bring together the technical expertise from both agencies to focus on the development of cost-effective testing and evaluation techniques and methods for assessing the security features in commercial off-the-shelf IT products. The partnership emphasized the use of the CC, the involvement of other industrialized nations beyond the United States in recognizing the results of the security evaluations performed, and the participation of private industry, whenever possible, in developing security-enhanced IT products and in

conducting security evaluations. In the U.S., NIAP security evaluations are conducted by commercial testing laboratories that have been accredited under NIST's National Voluntary Laboratory Accreditation Program.

The NIAP Validation Body assesses the results of a security evaluation conducted by a testing lab and issues a CC certificate. The certificate, together with its associated validation report, confirms that an IT product has been evaluated at an accredited testing laboratory using the Common Methodology for conformance to the CC. The certificate also confirms that the IT security evaluation has been conducted in accordance with the provisions of the testing program and that the conclusions of the testing laboratory are consistent with the evidence presented during the evaluation that the product conforms to its security specification. I should note, the certificate does not mean that the product is necessarily secure. I will speak more about that later.

NIAP maintains a Validated Products List on its web site containing all IT products that have successfully completed evaluation and validation under the testing program. The validated products list also includes those products that have successfully completed similar processes under the testing programs of authorized signatories to the CC MRA.

Today, NSA leads the day-to-day operations of the Validation Body, that is, NSA reviews and validates the test results and issues the CC certificate for the vendor's product based on the lab assessment. NIST leads the laboratory accreditation program bringing in new laboratories to the testing program and re-accrediting the current network of CC testing labs. Given resource constraints, this division of labor and responsibilities for the testing program seems to be the most effective method of allocating resources.

The Meaning of a NIAP (or Other) Common Criteria Certificate

As I mentioned earlier, it is important to understand exactly what CC evaluation, and specifically a CC certificate means. A CC evaluation is a measure of an information technology product's compliance to the vendor's claimed security (specification using the Common Criteria). It is not a measure of how much protection the claimed security specification provides nor does it guarantee that the product is free from malicious or erroneous code. Any product that has a CC security specification can undergo an evaluation and receive a certificate if it successfully completes the evaluation. It is important for users to understand what the issuance of a CC certificate does and does not imply. A CC certificate:

- **Does** mean that NIST and NSA (or equivalent government organizations participating in the CCMRA) believe the evaluation has been conducted properly and the conclusions of the private sector testing laboratories are consistent with the evidence produced.
- **Does** imply that a good faith effort has been made to ensure that the product conforms to the security claims stated by the vendor in the security specification.
- **Does not** imply **with absolute certainty** that the product conforms to the security claims stated by the vendor in the security specification.

- **Does not** imply that the product conforms to security claims in documents other than the security specification (i.e., security claims in promotional literature, vendor documentation, and other documents **are not** covered by the validation certificate).
- **Is not** an endorsement or warranty of the product by NSA and NIST (or by equivalent government organizations participating in the CCRA).
- **Does not** imply or guarantee that the product is free from malicious or erroneous code.
- **Does not** imply that security functional specifications and achieved level of assurance of the product provide adequate protection for data contained in the product's intended operational environment.
- **Does not** presume that subsequent versions or releases of the product should not be or do not have to be evaluated.

Upon successful completion of a CC evaluation, the product's security specification and the Validation Report are posted to the NIAP website (http://niap.nist.gov/cc-scheme/ValidatedProducts.html) to allow consumers to confidently make acquisition decisions regarding different products.

Use of the Common Criteria

Within the U.S. Federal Government, the use of CC and NIAP- evaluated products is addressed by NIST through its advice to agencies for non-national security systems through "Guideline to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products," (See NIST Special Publication 800-23, available at http://csrc.nist.gov/publications/nistpubs/index.html). This publication describes how assurance in acquired products supports security and the benefits that can be obtained through testing of commercial products against customer, government, or vendor-developed specifications. Also discussed is the need for Federal departments and agencies to acquire and use products appropriate to their risk environment while considering cost-effective selection of security measures. NIST recommends that Federal agencies give substantial consideration in IT procurement and deployment for IT products that have been evaluated and tested by independent accredited laboratories against appropriate security specifications and requirements. The Committee for National Security Systems (CNSS) has issued its CNSS Policy #11, recently amended, to address national security systems, and I will defer to my colleagues from that community to address it. The potential extension of CNSS Policy #11 beyond the national security community may be addressed as part of the national review of NIAP called for in the White House's *National Strategy to Secure Cyberspace* (February 2003). However, more data is needed on the impact of the policy before extension is considered or recommended. As the national security community gains experience from its policy, one can consider whether it should be extended to non-national security systems.

Other governments are also adopting, on either a voluntary or regulatory basis, the use of the CC. France has in place a regulation recommending use of CC evaluations for public administration. The European Union has passed a resolution on information and network

security addressing use of the CC for electronic signatures. The CC has been adopted by NATO as a standard. In Germany CC evaluations are required in their digital signature legislation.

Use of the CC by User Communities to state their security requirements

As mentioned earlier, we believe the most under-utilized aspect of the CC is as a requirements specification language. While there are some excellent examples of such use, the full benefits of the CC will not be achieved until there is a better balance between its use for evaluation and for security requirements specification. When used as requirements specification language, the CC allows communities-of-interest that procure IT products to state the security requirements they wish to have developers supply in products. The security requirements can be for technology-specific products or for application-oriented use. As an example of technology specific security requirements, NIST and NSA are developing security requirements for technologies such as firewalls, intrusion detection systems, biometrics, and operating systems. The security requirements are developed using the CC Protection Profile construct. These profiles are statements by NIST and NSA about what "good" security requirements are for these technologies.

As examples of application-oriented Protection Profiles, we cite:

- The major bankcard issuers (e.g., American Express, Mastercard, Visa) formed a working group that used the CC to develop a profile for the smartcards they issue to their customer banks. A significant effort (the first of this type) was the group's development of their profile for smartcards.
- The Financial Services Roundtable/BITS, whose members consist of major banks and insurance companies, has used the CC to specify the security functionality its members would like to see in various IT products. When a product that meets BITS security functionality receives a CC certificate, BITS will issue its mark on that product based on the CC evaluation that was performed.
- The Process Control Security Requirements Forum (PCSRF), led by NIST, is composed of government and private sector representatives who are defining security requirements for products used in real-time processing and SCADA systems. The goal of this effort is to influence the key vendors that supply products and systems globally for real-time and SCADA systems to meet process control security requirements. If vendors respond to these market signals, the improved security would be reflected in major critical infrastructure systems such as nuclear power plant control; electric power generation and distribution; control of water distribution; building environmental, security, and safety controls; and manufacturing plant controls.
- The healthcare community, with NIST's assistance, has used the CC for defining security requirements. Examples include: functional security requirements for Health Care Financing Administration's Proposed Internet Security Policy; functional security requirements for the Department of Health and Human Services which maps the Health Insurance Portability and Accountability Act of

1996 Proposed Rule on "Digital Signature and Security Standards" into CC constructs; and a complete profile for patient "Point-of-Care Admission, Discharge and Transfer" in collaboration with Share Medical Systems (SMS).

As can be seen by these examples, the use of the CC for requirements specification is a first key step in improving the protection of our critical infrastructures—identification of sets of security requirements for IT products. This would have significant benefits even if security evaluations were not conducted. However, utilizing the CC as an evaluation tool against user-defined security requirements provides additional confidence that the products procured and deployed actually meet the desired security specifications.

The Road Ahead: Research and Resource Challenges

One of the criticisms often levied on NIAP is that evaluations take too long and cost too much. We hear this particularly from the small business community. Of course, one would expect to hear that of any evaluation process that is not free and instantaneous. But, in products involving great complexity and often millions of lines of code, such evaluations are time consuming. They also require rare expertise that is pricey in the marketplace. But we must ask ourselves whether improvements can be made? Indeed, given resolve, flexibility, resources, and research, I believe significant progress can be made.

Improving Current NIAP Testing

Here are some examples of what *could* be done:

- Develop NIAP guidance advising product developers how to reuse evaluation results from prior evaluations of the product.
- Develop NIAP guidance to maintain Common Criteria certificates for product maintenance changes (i.e., new versions) without the need to undergo a complete new evaluation.
- Develop an Assurance Maintenance module for the standard so only the changes to a previously evaluated product need be evaluated.
- Develop CC interpretations that clarify and simplify how parts of the CC are to be evaluated.
- Develop technology area-specific tests and test methods (e.g., smart cards, biometrics) that will provide more uniformity and comparability of evaluation results and result in more rapid evaluations for products.
- Using technology area-specific tests and test methods, establish accreditation criteria for labs that wish to specialize in evaluating products in a specific technology area (e.g., smart cards). Extend NIAP accreditation, on a voluntary basis, to those labs that wish to specialize in the technology area. This will result in cheaper, more rapid and more consistent evaluations for products in those technology areas
- Provide better training to lab evaluators and NIAP validators, with emphasis on which actions need to be performed and which do not.

- Provide an extensive/complete set of guidance documents for all stakeholders in the evaluation process (e.g., developers, evaluators, validators, commercial and government users).
- Provide clear guidance to stakeholders to choose only those assurance requirements that are meaningful for their intended use/environments.
- Perform a critical assessment of the current evaluation process to ensure that:
    - NIAP activities and levels of effort are consistent with those of other CC Recognition Arrangement partners
    - Evaluation activities are being performed efficiently
    - There are no unnecessary activities being performed
    - All activities that can be performed in parallel are in fact done that way.

We intend to seek out new partners, particularly in the homeland security community, to help support these activities in the near future.

Beyond NIAP

While these are key examples of what can be done to improve the current process, there is much more that should be done in order to address security assurance. Here are some examples:

- Conduct more research with the objective of developing new means to conduct security testing. The current techniques we have are either too expensive, involve too much human subjectivity, or both. The sooner the community pursues such research, the sooner we will benefit from their results.

- Develop comprehensive security requirements in both plain English and in the CC "language" that will be used to build more secure systems and networks. These security specifications must be developed with significant industry (users *and* vendors) and government involvement in key technology areas such as operating systems, firewalls, smart cards, biometrics devices, database systems, public key infrastructure components, network devices, virtual private networks, intrusion detection systems, and web browsers. These efforts can be adopted by voluntary industry consensus standards bodies as appropriate and can draw upon efforts underway in the NSA for national security systems.

- While it is important to understand and test security at the *product* level (the principal focus of NIAP), we need also to look outwards at the *system* and *enterprise architecture* level. For example, we need a means to rigorously understand the security implications that result when NIAP evaluated products are integrated together into a system. We also need to look inwards at IT building blocks such as protocols. Again, research will be a key to advancing our ability to make significant strides.

- We also need to look at other important security issues beyond just the (admittedly important) question of whether a product meets a security

specification. How do we gain assurance that the product does not do what is unintended? How can we gain assurance that no malicious code is buried deep inside software or hardware? How can we do such analysis as more and more development is taking place off-shore? Again, research is needed.

I would point out that the Cyber Security Research and Development Act of 2002 provides a means to support such research via academic and for-profit partnerships, in addition to intramural research at NIST.

Summary

The CC provides a means to develop security specifications and a common means to conduct security evaluations. NIST and NSA have created the NIAP, which uses accredited labs in the private sector to conduct such evaluation. However, more can be done to streamline this process through research and standards development.

Thank you for the opportunity to testify here today. I would be pleased to answer any questions you may have.