INFORMATION SECURITY AND PRIVACY ADVISORY BOARD

Established by the Computer Security Act of 1987
[Amended by the Federal Information Security Management Act of 2002]

The Honorable Rob Portman
Director
Office of Management and Budget
725 17th Street, N. W.
Washington, D.C. 20503

Dear Mr. Portman:

The Information Security and Privacy Advisory Board was established as a result of the Computer Security Act of 1987. The Board is charged to identify emerging managerial, technical, administrative, and physical safeguard issues relative to information security and privacy. The Board is to advise the National Institute of Standards and Technology (NIST), the Secretary of Commerce and the Director of the Office of Management and Budget (OMB) on information security and privacy issues pertaining to Federal government information systems. The Board is an advisory committee operating in accordance with the Federal Advisory Committee Management Act.

The Board has followed the progress of the National Information Assurance Program (NIAP)[1] review sponsored by DoD and DHS and conducted by the Institute for Defense Analysis (IDA) since its initiation in mid-2004 and has received several progress briefings on the review, most recently at its March 2006 meeting. While the final report of the review has still not been released, the March briefing gave the Board a clear sense of the direction that the review has taken. At its March meeting, the Board also received briefings on the Software Assurance efforts under way at DHS and NSA.

The process involved in these efforts is multifaceted. NIAP exists to conduct security evaluations of commercial IT security products and products that include security features, under the internationally recognized Common Criteria for IT Security Evaluation standards. Product vendors pay commercial laboratories to perform the evaluation work under the supervision of NIAP. NIAP was formed as a partnership of NIST and NSA, but the NIST role has diminished in the years since NIAP's founding, and today is limited to accreditation of commercial testing laboratories.

The NIAP review resulted from comments by IT vendors that evaluations were slow and costly,

[1] The National Information Assurance Program was formerly known as the National Information Assurance Partnership. The original partnership formed by agreement between NIST and NSA was intended to provide Federal agencies with a cost-effective, independent assessment of the security features of commercial information technology products.

and by IT users that evaluations were outdated by the time they were completed, and that they did not provide a true indication of products' security. Common Criteria evaluation (either by NIAP or by a Common Criteria authority from a country that participates in mutual recognition) of many IT products used in national security settings is required by NSTISSP-11, a policy of the Committee on National Security Systems.

A related set of efforts to improve product security is referred to by the term "software assurance." Software assurance focuses on improving the design, analysis, implementation, and testing of software with the aim of discovering and removing security vulnerabilities before the software is released to end users. NSA's newly formed Center for Assured Software and the Software Assurance program at DHS are the two major centers of US Government software assurance efforts.

Based on the briefings it has received, and on the independent understandings of the Board members, the Board finds that:

- While Common Criteria evaluation of IT products is only mandated for national security systems (under NSTISSP-11), civilian government agencies can in fact require more secure products; given the pervasiveness of evaluated products, the potential benefits of independent evaluation extend beyond national security systems.

- NIAP is serving a useful purpose by providing Federal agencies with an independent and objective characterization of the security features of commercial products. In addition, NIAP and the associated Common Criteria evaluation process benefit product vendors by the fact of international mutual recognition of evaluation results.

- While the characterization of product security features is useful, NIAP and Common Criteria fail to meet the need of IT users for a characterization of products' likely resistance to security attack. In particular, analysis of products' implementation – a key factor in assessing products' resistance to attack – is only undertaken at higher evaluation levels that are impractical for commercial products.

- Common Criteria as it exists today is only applied to packaged IT products; new forms of IT offerings such as web-based services and "software as a service" are out of the scope of NIAP and Common Criteria evaluations.

- Based on its understanding of the IDA review, the Board does not believe that the review addressed key issues with NIAP. While the review has correctly identified funding concerns, it is silent as to the benefits and deficiencies of the NIAP process such as the need to address resistance to attack and to consider new forms of IT services.

- There is little vendor or user input to the NIAP process or to the evolution of Common Criteria.

- There is an opportunity to integrate Federal efforts on software assurance into the product evaluation process. The Board found the NSA presentation on software assurance to be especially compelling; one of the shortcomings of the IDA review is its failure to raise the potential synergies between NIAP evaluation and software assurance.

- Given the issues with the current Common Criteria, it would not be appropriate at this time to extend the mandate for Common Criteria evaluations (NSTISSP-11) beyond national security applications. This finding is consistent with the findings of the recent GAO report on NIAP.

The Board recommends that:

- For the immediate term, NIAP should continue to perform Common Criteria evaluations under its existing processes; however, this should be viewed as an interim measure to provide continuity until improved processes can be devised.

- NSA, NIST, and DHS should devise an updated evaluation process that integrates considerations of software assurance and provides Federal IT users with more useful characterizations of real world IT product security. Such a process should focus on implementation as well as paper design, and on resistance to attack as well as richness of security features. The process should provide information that supports user agency certification and accreditation processes in meaningful ways.

- Any updated evaluation process should preserve international mutual recognition and should better reflect the input of IT users and vendors.

- The government should not extend the NSTISSP-11 mandate for the use of evaluated products beyond its current scope (national security systems) at the present time. The government should consider the extension of the mandate for the use of evaluated products to other Federal applications (beyond national security systems) only after developing an updated evaluation process that achieves demonstrable effectiveness at reducing products' susceptibility to attack.

Thank you for the opportunity to share our findings.

Sincerely,

Dan Chenok,
Chairman

Board Secretariat: National Institute of Standards and Technology
100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899-8930
Telephone: 301/975-2938 *** Fax: 301/975-4007