EXECUTIVE SUMMARY

About the Task Force

The Technical Standards and Common Criteria Task Force is an industry-led coalition of interested security experts from the public and private sectors created as part of the National Cyber Security Summit process. Task force members include representatives from trade associations, non-profit organizations, publicly traded and privately held companies, and state, local, and federal government employees. Task force members participated voluntarily, donated their time, and were not paid for their participation. The task force is not an advisory group to the Department of Homeland Security (DHS) or any other state, local or federal government department or agency. Instead, the task force operates under the guidance and coordination of the National Cyber Security Partnership, a coalition of trade associations, including the U.S Chamber of Commerce, the Information Technology Association of America, TechNet and the Business Software Alliance, that sponsored and organized the National Cyber Security Summit held in Santa Clara, California on December 2-3, 2003.

TASK FORCE MISSION

On December 3rd, 2003, the Technical Standards and Common Criteria Task Force was formed by members of academia, industry and government at the first National Cyber Security Summit in Santa Clara, CA. This task force, along with four others chartered that day by the National Cyber Security Partnership, was directed to identify gaps and develop recommendations to promote the adoption and implementation of the President's *National Strategy to Secure Cyberspace*. In the area of technical standards, the task force was directed to seek ideas on how to bring together and leverage expertise within the private and public sectors to develop new tools, technologies or practices that can reduce vulnerabilities at every level – from the Federal Government to large and small enterprises, and individual home users. In the specific area of Common Criteria (CC), the suggested focus was on developing recommendations to improve the CC evaluation process, as well as to explore alternative mechanisms, as it pertained to more effective industry usage and compliance and enhanced government guidance and support.

In addressing these critical areas, the task force adopted its formal mission statement: "To respond to current technical vulnerabilities and risks, analyze security requirements at industry-specific and general infrastructure-wide level, associate means to obtain assurance of correct and secure implementation and deployment, means for technical operational guidance (settings/configurations) and means for vulnerability and threat mitigation, including those for existing testing activities, such as the Common Criteria standard and the National Information Assurance Partnership (NIAP) testing program in support of the 'NIAP Review'."

Leadership

- Mary Ann Davidson, Oracle Corporation
- Chris Klaus, Internet Security Systems
- Edward Roback, National Institute of Standards and Technology (NIST)

Secretariat

- Jasmeet Ahuja, TechNet
- Leslie Saul Garvin, TechNet

CHALLENGE

To accomplish the goals set forth in its mission statement, the task force established five working groups, each focusing on a specific technical area or challenge as follows:

- The Common Configuration Working Group was focused on the challenge of responding to risks identified by the lack of common, baseline security capabilities, settings and documentation in all information technology (IT) infrastructure components and to develop and document recommendations for the collection and promotion of these common capabilities.

- The Research Working Group examined potential areas of research in furtherance of support of the CC, particularly in the area of product security verification.

- The Best Practices for Technical Standards Working Group was formed to review, assess, and amend, if necessary, existing checklists of recommended best technical cyber security practices. A specific focus was to compile existing sources of best practices, as failure to recognize the variety and specificity of best practice sources could lead to mistaken conclusions that government needed additional standards or that the CC process had to be used by default.

- The Equipment Deployment & Architecture Guidelines Working Group was formed to start addressing the challenge of the lack of guidelines for architecting secure Internet Protocol (IP) network infrastructures in which recommended security equipment and components are deployed.

- The Common Criteria, NIAP Review and Metrics Working Group was formed to develop recommendations for how to define better security metrics, develop a mechanism to express consensus-based requirements and to provide inputs to the NIAP Review.

RECOMMENDATIONS

In meeting the above challenges, the working groups identified current practices or related works in their respective areas of focus, described relevant gaps and issues facing individuals and organizations today, and developed white papers documenting dozens of actionable recommendations for improvement. A high-level summary of the task force's recommendations is presented below categorized by working group; the reader is referred to the specific working group white papers for the full list of recommendations and supporting discussions:

- The Common Configuration Working Group presents 28 recommendations in six core focus areas. The recommendations include a range of actions to encourage better security documentation and maintenance, to increase industry and government coordination and collaboration, and to promote development and management of more secure product configurations by default and in deployment. The recommendations are primarily aimed at the vendor community. At the same time, it is recognized that the United States (U.S.) Government, as well as user groups and consumers, play a major role in the development and implementation of these recommended practices. Where applicable, specific incentives or entity-specific initiatives are endorsed. For example, in the area of coordination of security recommendations, the working group recommends government promotion of the use of the NIST central repository for IT security configuration checklists already under development.

- The Research Working Group recommends focused action in the area of software vulnerability analysis research. Specifically, the working group recommends that the U.S. Government fund research into the development of better vulnerability analysis or "code scanning" tools that can identify software defects. The working group also recommends that the U.S. Government require vulnerability analysis of products, either by moving vulnerability analysis to lower assurance levels or as a condition of procurement. Accordingly, the working group recommends removal of the requirement for medium or higher assurance evaluations (Evaluation Assurance Level 4+ [EAL4+]) for commercial products, since the stated purpose for these by U.S. Government proponents is the vulnerability analysis required at higher assurance.

- The Best Practices for Technical Standards Working Group presents a compilation of existing guidance in several areas, including information security management models (both control- and principles-based), product security models, board government guidelines, sector-specific and general management guidelines, risk management models, guides for home and individual users, and configuration/patching guides. The working group notes that there are significant sources of guidance and direction on how to improve cyber security, and while the compilation is thorough, it is not considered exhaustive; additional sources can and should be easily added to the various lists. The compilation is offered to minimize the risk of duplicative or unnecessary private sector work, to avoid presumptions that additional government standards might be necessary to fill the "void," and to dispel a belief that the CC process has to be used by default.

- The Equipment Deployment & Architecture Guidelines Working Group focuses on the following two generalized recommendations, with appropriate additional sub-recommendations also defined. First, the working group recommends that industry work together to develop a set of defined security standards for using recommended security equipment as well as a set of best practices for designing and implementing secured IP network infrastructures. Second, it is recommended that industry work together to develop a defined set of standards for determining the security level or security status of cyberspace.

- The Common Criteria, NIAP Review and Metrics Working Group proposes 35 recommendations in six core focus areas: 1) Increase the NIAP Evaluation Scheme effectiveness; 2) Make government Commercial Off-the-Shelf (COTS) procurement policies realistic; 3) Reduce the costs of CC evaluations; 4) Increase the demand for CC-evaluated products; 5) Improve the use and utility of Protection Profiles (PP); and 6) Increase product security through CC specifications and evaluation. In each focus area, the working group discusses the current landscape, and provides specific findings and recommendations targeted for both government and private sector action. These recommendations are intended to address the current issues with CC and to make it a viable, value-added process towards improving the security of the products within our information infrastructure. Over half of the recommendations offer specific direction with respect to the Administration's ongoing NIAP Review process, and other recommendations propose specific government incentives, encouragement, or support to increase CC effectiveness. For example, the working group recommends that NIST receive new appropriations (in the amount of $12 million upfront and $6 million per year thereafter) for the purposes of developing non-classified PPs (i.e., consensus security requirements for specific product classes, like intrusion detection systems and virtual private networks) and developing best practices and methodologies to enable labs to evaluate products against these PPs.

The guidelines and recommendations presented in this report are the result of extensive discussions and vigorous debate among the task force participants and are offered with the intention of moving all stakeholders in the direction toward a more secure information infrastructure. The task force recognizes that while unanimity was not always achieved on each recommendation, indeed, dissenting views were occasionally aired, a policy of including consensus language in this report was appropriate to engage the broader community in the discussion and to solicit wider public comment. Accordingly, the presentation of any recommendation does not imply unanimous agreement by the participants. Recommendations should not be attributed to, or assumed to be accepted by, any particular industry, association, or academic segment, or any particular member of the task force.

NEXT STEPS

The Technical Standards and Common Criteria Task Force solicits public comment and input from private and public sector stakeholders on its recommendations as set forth in the task force report. Reviewers are asked to consider the recommendations as posed, as well as to provide specific suggestions regarding effective adoption and implementation. Comments on this report should be sent to Leslie Saul Garvin – lsaul@technet.org.

The task force plans to:

- Provide its "Inputs to the NIAP Process" recommendations directly to government representatives (i.e., Department of Defense [DOD], National Security Agency [NSA], DHS) for consideration and incorporation.

- Provide its "Equipment Deployment & Architecture Guidelines" paper to NIST and other appropriate standards organizations for peer review and further development.

- Review the other National Cyber Security Partnership Task Force reports and coordinate as necessary to identify further opportunities for collaboration and potential overlaps in effort.

- Schedule a follow-up session to review and incorporate feedback as appropriate.

- Track select recommendations in conjunction with the secretariat, and convene ad hoc meetings on selected topics as needed in furtherance of task force objectives.

CONCLUSIONS

In four months, the task force has moved forward from its initial meeting in December at the National Cyber Security Summit to develop significant recommendations that successfully address key components in the President's *National Strategy to Secure Cyberspace*. The task force members look forward to their review by the summit sponsors and stand ready to assist in next steps as needed. Additionally, the task force recognizes that industry and government must continue a proactive approach to addressing the evolving and accelerating challenges of securing cyber space. This is particularly true in the area of technical standards/Common Criteria. The task force recognizes that it will take time to fully implement solutions like those proposed, and the need for continued engagement on the part of industry, academia, and government.