CYBER SECURITY
INDUSTRY ALLIANCE

NIAP Certification:

Proposals by CSIA for Strengthening Security Certification

July 23, 2004

CONTENTS

SUMMARY

NIAP is the National Information Assurance Partnership. This U.S. government initiative aims to meet security testing needs of consumers and producers of information technology. NIAP is a collaboration of the National Institute of Standards and Technology and the National Security Agency. It oversees U.S. implementation of the international information technology security standards called Common Criteria – the essence of NIAP testing. The intention of NIAP is to increase the level of trust in information technology systems and networks with cost-effective security testing, evaluation and validation programs. The Cyber Security Industry Alliance (CSIA) supports broad use of a single efficient and effective process for security certification. CSIA is the public policy and advocacy group of security software, hardware and service vendors addressing key cyber security issues. CSIA wants to improve the Common Criteria and NIAP process to achieve the promises of NIAP certification. We especially want to avoid pitfalls of a balkanized certification environment.

In this briefing, CSIA echoes broad concern from industry and user organizations about NIAP. NIAP mainly serves government agencies in the U.S. defense and intelligence community. NIAP is not used by federal civilian agencies or the commercial sector. Many commercial users are concerned that NIAP testing is ineffective, unrealistic, cost prohibitive, has low demand and does not guarantee strong cyber security.

On the other hand, CSIA believes the potential benefits of helping NIAP achieve its goals are too important to ignore. The Alliance urges NIAP to consider the issues described in this report. Common Criteria for security products may not be a panacea, but global standards are the nation's best bet for improving cyber security and protection of critical infrastructure. The Alliance briefing recommends four ways to reach the promise of NIAP testing and certification, beginning with a Common Criteria Users Forum meeting in the Washington, DC area in October 2004.

NIAP'S CHARTER

CHARTER

To increase trust in IT systems and networks with cost-effective security testing

The National Information Assurance Partnership aims to increase the level of trust in information technology systems and networks with cost-effective security testing, evaluation and validation programs. NIAP states five goals (see http://niap.nist.gov/):

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

BENEFITS OF NIAP TESTING

BENEFITS

- **National testing program**
- **Standard way to test and compare**
- **Aims to lower costs of testing**
- **Help foster stronger cyber security**

NIAP certification testing is based on the Common Criteria Evaluation and Validation Scheme (CCEVS) and ISO 15408. Common Criteria is the global standard framework for information technology product evaluations. Nineteen countries recognize Common Criteria certifications. The Department of Defense requires its agencies to purchase NIAP-certified information technology products. Currently, federal civilian agencies and commercial users are not required to use NIAP-certified products.

NIAP promotes and manages the CCEVS Validation Body as a national program for evaluating information technology products for conformity to Common Criteria. Commercial testing laboratories require accreditation by the National Institute for Standards and Technology and approval by the Validation Body to conduct NIAP evaluations.

The NIAP evaluation is a standard way to test and compare security products and validate vendor security claims. The value of NIAP testing includes use of a repeatable, objective methodology plus evaluation with expert judgment and background knowledge.

Most organizations traditionally have relied on the reputations of vendors or tested products themselves with in-house staff or consultants. NIAP testing brings the benefit of independent, third party testing and a standard methodology. The program’s Mutual Recognition with other countries supporting Common Criteria automatically provides worldwide acknowledgement of certification.

With NIAP testing, all buyers of information technology get trusted, independent assurance that technology products perform to standard security specifications.

ISSUES WITH NIAP TESTING

TESTING ISSUES

- **Too expensive and slow**
- **Protection Profiles need broader input**
- **Custom testing processes inhibit goal of NIAP**
- **Procurement policy is misunderstood and application is inconsistent**
- **Uneven acceptance of certified products**

NIAP testing promises important benefits. But in light of issues detailed below, CSIA believes the current NIAP testing scheme is impractical for many organizations. Taken alone, NIAP testing does not always result in stronger cyber security because certification only warrants that a product performs according to a security specification. Some viruses and worms can affect a portion of the product that was not claimed in a Security Target or Protection Profile. In those cases, NIAP certification is irrelevant. CSIA believes NIAP can enhance the value of its certification program with joint development of security specifications by the government, users and security experts. Our briefing incorporates recent findings from the National Cyber Security Partnership (NCSP) Technical Standards and Common Criteria Task Force (www.cyberpartnership.org/init-tech.html). The NCSP Task Force included experts from the Business Software Alliance, the Information Technology Association of America, TechNet and the U.S. Chamber of Commerce in voluntary partnership with academicians, CEOs, federal government agencies and industry experts. Addressing these findings now is vital to shore up the viability of NIAP and Common Criteria as a true international security-testing scheme to be used by commercial as well as government organizations. Security needs of commercial users are particularly important because 85% of critical infrastructure in the U.S. is operated by the private sector (www.dhs.gov/dhspublic/interapp/editorial/editorial_0465.xml).

NIAP Testing Is Too Expensive and Slow

Lab fees for NIAP/Common Criteria evaluations can be hundreds of thousands to millions of dollars for testing each product. Vendors pay for these evaluations without the ability to pass costs to customers requiring NIAP certification. The financial burden is onerous for vendors with a broad range of products requiring NIAP certification. The long certification process also slows time-to-market for new products because testing can take months or more than a year. Updates to products require a re-certification of the product, further adding to the cost and evaluation time. In particular, NIAP testing does not meet the needs of new-generation Commercial-Off-The-Shelf (COTS) products that are created or integrated with rapid development cycles. Vendors would be more willing to invest in NIAP testing if there were appropriate returns on these investments in the form of customer demand and improved product security.

Protection Profiles Need Broader Input

NIAP is too focused on needs of the U.S. government defense and intelligence community. Many Protection Profiles are developed by the National Security Agency and are not appropriate or applicable to requirements of civilian agencies and the private sector. These profiles get little input from the actual users and developers of the products. End users either cannot articulate their security requirements or are not asked to contribute toward the development of Protection Profiles. Revisions to and re-certification of Protection Profiles take too long. Some are too specific, especially when they reflect old security technologies. This stifles innovation by developers. A major issue is that NIAP testing currently assumes a monolithic product model. Evaluated products are assumed to combine hardware, operating system and application software. This is especially true with the development of the Medium Robustness Environment guidance. That assumption makes certification difficult, if not impossible for many application software products that are developed on top of operating systems, networks and other products. Certification is especially challenging when security products are integrated with several COTS products. CSIA believes Protection Profiles will continue to have limited utility without more input from users and security experts.

Custom Tailored Testing Processes Inhibit Goal of NIAP

The whole point of NIAP and Common Criteria is uniform testing and evaluation. In reality, testing processes by accredited labs are not uniform and do not enforce repeatability with automation. Emphasis during testing shifts with experiences of respective evaluators. CSIA acknowledges the difficulty of maintaining 100 percent consistency during an evaluation, particularly when unique tests must be written for each product. Nevertheless, NIAP could provide more comprehensive guidance to accredited evaluators and labs with sample test documentation showing the level of expected coverage.

Procurement Policy Is Misunderstood and Application Is Inconsistent

Many buyers are either unaware of NIAP/Common Criteria or do not consider it as an essential quality measure for security products. Some buyers treat NIAP/Common Criteria as a checkbox item. They often do not understand how a particular NIAP certification applies to security policies stipulated by their agency. This practice may stem from the lack of involving users in articulation of security requirements for Protection Profiles. NIAP certification is required when Department of Defense agencies buy security products using COTS software (see NSTISSP #11 and DoDI 8500). This policy is flawed because NIAP testing requirements are unrealistic for COTS products. It assumes vendors use a development model that freezes product requirements early in the design phase. That's the opposite of how most developers now make software. Use of COTS tools, standard application programming interfaces and web services makes it easier to add or enhance features. Cyber security threats change daily so it is appropriate that developers quickly improve COTS products to be more effective and competitive. Unfortunately for buyers requiring NIAP certification, any change in a product invalidates its certification. Re-certification can take as long as a complete re-evaluation so buyers limited to NIAP-certified products often must use out-of-date software in order to comply with Department of Defense directives. Inconsistent implementation of this policy is another issue. Some agencies allow procurement of products "in evaluation" and others have no requirement for evaluation.

GLOSSARY

CC or Common Criteria
Global standard framework for information technology product evaluations

CCEVS Common Criteria Evaluation and Validation Scheme for product producers and users

COTS Commercial-Off-The-Shelf-Software

EAL Evaluation Assurance Levels provide predefined values where EAL1 is the lowest and EAL7 is highest level of security robustness

NIAP National Information Assurance Partnership, a collaboration of National Institute of Standards and Technology, and National Security Agency

Protection Profile
Specification document of product requirements for security

Security Target
Specification document vendor uses for claims about security functionality, sometimes called a TOE or Target of Evaluation

Uneven Acceptance of Certified Products

NIAP certification is required by a small fraction of the market for security products. U.S. Department of Defense buyers are the main group requiring NIAP certification. Commercial buyers hardly ever require NIAP certification; many are unfamiliar with NIAP testing and Common Criteria. The low demand for NIAP certification promises low revenue for selling those products. CSIA believes the financial incentive for vendors to fund all NIAP testing is low, which leads many vendors to forego NIAP evaluations and deprives buyers from the broadest choices of security products. Testing fragmentation compounds when commercial sectors develop their own certification program. For example, the financial services sector felt compelled to develop its own security standard called the BITS Product Certification Program. BITS includes some aspects of Common Criteria but adds other unique requirements. CSIA believes NIAP must extend its practical appeal beyond the government intelligence community to avoid balkanizing security certification into a costly, cumbersome and ineffective hydra.

CSIA ACTIONS & RECOMMENDATIONS

A/R'S FROM CSIA

1. **Discuss & develop improvements**
2. **Provide open forum**
3. **Develop specific timelines and individual actions**
4. **Educate about Common Criteria benefits**

Governments have invested millions of tax dollars to develop the Common Criteria. With global recognition of Common Criteria by governments and particularly by the U.S. Department of Defense, the Cyber Security Industry Alliance believes the idea of NIAP-authorized certification is crucial for helping the IT industry improve cyber security and protect critical infrastructure.

The NIAP Review and the National Cyber Security Partnership Technical Standards Task Force recommendations report on Common Criteria are two efforts underway to address issues with Common Criteria and product security evaluations by NIAP. A key recommendation by the Task Force report was to assemble a forum for an open discussion about reported issues and to work together to aggressively fix them. Completion of the NIAP Review is expected in September 2004. CSIA believes this is an opportune time to address both the Task Force report and the expected NIAP Review recommendations.

Without proactive action, Task Force and NIAP Review recommendations may not be seriously considered and those efforts will be wasted. CSIA, in conjunction with the National Cyber Security Partnership and other organizations, proposes to sponsor a Common Criteria Users' Forum meeting composed of customers, vendors, Common Criteria evaluators and NIAP (NSA and NIST). The first meeting of the Common Criteria Users Forum will be in October 2004 in the Washington, DC area. CSIA proposes four Actions & Recommendations for the Forum:

A/R 1: Discuss and develop practical means to improve the Common Criteria processes and standards. The goal is to make them viable tools to strengthen cyber security for all users.

A/R 2: Provide an open forum to express perspectives on Common Criteria evaluations, discuss and resolve the apparent differences between the views of the commercial entities and NIAP.

A/R 3: Develop specific timelines and individual actions on recommendations from the NIAP Review and the Task Force Report as well as any additional recommendations developed by the attendees.

A/R 4: Share Common Criteria experiences to educate ourselves and foster widespread, cost-efficient use of NIAP testing.

ABOUT CSIA

The Cyber Security Industry Alliance is an advocacy group to enhance cyber security through public policy initiatives, public sector partnerships, corporate outreach, academic programs, alignment behind emerging industry technology standards and public education. Launched in February 2004, the CSIA is the only public policy and advocacy group comprised exclusively of security software, hardware and service vendors that is addressing key cyber security issues. Members include BindView Corp. (NASDAQ: BVEW); Check Point Software Technologies Ltd. (NASDAQ: CHKP); Citadel Security Software Inc. (OTCBB: CDSS); Computer Associates International, Inc. (NYSE: CA); Entrust, Inc. (NASDAQ: ENTU); Internet Security Systems Inc. (NASDAQ: ISSX); NetScreen Technologies, Inc. (NASDAQ: NSCN); Network Associates, Inc. (NYSE: NET); PGP Corporation; Qualys, Inc.; RSA Security Inc. (NASDAQ: RSAS); Secure Computing Corporation (NASDAQ: SCUR) and Symantec Corporation (NASDAQ: SYMC)

Cyber Security Industry Alliance
1201 Pennsylvania Avenue, NW
Suite 300 #3011
Washington, DC 20004
202-204-0838