National Cyber Security Partnership

Technical Standards and Common Criteria Task Force

RECOMMENDATIONS REPORT

April 2004

TABLE OF CONTENTS

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.

1.0 INTRODUCTION

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.

1.1 Task Force Mission

In addressing the critical areas of technical standards and CC, 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 CC standard and the National Information Assurance Partnership (NIAP) testing program in support of the 'NIAP Review'."

Task Force Co-Chairs:

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

Task Force Secretariat:

- Jasmeet Ahuja and Leslie Saul Garvin, TechNet

1.2 Approach

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. The working groups and individuals designated as champions to drive working group activities are 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.
  Champion: Glenn Brunette, Sun Microsystems, Inc.

- The Research Working Group examined potential areas of research in furtherance of support of the CC, particularly in the area of product security verification.
  Champion: Mary Ann Davidson, Oracle Corporation

- 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.
  Champion: Bruce Heiman, Business Software Alliance

- 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.
  Champion: Victor Rychlicki, Marconi Wireless

- 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.
  Champion: Wes Higaki, Symantec Corporation

1.3 Organization of Report

The remainder of this report is divided into the following sections:

- **Section 2.0 Recommendation Highlights** presents a high-level summary of the task force's recommendations categorized by working group. The reader is referred to the specific working group reports attached in the appendices for the full list of recommendations and supporting discussions.

- **Section 3.0 Conclusions** presents some concluding remarks and task force next steps.

- **Section 4.0 Acknowledgements** presents a list of task force participants and additional recognition from the task force Co-Chairs.

- **Appendix A** presents the Common Configuration Working Group Recommendations Report.

- **Appendix B** presents the Research Working Group Recommendations Report.

- **Appendix C** presents the Best Practices for Technical Standards Working Group Recommendations Report.

- **Appendix D** presents the Equipment Deployment & Architecture Guidelines Working Group Recommendations Report.

- **Appendix E** presents the Common Criteria, NIAP Review and Metrics Working Group Recommendations Report.

2.0 RECOMMENDATION HIGHLIGHTS

To address the specific focus areas or challenges, 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 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 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.

2.1 Common Configuration Recommendations

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. Selected high priority recommendations are as follows:

Recommendation: Vendors should provide stronger out-of-the-box security configurations and/or provide supported capabilities and tools that simplify and automate the process of securing their products.

While strong out-of-the-box security configurations are preferred, it is recognized that updating existing products to comply with this requirement can be costly, time-consuming and can result in various incompatibilities with current and supported versions of the product. As a result, it may not be possible for a vendor to transition a product to a more secure out-of-the-box state for several years, depending on product release cycles. To mitigate this gap, vendors are strongly encouraged to include software tools, scripts, or wizards to guide users through the process of securing their product post-installation.

Ideally, these tools would leverage vendor-provided, peer-reviewed or consensus-based security recommendations while also allowing users to configure the product to meet their specific security requirements and needs. These tools should always default to a secure setting.

Recommendation: Vendors should provide more substantive security recommendations, configuration checklists, best practices, assumptions, dependencies, and considerations in their product documentation. Vendors are generally in the best position to provide much of this information. Vendors should leverage feedback from user groups and government organizations to improve their security documentation based on actual deployment and usage.

Recommendation: The U.S. Government as well as user groups and consumers should encourage independent evaluation and/or certification of security management products. Users must have confidence in the tools they choose to deploy in their environments. It is important that these tools not only work as advertised, but they must also not be responsible for introducing new vulnerabilities or undocumented risks into the user's environment.

Recommendation: Vendors, user groups, consumers and the U.S. Government should work with NIST to develop standards and requirements for checklists, baseline policies for specific environments, and peer-reviewed or consensus-based checklists. Checklists, submitted by vendors, user groups and other organizations could be used as input for the creation of consensus-based checklists. NIST can serve as a neutral third-party to industry and facilitate the coordination between vendors, agencies, academia, industry, and other organizations such as consortia. Vendors should consider certification of their products against these checklists, to ensure that products configured per the checklists do not break other products that depend on them.

The complete list of working group recommendations is presented in **Appendix A**.

2.2 Research Recommendations

The Research Working Group recommends focused action in the area of software vulnerability analysis research. Specific recommendations include:

Recommendation: The U.S. Government should fund research into better code scanning tools that will help software development companies (both large and small) weed out more defects in software.

Recommendation: The CC can be amended to require vulnerability analysis at lower assurance levels (by a third party validating that a vendor does code scanning during development and remediates significant faults accordingly, or by the evaluation lab rerunning the scan separately). Alternatively, the U.S. Government can require vulnerability analysis by vendors, as a separate condition of procurement, if requiring vulnerability analysis at lower assurance levels is not accepted as a change to the CC.

Recommendation: In conjunction with the above recommendations, the requirement for medium or higher assurance evaluations (Evaluation Assurance Level 4+ [EAL4+]) for commercial products should be dropped, since the stated reason for higher assurance evaluations by the proponents is the ability to do vulnerability analysis. Higher assurance evaluations for commercial software impose a cost burden that even the largest IT vendors cannot bear or should not bear; they do not substantially improve product security, but may result in vendors paying multiple times for the same evaluation in different markets. Furthermore, finding faults in software that has already shipped is far more expensive and less effective than giving vendors the tools to be used during the development process.

The working group recommendations and supporting discussions are presented in **Appendix B**.

2.3 Best Practices for Technical Standards Recommendations

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 working group compilation is presented in **Appendix C**.

2.4 Equipment Deployment & Architecture Guidelines Recommendations

The Equipment Deployment & Architecture Guidelines Working Group focuses on the following two generalized recommendations, with appropriate additional sub-recommendations also defined:

Recommendation: It is recommended that the industry work together to develop a set of defined standards for using recommended security equipment, as well as best practices for understanding, designing and implementing secured IP network infrastructures.

Recommendation: It is recommended that the industry work together to develop a defined set of standards for determining the security level, or security status, of cyberspace.

Specific working group recommendations and supporting reference material are presented in **Appendix D**.

2.5 Common Criteria, NIAP Review and Metrics Recommendations

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)
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. Sample recommendations in the six focus areas include:

Recommendation: Provide greater funding to NIST so that they can return to represent the interests of the majority of the U.S. Some efforts are underway by individual companies and some industry organizations, and progress towards actual funding should be checked in September. NIST should receive new appropriations in the amount of $12 million upfront and $6 million per year thereafter for the purposes of developing non-classified PPs and developing best practices and methodologies to enable labs to evaluate products against these PPs.

Recommendation: Experienced vendors, consultants, evaluation labs and NIAP should provide greater security education and training to the Department of Defense (DOD) and other agencies to help them understand the role CC evaluations play in improving the security of their information infrastructure.

Recommendation: In order to promote the evaluation of more products, the U.S. Government should help offset the expenses of CC evaluation through research and development tax credits or paying part of the evaluation costs.

Recommendation: Vendors and NIAP must engage in increasing the recognition of CC into markets both vertically and horizontally in order to amortize evaluation costs and effort across a broader customer base.

Recommendation: NIST, customers, vendors and CC consultants and/or evaluators should develop consortia to develop and vet PPs. The coalition of all of these parties will ensure that the requirements are realistic and that the appropriate technologies can be delivered to address the needs. The requirements and vetting models used by organizations such as ICSA should be examined. The status of this activity should be checked in September.

Recommendation: Vendors need more reliable education and training on how to conduct effective CC evaluations. Moreover, vendors need to gain greater awareness of the impact CC evaluations can have on improving their organizational processes. NIAP and DHS can serve as a clearinghouse of information about reliable education, training and consulting resources.

The complete list of working group recommendations and supporting rationale are presented in **Appendix E**.

3.0 CONCLUSIONS

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., 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.

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.

4.0 ACKNOWLEDGEMENTS

The task force Co-Chairs wish to thank the task force members for their time and contributions to the critical work of the task force, particularly the leadership of the working group champions. Additionally, the Co-Chairs thank Jasmeet Ahuja and Leslie Saul Garvin of TechNet for their significant contributions to the task force report.

The following is an alphabetical list of those people who participated in or contributed to the task force working group initiatives and the development and review of this report.

Name	***Organization***
Brian Andersen	Phoenix Technologies, Ltd.
Jim Arnold	SAIC
Dave Aucsmith	Microsoft Corporation
John Banghart	Center for Internet Security
Chris Benjes	National Security Agency
Sandy Bird	Q1labs Inc.
Joel Birnbaum	Hewlett-Packard Company
Scott Blanchette	Stanford University Medical Center
Larry Bridwell	ICSA Labs
Glenn Brunette (Working Group Champion)	Sun Microsystems, Inc.
Richard Caliari	Harris Corporation
Diann Carpenter	Cable and Wireless
Denise Cater	Syntegra
Uma Chandrashekhar	Lucent Technologies
Victor Chang	RSA Security
Edward Coleman	Department of Homeland Security
Larry Coleman	Department of the Navy
Ruth Cowell	Department of Defense
Mary Ann Davidson (Task Force Co-Chair)	Oracle Corporation
Matthew Deane	American National Standards Institute
Lawrence Dobranski	Nortel Networks
Murray Donaldson	Decisive Analytics Corporation
Daryl Eckard	EDS
Jeremy Epstein	WebMethods
Liesyl Franz	EDS
Tim Grance	National Institute of Standards and Technology
Theresa Grant	The Dow Chemical Company
Elizabeth Grossman	House of Representatives, Science Committee
Eric Guerrino	Bank of New York
Tim Hackman	IBM
Duncan Harris	Oracle Corporation
Bruce Heiman (Working Group Champion)	Business Software Alliance
Brian Henderson	National Security Agency
Wesley Higaki (Working Group Champion)	Symantec Corporation
Paul Hoffman	VPN Consortium
Robert Hoffman	Oracle Corporation
Richard Holmes	Union Pacific Corporation
Katie Ignaszewski	Internet Security Systems
Wendi Ittah	Check Point Software Technologies
Greg Jackson	DeepNines Technologies
Matt Keller	Corsec Security
Chris Klaus (Task Force Co-Chair)	Internet Security Systems
Ron Knode	Computer Sciences Corporation (CSC)
Ray Komar	Preventsys
Clint Kreitner	Center for Internet Security

John LaCour	Zone Labs, Inc.
John Lainhart	IBM Consulting Services
Shaun Lee	Oracle Corporation
John Linton	SecureInfo Corporation
Steve Macke	Georgia Tech Research Institute
Richard Marshall	National Security Agency/LAO
Ron Mathis	Intrado Inc.
Sheila McCoy	Department of the Navy
Lynn McNulty	(ISC)2
Stephen Meer	Intrado Inc.
Simon Milford	Logica
Alex Noordergraaf	Sun Microsystems, Inc.
James Norris	Sprint
Will Ozier	ISSA GAISP Executive Committee
Andy Palan	Accenture National Security Services
Ann Patterson	BITS
Joseph Petragnani	St. Joseph's University
Judy Petsch	Department of the Navy
Hal Pomeranz	Deer Run Associates
Ray Potter	Cisco Systems
Frank Reeder	Center for Internet Security
Edward Roback (Task Force Co-Chair)	National Institute of Standards and Technology
Victor Rychlicki (Working Group Champion)	Marconi Wireless
Doug Sabo	Network Associates
Ted Schlein	Kleiner Perkins Caufield & Byers
Marty Schulman	Juniper Networks
Mark Selfon	Marconi Wireless
Ray Snouffer	National Institute of Standards and Technology
Jack Suess	University of Maryland, Baltimore County
Murugiah Souppaya	National Institute of Standards and Technology
Rati Thanawala	Lucent Techologies
John Wack	National Institute of Standards and Technology
Rod Wallace	Nortel Networks
Catherine Webb	IBM
William Wilson	Carnegie Mellon University – US CERT
Paul Zatychec	EWA-Canada

Appendix A

National Cyber Security Partnership
Technical Standards and Common Criteria Task Force

Common Configuration Working Group
RECOMMENDATIONS REPORT

April 19, 2004

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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 in conjunction with the U.S. Department of Homeland Security (DHS), was directed to identify gaps and develop recommendations to promote the adoption and implementation of the President's *National Strategy to Secure Cyberspace*. These recommendations will be presented to the DHS and other stakeholders for consideration in planning next steps.

WORKING GROUP MISSION STATEMENT

To accomplish its goals, the Technical Standards and Common Criteria Task Force established five working groups, each focusing on a specific technical area or challenge. As set forth in its mission statement, the Common Configuration Working Group was established to "respond to the 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."

RECOMMENDATIONS

The Common Configuration Working Group presents 28 recommendations in six core focus areas. The recommendations include a range of actions to encourage better security recommendation 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 U.S. Government, as well as user groups, consumers and the vendor community. Where applicable, specific incentives or entity-specific initiatives are endorsed. Selected high priority recommendations are as follows:

Recommendation: Vendors should provide stronger out-of-the-box security configurations and/or provide supported capabilities and tools that simplify and automate the process of securing their products.

While strong out-of-the-box security configurations are preferred, it is recognized that updating existing products to comply with this requirement can be costly, time-consuming and can result in various incompatibilities with current and supported versions of the product. As a result, it may not be possible for a vendor to transition a product to a more secure out-of-the-box state for several years, depending on product release cycles. To mitigate this gap, vendors are strongly encouraged to include software tools, scripts, or wizards to guide users through the process of securing their product post-installation.

Ideally, these tools would leverage vendor-provided, peer-reviewed or consensus-based security recommendations while also allowing users to configure the product to meet their specific security requirements and needs. These tools should always default to a secure setting.

Recommendation: Vendors should provide more substantive security recommendations, configuration checklists, best practices, assumptions, dependencies, and considerations in their product documentation. Vendors are generally in the best position to provide much of this information. Vendors should leverage feedback from user groups and government organizations to improve their security documentation based on actual deployment and usage.

Recommendation: The U.S. Government as well as user groups and consumers should encourage independent evaluation and/or certification of security management products. Users must have confidence in the tools they choose to deploy in their environments. It is important that these tools not only work as advertised, but they must also not be responsible for introducing new vulnerabilities or undocumented risks into the user's environment.

Recommendation: Vendors, user groups, consumers and the U.S. Government should work with the National Institute of Standards and Technology (NIST) to develop standards and requirements for checklists, baseline policies for specific environments, and peer-reviewed or consensus-based checklists. Checklists, submitted by vendors, user groups and other organizations could be used as input for the creation of consensus-based

checklists. NIST can serve as a neutral third-party to industry and facilitate the coordination between vendors, agencies, academia, industry, and other organizations such as consortia. Vendors should consider certification of their products against these checklists, to ensure that products configured per the checklists do not break other products that depend on them.

1.0 TASK FORCE 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 National Information Assurance Partnership (NIAP) testing program in support of the "NIAP review."

2.0 WORKING GROUP MISSION STATEMENT

To respond to the 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.

3.0 INTRODUCTION

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 in conjunction with the U.S. Department of Homeland Security (DHS) was directed to identify gaps and develop recommendations to promote the adoption and implementation of the President's *National Strategy to Secure Cyberspace*. These recommendations will be presented to the DHS and other stakeholders for consideration in planning next steps.

To accomplish the goals set forth in its Mission Statement, included in Section 1 above, the Technical Standards and Common Criteria Task Force divided its work among six working groups, each focusing on a specific technical area. Each working group was asked to:

1. Identify the current practice and any related works in their respective area of focus;
2. Describe the gaps and challenges facing individuals and organizations today; and
3. Develop actionable recommendations for improvement.

The working groups created by this Task Force include:

- WG1 – Common Configuration
- WG2 – Research
- WG3 – Inventory Awareness Materials[1]
- WG4 –Best Practices for Technical Standards
- WG5 – Equipment Deployment & Architecture Guidelines
- WG6 – Common Criteria, NIAP Review and Metrics

This report focuses on the current practice, gaps and recommendations developed by Working Group 1 (WG1) - Common Configurations. This material is limited in scope based on the Mission Statement included above in Section 2.

4.0 PROBLEM STATEMENT

The current state of security in cyberspace is one of inconsistency and confusion. Few products clearly document their out-of-the-box security configuration and assumptions, supported security capabilities, recommended practices for using and managing the product in a secure manner, or even how to maintain the security of the product over its lifecycle. Further, many products fail to clearly document their security assumptions and feature dependencies thereby making it more difficult for users to configure the product to meet their specific security policies and requirements. Finally, those products with security capabilities frequently do not perform sufficient integration and

[1] The Inventory Awareness Materials Working Group was integrated into the Common Criteria, NIAP Review and Metrics Working Group.

interoperability testing to ensure that their capabilities are actually deployable in customer environments, including large enterprises with heterogeneous computing environments.

For organizations, both large and small, this lack of information presents numerous problems when deploying and maintaining products in their environment. This problem is amplified when products must be integrated together to address a specific need. Without sufficient documentation describing the assumptions, interdependencies and capabilities of these products when assembled together, the task of deploying and maintaining products in a secured configuration is made significantly more difficult.

The lack of strong security documentation has led many user communities as well as industry and government organizations to develop their own set of product-specific security recommendations. While on the whole, the development of such efforts should be encouraged, the lack of oversight, vendor cooperation and peer review of such efforts has led to the development and dissemination of incomplete and even incorrect or unsupportable recommendations that often do more harm than good. By leveraging a coordinated mechanism, however, where all interested parties can actively participate and collaborate, better product configurations and recommendations can be achieved[2]. Frameworks such as the recent standard ITU-T X.805 *Security architecture for systems providing end-to-end communications [X.805]* help identify the minimum security requirements that need to be fulfilled.

Frequently, these initial sets of recommendations are neither maintained nor supported as products are updated, corrected or enhanced. An interesting property of cyberspace is that any information posted is propagated and kept accessible long after its utility has ended. Security configuration recommendations are no exception. The result is that recommendations that were once appropriate may no longer be so, and users implementing outdated recommendations can be left with unsupported or unstable product configurations. Worse still, these obsolete recommendations may fail to fully address new risks or threats associated with the updated product leaving an organization unwittingly at risk of compromise.

All of this makes the assumption that users can actually find complete, factual and well-tested product security recommendations in the first place. Often such recommendations are scattered throughout cyberspace on individuals' web sites as well as those maintained by user groups, vendors or government organizations. Within the government sector, organizations such as the National Institute of Standards and Technology (NIST), the National Security Agency (NSA) and the Defense Information Systems Agency (DISA) serve as clearinghouses for security recommendations such as these. Outside of that sector, no one site is widely accepted, although both NIST and the Center for Internet Security (CIS) are often used in this capacity. This problem is compounded by the fact that any two recommendations or “best practices” authored by different groups may not even be in agreement with one another (even when both are addressing similar threats and levels of risk). This only serves to confuse and create additional work for users who must then try to identify the proper course of action in light of conflicting information.

The goal of this report is to discuss each of these problems in more detail and provide recommendations that if implemented, will serve to significantly improve the current situation.

5.0 FINDINGS AND RECOMMENDATIONS

The findings and recommendations are divided into six core focus areas with the intent to divide the problem space into more manageable sections. Each focus area, discussed in more detail below, will include a brief overview along with a set of recommendations for improvement as well as a list of related works (if applicable). The focus areas covered by this report are:

- Documented Security Recommendations
- Collaboration on Security Recommendations

[2] This is very similar in concept to the Adverse Event Reporting System (AERS) developed by the Food and Drug Administration (FDA). By allowing health care professionals and consumers to report possible adverse reactions, patients’ lives can be better protected. Similarly, by disclosing adverse reactions resulting from the use of security recommendations, individuals and organizations will be better armed to more securely deploy, integrate and manage products in their environment. Last, vendors collaborating with such a service could leverage this information to improve their products and make them easier to secure in light of how they are actually being used. See: http://www.fda.gov/cider/ears/

- Coordination of Security Recommendations
- Secure by Default
- Secure in Deployment
- Management of Secured Configurations

5.1 Documented Security Recommendations

5.1.1 Current Landscape

Most products available to consumers today do not provide any guidance as to what their potential security exposures are or how they should be securely configured and maintained. As a result, users are left unaware of the risks posed by the use of the product or how such risks can be mitigated through product configuration or integration. Further, the lack of security recommendations and practical guidance limits the ability of users to configure and use the product in accordance with their security policies, requirements and levels of risk.

Reference manuals for products with configurable security parameters generally discuss valid parameter values as well as methods for enabling or modifying those settings. While this is certainly useful and necessary, it is not sufficient. Such documentation rarely describes the context associated with the parameters. For example, answers to questions such as "when should this parameter be used?", "what values should be used to achieve a desired level of security?", "how should I know if this parameter applies to my environment?" and "what are the benefits and risks associated with changing this parameter from its default value?" are rarely answered.

This complexity is forced on the user of the product who must seek out answers to each of these questions before embarking on the product's initial configuration and deployment. Typically, this task must be repeated as products are upgraded or patched. Considering all of the products available today in most organizations, it becomes apparent that this is no trivial effort. Therefore, it is understandable why many organizations simply accept product defaults, never bothering to tune those products for added security. Frequently, this is the result of a risk assessment that concludes that the cost of a particular security failure will be less then the ongoing effort to exhaustively evaluate product security features and capabilities.

While basic documentation may suffice for simple products that have a very limited set of user configurable options, most products are quite complex and offer a rich set of configurable options that allow individual organizations to tune a product to meet specific requirements. Certainly, while such high degrees of flexibility can be useful, the inherent complexity often associated with this freedom overshadows the benefits, especially when it makes the resulting product configuration difficult to understand, set or maintain.

Lastly, most security recommendations available today do not take into account the intended use of the product or the environment into which the product will be placed even though the threats to the product (and ultimately to the organization deploying it) will vary depending on these and other factors. A product deployed on a network connected to the Internet may require more security than the same product deployed in a closed lab. Failure to take into account variables such as these can often leave the security recommendations applicable to only certain classes of environments. Today, very few documented security recommendations address changes or settings that may be applicable only to specific risk profiles.

It should be noted here that the intended use of a product is difficult for a vendor to predict and therefore the testing of all potential deployment scenarios is often not only difficult but also cost prohibitive. This problem could be addressed by the development of a baseline set of security policies and real-world deployment scenarios. Such policies would provide vendors with a known baseline against which they can design, build and test their products. Further, such baseline policies could help those developing security recommendations to better tailor their recommendations to specific environments.

5.1.2 Ongoing and Related Work

A small, but growing number of vendors, user groups and government organizations have published both general and product specific security recommendations. While the majority of these published documents focus on operating systems and related frameworks, the number of other product-specific security recommendations is also

growing. In general, the security recommendations, practices, checklists and related material available today can be characterized by a number of factors such as:

- Target audience
- Target baseline environment
- Interaction with other guides and applications
- Level of review (individual, peer review, consensus)
- Level of detail (step-by-step, introductory, detailed, reference)
- Availability (freely available, for fee, restricted to a group)

Examples of such security recommendations include, but are not limited to the following.

Organization	***Title of Security Recommendations (Focus Areas)***
Center for Internet Security	Security Benchmarks
CERT Coordination Center	Security Practices
Defense Information Systems Agency	Security Technical Implementation Guides (STIGs)
Hewlett-Packard Company	Security Whitepapers
IBM	Redbook Security Supplements
Information Security Forum	Various Security Practices, Recommendations and Checklists
Microsoft Corporation	Authoritative Security Guidance for the Enterprise
National Institute of Standards and Technology	Federal Information Processing Standards (FIPS) and Special Publications, NIST Recommendations and Security Checklists
National Security Agency	Security Recommendation Guides
Oracle Corporation	Oracle Security Guide
SANS Institute	Step-by-Step Security Guides
Sun Microsystems, Inc.	Sun Security BluePrints

5.1.3 Gaps and Recommendations

Given the sheer number of products deployed in today's environments, it is disconcerting that only a small number of those products provide specific security recommendations and guidance to aid users in safely deploying the products in their environments. While a great deal of work has been done in this area over the last few years, there is still much to do. Arming users with information that they need to successfully and securely configure, deploy, and integrate products in their environment is critical.

Recommendation: Vendors, user groups, and government organizations should take a more proactive role in the development of and collaboration on product security recommendations. The U.S. Government can play an important role by encouraging such collaboration.

Recommendation: Vendors should perform more realistic functional and security testing of their products in real-world situations. All too often, product testing is done in a lab setting that almost never reflects how the products will actually be deployed in a user's environment. The results from this testing can be used to determine what security features and capabilities may be missing that should be added to the product. This information is also useful for the development of product security recommendations. The U.S. Government as well as user groups and consumers should actively participate in this testing by contributing their use cases, usage and deployment considerations and other feedback.

Recommendation: Vendors should provide more substantive security recommendations, configuration checklists, best practices, assumptions, dependencies, and considerations in their product documentation. Vendors are generally in the best position to provide much of this information. Vendors should leverage feedback from user groups and government organizations to improve their security documentation based on actual deployment and usage.

Recommendation: Vendors should work with their independent software and hardware vendors (ISVs and IHVs) and original equipment manufacturers (OEMs) to better certify common security configurations impacting a set of products rather than developing secured configurations in isolation. This includes documenting any shared assumptions, dependencies or requirements. As a result of this collaboration, vendors may be able to participate in logo or certification programs.

Recommendation: The U.S. Government should encourage organizations to develop security recommendations that apply to one or more specific risk profiles. Recognizing that security is a spectrum and not an absolute, it is both appropriate and necessary to provide common set of recommendations based on a selection of pre-defined thresholds for risk. Similarly, encourage organizations to develop baseline security recommendations (if applicable) that apply to various user communities or environments. These could serve as the foundation for more comprehensive sets of recommendations that may apply only to specific risk profiles or product combinations.

To support this recommendation, risk profiles and security objectives such as those defined by the FIPS 199 publication [FIPS199] should be better promoted to academia and industry in addition to government for the purpose of building baseline recommendations and consensus. Such agreement, if achieved, would help promote the development and collaboration of security recommendations based on such models. In addition, the NIST draft publication titled "Security Checklists for IT Products" [SCIP] provides additional examples that highlight a baseline set of environments for which security recommendations could written. Note that FIPS 199 was developed in response to tasking to NIST under the Federal Information Security Management Act of 2002 [FISMA].

5.2 Collaboration on Security Recommendations

5.2.1 Current Landscape

The development of strong security recommendations requires a solid understanding of the product in question, its security capabilities and a good understanding of security principles, attack methods, scenarios and countermeasures. While these may provide a good starting point, these items alone are not sufficient. The intended and actual uses of the product must also be considered. Many times, assumptions made during product development do not hold true when the product is actually deployed and used. As a result, it is important to also consider environments into which the product will be deployed.

Products are not typically used alone. They either require or are used in conjunction with other products to solve more complex problems. So, it is clear that product interdependencies must also be addressed. Failure to understand these interrelationships can cause recommendations to become ineffective, incomplete, or even invalid.

Today, very few product-specific security recommendations are developed using a consensus-based[3] approach with input from the vendor, user groups and government organizations. All too often, security recommendations are published either solely by the vendor or organization who developed the product or by individuals, user groups or other bodies who deploy the product in their environments. While this is not necessarily a problem, the collaboration between these types of groups is very often insufficient and even adversarial in some cases where user communities are working in the same area. This can lead to a variety of problems, such as:

- Unilateral Recommendations. Information that comes from just one source, such as from a product vendor, is many times considered inadequate, even if the information presented is correct. It is human nature to seek confirmation from an unbiased party before accepting information as fact. This speaks not to the quality of the recommendations presented but more toward users inclination to want independent

[3] It must be noted that developing consensus can be both a time and resource intensive process. As a result, there is often a considerable delay between when a product is made available and when consensus-based recommendations are finalized. The longer the delay, the greater the likelihood poorly configured products will be deployed in operational environments.

confirmation of the appropriateness or effectiveness of security recommendations made by a vendor or other party[4]. This is true even in cases where the vendor may be the best party equipped to provide such recommendations. As a result, user communities gravitate towards recommendations that are independent, peer-reviewed, vetted or consensus-based in some way. This can be a very good practice as long as those recommendations developed independently or by consensus do not suffer from the other problems listed below.

- Impractical Recommendations. These recommendations are often the result of solutions developed that while technically correct can never be practically deployed in an actual user environments due to complexity, time, cost or other factors. Such recommendations may also take the form of abstract statements that provide no practical instructions or examples to assist the user in implementing them. Recommendations such as these often were developed without feedback from those user groups who would be most impacted by the recommendation.

- Incomplete Recommendations. These recommendations fail to completely solve the problem, solve the problem but only for limited use cases, or solve the problem in a less elegant or appropriate way. Recommendations such as these can leave the user with a false sense of security if the user is not made aware of the assumptions. Further, these recommendations can prove dangerous if harmful interactions are not clearly understood or documented. Lastly, as products improve, it is important that any recommendations take advantage of new capabilities and/or methods to solve problems. Incomplete recommendations often stem from the development of recommendations without vendor involvement. All too often, an individual or small group's experience with the product is published as recommended or "best" practice without vetting from larger or more diverse user communities and just as important without feedback from the product vendor.

- Outdated Recommendations. Security recommendations tend to linger. In one such example[5], a myth regarding a security configuration recommendation has continued to propagate on the Internet for over four years. The recommendation in question is completely ineffective and was corrected in a later update to the original article, yet the outdated information continues to be included in new publications. Conflicting recommendations such as those created when comparing recommendations that are obsolete serves to propagate myths and confusion among users of the product. In this specific example, a failure to adequately test the recommendations prior to publication was the culprit. Regardless, better cooperation between the product vendor and groups developing security recommendations would have certainly helped prevent outdated information from being published in the first place. Better coordination with sites that cache or mirror such information is also needed to help limit the availability of outdated security recommendations.

- Unsupportable Configurations. Another problem arising from current practice is the creation and dissemination of recommendations that render product configurations unsupportable by the vendor. While there may be valid reasons for the use of such recommendations, failure to declare that a vendor will not support the recommendations is absolutely critical information for users who may want to leverage them. Many users take published security recommendations as fact and do not question their correctness or appropriateness. Often, these same users do not consider the ramifications that the security recommendations will have on the supportability, performance, reliability, or availability of the product or related products. It is all the more critical then to ensure that security configuration recommendations are as supportable as possible.

  Recommendations that do not meet this goal have typically been developed without feedback from the vendor who could have pointed out potential problem areas, identified more supportable solutions and even provided feedback to help document the impact of the recommendations on their products. As an aside, by

[4] This is the basis for the Common Criteria. Vendors must provide evidence of their security claims that are evaluated according to specific rules by an independent party who is responsible for certifying the results. The results of such an evaluation can then be accepted by other organizations, and in the case of Common Criteria, other countries.

[5] Several documents, some dating back to 1999, refer to the Sun Solaris Operating Environment parameter sys:coredumpsize in the file /etc./system. This parameter never actually existed in any release of that operating system, yet its use continues to this day to be referenced in newly published security recommendation material and tools by user groups and other organizations.

highlighting security concerns in this manner, a vendor can develop a greater understanding of customer requirements and would therefore be in a better position to address those requirements in a future update of the product.

It is clear that no one vendor or user community has all of the answers, knowledge or experience to develop comprehensive security recommendations. In fact, for the majority of products available today, no security recommendations exist. For the material that does exist, much of what is widely available suffers from one of the problems listed above. It is only through a collaborative partnership, combining feedback from vendors, user groups and other parties, that strong, comprehensive and supportable security recommendations can be developed and maintained.

5.2.2 Ongoing and Related Work

There are a number of individual organizations and vendors working on the development of security recommendations. These organizations are typically comprised of one or a small set of user communities. As a result, the recommendations stemming from these organizations can sometimes suffer from one or more of the above problems.

Of particular note are two groups who strive to provide high quality recommendations based on collaboration between vendors and various user groups:

- National Institute of Standards and Technology. NIST helps to drive and publish some of the widely used standards in the IT industry. NIST extensively collaborates with the private and public sector especially in the open, voluntary, and consensus-driven standards arena. In particular, the Computer Security Division (CSD) works with the various stakeholders via open workshops, public comment periods, peer-reviews, standards groups, industry groups, advisory boards, security groups, and other means to produce its proposed security standards and recommended practice documents. For more information on the NIST CSD, see: http://csrc.nist.gov/.

- Center for Internet Security. CIS has taken a consensus-based approach and has explicitly welcomed vendors, users communities, government and other organizations to participate in the development of security "benchmarks" or baselines. While not a perfect solution, their work has shown the great potential that can be achieved through a consensus-based benchmark approach. For more information on CIS, see: http://www.cisecurity.org/.

Groups such as these should be commended for their development and publication of baseline security recommendations and related tools. Their consistent willingness to work with vendors, users and organizations of all types is a testament to their commitment to developing quality recommendations.

5.2.3 Gaps and Recommendations

Today, the development of recommended security configurations still does not benefit universally from strong collaboration from product vendors, user groups and government organizations. The result is a complex mesh of suggested security configurations that are often conflicting, inaccurate or incomplete. This does not imply however that a single baseline security recommendation is appropriate. It is not inconsistent to have a set of baseline security recommendations, for example, that applies to specific environments or risk profiles. Security is not an absolute, and as such baseline security recommendations will always be tailored for their specific environment and requirements.

Recommendation: Vendors, user groups, and government organizations should take a more proactive role in the development of and collaboration on product security recommendations. The U.S. Government, user groups and consumers play an important role by encouraging such collaboration.

Recommendation: Vendors, user groups, consumers and the U.S. Government should encourage groups developing product security recommendations to make every attempt to ensure that products that are configured in accordance with their recommendations are left in a vendor-supported state (unless clearly declared at the beginning of the recommendation).

Recommendation: Vendors, user groups, consumers and the U.S. Government should encourage groups developing product security recommendations to clearly delineate the product versions for which the recommendations apply. In addition, reinforce the need for these organizations to ensure that their recommendations are reviewed and corrected as the product is patched, updated or enhanced. Vendors should maintain product security recommendations as products are patched, updated or enhanced.

Recommendation: Vendors, user groups, consumers and the U.S. Government should encourage groups developing product security recommendations to work closely with product developers to ensure that security recommendations are available at or near the actual product launch date. Many times such recommendations are provided well after the product has been deployed in many environments leaving those users in a potentially vulnerable state for weeks or even months.

Recommendation: Vendors should leverage heightened forms of collaboration with user communities and government organizations, where possible, to improve the security capabilities and out-of-the-box security posture of their products.

Recommendation: Vendors should endeavor to provide both secure and supported product configurations. Similarly, vendors should not hide behind claims of unsupportability but instead actively participate in the development of supported baseline security configurations and recommendations for their products.

5.3 Coordination of Security Recommendations

5.3.1 Current Landscape

The coordination and management of security recommendations is a critical function that must be implemented for numerous reasons, including the following:

- Coordinated, broad-based efforts usually produce more effective, useful checklists and consensus-based benchmarks;
- Centralized access to security configuration checklists, benchmarks and related information enables users to quickly and easily locate, test and implement security recommendations;
- Broad-based efforts using vendors, experienced large scale users and other user communities usually results in more accurate, usable, and well-tested security recommendations[6];
- Common formats for broad, peer-reviewed, vetted or consensus-based security recommendations and check lists are more easily integrated with configuration and policy management tools;

The current landscape falls short of these goals. While some organizations such as NIST, NSA, CIS and individual vendors provide security recommendations; they are often not widely known to the average user or administrator, although to a degree user awareness is growing. Today, in many cases, users must find their way through a maze of web sites, mailing lists and other forums to find security recommendations that may be relevant to them. Once located, there is often no assurance for these users that the security recommendations offered are relevant, correct, current or even appropriate for their environment. The problems facing the current landscape can be divided into the following categories:

- Lack of Central Coordination. Security recommendations are not coordinated by a central organization nor is there any one, common portal for users to obtain these recommendations. As a result, users are forced to search vendor, user group, government and other sites in order to find the information that they need to secure their products and environments.

[6] Consensus or broad-based security recommendations and settings should be used as a baseline to secure IT products with the recognition that different communities will have different security policies and needs. This will result in the need for checklists that meet different security policies. There is no one monolithic model to meet all policies, although there may certainly be certain baseline properties that can be shared between them.

- Lack of Common Formats and Frameworks. There is no standard or common set of requirements to describe and characterize security recommendations, benchmarks or check lists nor does there exist a common format or language for specifying this information. The terms used in security recommendations are often industry specific and in proprietary formats. A common, non-proprietary format and language to express security recommendations would assist users in understanding, customizing and applying security recommendations. Such common formats and frameworks would also promote better integration with configuration management tools.

- Lack of Policy. There is currently no common agreement on baseline policies to which security recommendations would apply. The lack of stated, common policies creates difficulty for users integrating security recommendations into their local policies and requirements.

In general, users must work very hard to locate, acquire, and apply security recommendations. These recommendations tend to be relatively scarce. When such recommendations can be found, users discover that the material is often incomplete or not well maintained. If multiple sources of recommendations are found, it is not uncommon for each of these sources to present conflicting recommendations and viewpoints with no indication or background as to why. Further, the policies upon which the security recommendations are founded are often unstated making it difficult for the user to determine if the recommendations apply to their environment.

Aggravating the problem is that often security recommendations are developed in silos often with no vendor participation. The recommendations resulting from such efforts are often poorly documented and tested (except in limited cases), incomplete or even in some cases incorrect. If the vendor is not involved in the development process, it is also likely the recommendations will not be supported leaving the user with few means for obtaining technical support to help answer questions or address problems arising from the use of the security recommendations.

5.3.2 Ongoing and Related Work

Security recommendations are coordinated by different entities for different organizations. Federal agencies look toward NIST for guidance, while Department of Defense (DOD) uses guidance developed by the NSA and DISA. Industry uses guidance provided by various organizations, including CIS, the SANS Institute, Information Security Forum (ISF), the CERT Coordination Center (CERT/CC), individual vendors and others.

- Consensus Efforts. Consensus efforts in producing security recommendations typically include the involvement of several independent groups who identify and create security recommendations for a particular product. CIS is one such group who brings together user communities, vendors and government organizations such as NIST, NSA, and DISA to create and producing consensus-based security checklists or benchmarks. The involvement of various groups in the decision-making process can lead to a documented, tested, baseline set of recommendations that can then be modified to meet an organization's local policy.

  For example, the “Windows 2000 Gold Disk” developed and used by the DOD scans a Microsoft Windows 2000 system and applies, where appropriate, security settings that were published in the CIS Windows 2000 Benchmark. This Benchmark document was developed through a census process with participation from Microsoft, NIST, NSA, DISA, CIS and many others. The success of this effort continued after Microsoft developed and published the Windows 2003 Server Security Guide. Microsoft leveraged the CIS Benchmark process to obtain consensus on these new baseline recommendations. As a result, the NSA has elected not to produce its own security guide for the Microsoft Windows 2003 Server product in favor of recommending the material published by Microsoft. This example illustrates what can be achieved when vendors, user groups and other organizations work with one another and collaborate on a baseline set of security recommendations.

- Vendor Efforts. Some vendors have begun to produce security recommendations for their products. Such work can take a variety of forms including product documentation, reference documents, checklists or benchmark guides. Often, these vendors have been driven by the involvement of various federal agencies and industry. While the checklists represent tremendous benefit to users in a homogeneous environment, they could present interoperability problems with third party applications or when applied to a heterogeneous environment.

- NIST Checklists Program. The Cyber Security Research and Development Act of 2002 [CSRDA] tasks NIST to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government."

  In response, NIST is developing the Security Checklists for IT Products program to facilitate the development of checklists for many IT products. NIST is also creating a central repository for the checklists and a search capability for locating and retrieving checklists. The checklists would be submitted ideally by or with the support of vendors (in consultation with a broad spectrum of security experts, user community, and others with operational expertise) for specific products, and would also include checklists developed by consensus groups, the U.S. Government, academia, or other sources. NIST is developing a checklist description framework and several security environments, including a home users/small-business security environment, and enterprise security environment, and a high security environment.

  The overall aim of the program is to (1) facilitate the development of high quality checklists in a coordinated manner with the eventual aim of encouraging vendors to produce products with the checklists embedded, and (2) to make the checklists easily available to users. NIST is considering creating a logo program for use by vendors in their product advertising to inform users that a product checklist is available at the NIST repository.

- DOD STIGS and NSA Security Guides. DISA working with NSA has been producing security recommendations known as Security Technical Implementation Guides (STIGs). The STIGs were developed to assist DOD sites in securing their systems. STIGS exist for a variety of products and applications, including many versions of UNIX, Windows, and common technologies such as wireless networking. The STIGS are produced by DISA through contributions from various parts of the DOD. These STIGs are also hosted on the NIST web site.

- CERT/CC Efforts. The CERT/CC generally has coordinated response to Internet related security problems, but has also produced various security recommendations for technologies and services such as for IT products. Other incident handling teams that coordinate with the CERT/CC through FedCIRC and the Forum of Internet Response and Security Teams (FIRST) have also produced security recommendations. These recommendations have been written by incident handling team members after dealing with numerous security attacks and vulnerabilities and often represent a wealth of information.

5.3.3 Gaps and Recommendations

The NIST Security Checklists program, sponsored and funded by DHS, aims to provide an overall framework for the specification, development, and dissemination (e.g., portal access) of security checklists.

Recommendation: The U.S. Government should complete the development of the NIST central repository for security recommendations and checklists based on a common description language, format and framework. This portal should include appropriate security mechanisms to greatly assist in locating and retrieving relevant security configuration information as well as comparing checklists that may be available for the same or similar products.

Recommendation: Vendors, user groups, consumers and the U.S. Government should work with NIST to develop standards and requirements for checklists, baseline policies for specific environments, and peer-reviewed or consensus-based checklists. Checklists, submitted by vendors, user groups and other organizations could be used as input for the creation of consensus-based checklists. NIST can serve as a neutral third-party to industry and facilitate the coordination between vendors, agencies, academia, industry, and other organizations such as consortia. Vendors should consider certification of their products against these checklists, to ensure that products configured per the checklists do not break other products that depend on them.

Recommendation: The U.S. Government as well as user groups and vendors should promote the use of the completed NIST central repository for security recommendations and checklists. Promote the existence and use of this portal as a common source for submitting, collecting and developing agreement on security recommendations and checklists.

5.4 Secure by Default

5.4.1 Current Landscape

Many products built and deployed in today's environments are not designed for survivability. Their lack of "out of the box" protection is often justified by a perceived lack of customer interest or by a desire to be completely functional and interoperable as soon as the device is powered on. While certainly issues such as these will drive market demand, the lack of "out of the box" security in many products is staggering.

There have been studies showing that products deployed into hostile computing networks, such as the Internet, have been compromised in anywhere from minutes to days[7]. Often, the length of time between when a vulnerable product is deployed and when it is compromised comes down to luck. Attackers with a variety of interests and motives are actively scanning networks such as the Internet to find and take control of vulnerable systems and products. These problems are not limited to public networks such as the Internet, however. In fact, the Computer Security Institute (CSI) and Federal Bureau of Investigation (FBI) have released computer crime statistics[8] showing that over the last four years, organizations were just as likely to be attacked by one of their own (disgruntled) employees as by an independent hacker.

By failing to implement secure by default configurations, vendors are placing the entire burden of securing products on their users. In many cases, users are not made aware of the risks of or threats to using a product in its default configuration. Such users may never change the default values leaving them vulnerable to attack. Further, combined with incomplete or inadequate security documentation, recommendations and guidance, this problem is compounded often leaving the user unsure of what to change and how those changes should be implemented. For those users wishing to adequately secure their products, the lack of secure by default configurations add to the complexity and recurring administrative and support costs of product ownership.

With the growing interest in security among user communities of all types, it is no wonder that some vendors and other organizations are attempting to develop products and solutions that are secure by default. There is a lingering question however whose answer is just as varied as the problem: "What does it mean to be secure by default?" The answer to this question will most certainly vary based on who provides the answer. To many organizations, this means protecting from external threats, but this approach may not apply to all products, organizations or situations.

To date, there is no single vision of how products should be configured for "out of the box" security when shipped from their manufacturer. Consider for example, two operating systems OpenBSD and Microsoft Server 2003. One approach taken by OpenBSD, since its inception, has been isolation[9]. All services with the exception of one remote access protocol are disabled by default. It is hard to be vulnerable if you are not running anything. In this regard, OpenBSD clearly represents one end of the spectrum focusing primarily on security over out-of-the-box interoperability and convenience. Toward the middle of the spectrum, Microsoft chose to selectively disable frequently unused or problematic services so that the resulting configuration is both more secure by default and can still be easily integrated into existing environments. On the far side of the spectrum, there are many organizations that do nothing to address the out-of-the-box security of their products.

Another similar approach taken by organizations such as Hewlett-Packard Company, Red Hat and Sun Microsystems is to provide tools that enable their products to be secured during installation. While not technically, secure by default, this approach solves the same class of problems and often provides users with a more flexible means of configuring the security at install time to meet their specific needs.

---

[7] The Honeynet Project has been actively looking into the issues surrounding attacker methods, motives and techniques. In July 2001, this non-profit research organization released a report entitled "Know Your Enemy: Statistics" [HNP2001] that illustrates the severity of the problem based on eleven months of empirical data. While the report is now dated, the problems have not disappeared. In some respects, they have continued to multiply as more users and products connect to the Internet without first properly securing their environments.

[8] This information was taken from the 2003 FBI/CSI Computer Crime Survey [CSI2003].

[9] The OpenBSD team does not rely only on the secure by default security posture of their product. In addition, since 1996, the team has pro-actively and continuously evaluated the OpenBSD software for security flaws, quickly fixing problems as they were found. Also, since the Canadian-based OpenBSD project was not subject to U.S. export controls, OpenBSD has, for some time, been able to leverage the benefits of integrated strong cryptography. For more information, see http://www.openbsd.org/security.html.

5.4.2 Ongoing and Related Work

There is a fair amount of ongoing work in this area mostly due to increased support from a number of product vendors. It would be impossible to list all of the vendors with ongoing or related work in this space. Included below are just a few vendors that are actively working to develop their own secure by default configurations and/or install-time security configuration tools:

- Hewlett-Packard Company
- Microsoft Corporation
- OpenBSD
- Oracle Corporation
- Red Hat, Inc.
- Sun Microsystems, Inc.

In addition, many vendors, especially those providing security products and services, also provide secure by default configurations even though they are not touted as such. For those organizations, such configurations have become a way of life. Examples of such organizations include:

- Checkpoint Software Technologies, Ltd.
- Internet Security Systems, Inc.
- SourceFire, Inc.

While no single solution is perfect for every user community or risk profile, the work of these and other organizations to facilitate the deployment of secured configurations either out of the box or during installation time should be applauded and encouraged.

Vendors are not the only ones who can "develop" secure by default configurations. Consumers, especially large organizations and government agencies, can often stipulate contractually that a vendor must deliver their product in a pre-defined configuration. As a result, such organizations are at an advantage since they can require products to be delivered in secure by default configuration (based on some pre-defined set of security recommendations). Further, such organizations can also stipulate that updates to the product meet specific security requirements as well.

A recent example of this was the work done by the U.S. Department of Energy (DOE), in concert with DHS, NSA, DOD and the General Services Administration and others. Working with Oracle and CIS, these agencies developed a consensus-based security benchmark for the Oracle database product, versions 8i and 9i. This Oracle Benchmark was published by the CIS along with an assessment tool.

Separately, Oracle, working with a third party (Opsware), worked to support the pre-configuration of licensed Oracle software for DOE in accordance with CIS guidelines. This allowed automated configuration of Oracle, per the CIS benchmark, as deployed in DOE. In this case, the purchasing power of the U.S. Government was certainly a deciding factor, but nonetheless, success can still be achieved for smaller organizations if they make security, including "out-of-the-box" security, a key criterion in their proposals and during their decision-making process.

5.4.3 Gaps and Recommendations

Today many products still do not provide strong out-of-the-box security configurations. Regardless of the method used to achieve a strong out-of-the-box security posture, it is important that such practices be more widely adopted to help reduce the window of vulnerability, complexity and costs associated with product installation and configuration.

Recommendation: Vendors should collaborate more directly with their user communities to better determine what changes are commonly made to their products during or immediately after installation to improve upon their out-of-the-box security posture. Using this information, vendors may be able to change default configuration parameters to make products more secure by default. Note that in some cases the inverse of this recommendation is also true. Some user communities appear to feel that too much vendor involvement will compromise their actions. Only with true involvement from both parties will an effective and complete set of changes be developed and integrated into

products. The U.S. Government, user groups and consumers have a key role to play in encouraging and participating in such collaboration.

Vendors should make secure by default a product release requirement. In the short term, vendors may elect to adjust default security settings so that dependent products will continue to function. However, vendors should improve (i.e., harden) default security settings from major product release to major product release, so that product defaults become more secure over time.

Recommendation: Vendors should provide stronger out-of-the-box security configurations and/or provide supported capabilities and tools that simplify and automate the process of securing their products.

While strong out-of-the-box security configurations are preferred, it is recognized that updating existing products to comply with this requirement can be costly, time-consuming and can result in various incompatibilities with current and supported versions of the product. As a result, it may not be possible for a vendor to transition a product to a more secure out-of-the-box state for several years, depending on product release cycles. To mitigate this gap, vendors are strongly encouraged to include software tools, scripts, or wizards to guide users through the process of securing their product post-installation.

Ideally, these tools would leverage vendor-provided, peer-reviewed or consensus-based security recommendations while also allowing users to configure the product to meet their specific security requirements and needs. These tools should always default to a secure setting.

Recommendation: Vendors that deliver products supporting multiple installation or risk profiles should provide and support at least one configuration profile that implements a baseline level of security. This option should be the default. A user installing the product should be able to override this option based on specific site policies and requirements.

It is recognized that there are scenarios where security requirements for products will vary significantly so it is important that users be given the choice to install a product in a manner appropriate for them.

Recommendation: Vendors should more clearly document the out-of-the-box security risks and assumptions for their products including any external dependencies that may exist such as requirements for the device to exist only on a "private network." Vendors should provide recommended (secure) deployment scenarios as part of product documentation.

Recommendation: Vendors should develop awareness plans to educate users and vendors about the risks of out-of-the-box security configurations and the need to tune the security configuration of products for their specific security policies, requirements and risk profiles.

Recommendation: Vendors should respect the installed security configuration of products when patches are applied or upgrades performed. Where possible, such user configurable settings should not be overwritten thereby possibly degrading the security posture of the upgraded product.

Recommendation: Vendors should include with their products, a tool or capability that allows a user to quickly and easily report on the security posture of the installed product. This information can then be used to identify common security configuration changes and to help simplify ongoing security administration and management.

Additionally, third party vendors are encouraged to leverage these tools (and their respective APIs), to extend upon the baseline level of functionality to provide more sophisticated security assessment solutions. For example, third party tools could be developed to deliver a more thorough, targeted or even profile-based security assessment. Similarly, such tools could be used to evaluate groups of related or integrated products in an attempt to provide a more complete security assessment.

5.5 Secure in Deployment

5.5.1 Current Landscape

The challenges associated with product installation are minor relative to the issues involved with the integration and deployment of products, especially when several products must be integrated to solve a particular problem. Today, even if a product does indeed document its security capabilities and perhaps baseline recommendations, most products today do not come with documentation that clearly discusses the product's security assumptions and dependencies.

For example, if a given application is sold to work with a particular vendor's operating system, rarely does the application documentation describe what software components or services of the vendor's operating system are interrelated. This can create significant challenges for users attempting to secure that operating system since they do not know if any of their changes will adversely impact the operation or support of the application. This problem is significant because even changes that appear to be benign could result in the failure of component that is less often used. As a result, changes that appear to work successfully may result in failure at some unknown point in time. Very often this is because the application vendor is only attempting to verify that their application works as expected on the target operating system. As a result, the application vendor's testing may only be done on a system that has not been secured even in a minimal way. The lack of product testing using real world deployment scenarios contributes to this problem[10]. Very often the result is that neither the application nor the operating system vendor can easily help the customer to understand the impact of security configuration changes on the operation or support of the products. This leaves the user with two options: (1) to move forward with a secured configuration and implement a significant amount of testing to ensure proper functionality or (2) do nothing and leave the products configured in their default state.

The first path forces each user to take on this additional cost and complexity, for each product installation, upgrade or patch, with no assurance that the final results will adequately ensure that their security configuration will not cause the product to fail at some future time. The second path is even worse leaving the user potentially vulnerable to any number of vulnerabilities associated with the default configurations of the application and operating system. This example looked at just two products. The typical environment is however comprised of many more products often working together on the same system. As products are added to the configuration, the complexity associated with determining the impact of security changes on all of the other products increases significantly. There is actually a third path as well. Some users may move forward with a secured configuration only to be frustrated with product failure or by the lack of documentation and support for such secured configurations. Often these users may give up and fall back to using the products in with their out-of-the-box configuration. In the worst case, the vendor may even require the customer to revert back to a default configuration in order to receive technical support.

5.5.2 Ongoing and Related Work

Very few vendors provide sufficient documentation describing the security assumptions and dependencies associated with their product. Even fewer work with their ISVs, IHVs or OEMs to ensure that their partners products are tested using typical, secured configurations that are indicative of their user community.

5.5.3 Gaps and Recommendations

Products are rarely used in isolation. More often products must be layered onto one another or otherwise integrated in order to solve a particular problem. The assumptions and dependencies associated with these interrelationships are rarely documented. As a result, users must sometimes choose between security, supportability, and cost – associated with the time it would take to manually uncover these interdependencies. This is a significant problem for environments today with no immediate solution in sight.

Recommendation: Vendors should work with their ISVs, IHVs and OEMs to ensure that security assumptions and dependencies are well known and documented.

[10] Aggravating this problem, however, is the lack of agreement as to what constitutes “real world deployment scenarios.”

Recommendation: Vendors should perform quality assurance and functional testing of their products using baseline security configurations commonly used by their customers. To be effective, however, consumers, user groups and the U.S. Government should collaborate with vendors on the development of these common security configurations.

Recommendation: Vendors, user groups, consumers and the U.S. Government should work together on standard protocols and methods for documenting and validating compliance with security requirements and dependencies. One such early draft in this area is "XCCDF - An Extensible Configuration Checklist Description Format for the Security Community" [XCCDF]. This proposal seeks to establish a common, uniform way of representing security benchmark or checklist criteria.

5.6 Management of Secured Configurations

5.6.1 Current Landscape

Security configuration recommendations for IT products, even those emerging from a collaborative process, are ineffective unless correctly and consistently applied. Unfortunately, properly implementing security recommendations can be a complex, labor-intensive task, demanding a level of skill and commitment of time often beyond that of average organization.

Today, the majority of tasks associated with discovering, customizing, and implementing security recommendations remain quite manual and labor intensive. Such processes are also often error-prone and inconsistent when applied to even a moderate set of products in a typical organization. The process of evaluating the security posture of a product against a defined security configuration is no better. While there are both commercial and open-source products available on the market to minimize some of the pain associated with deploying and maintaining the security configurations of products, their use is typically not widespread or even consistent within the same organization.

Security configuration management tools must fulfill two primary functions. First, the tool must be able to assess and compare the security configuration of an installed product against an established configuration standard and report any inconsistencies that are found. Secondly, security configuration management tools must also be capable of implementing recommended changes to a product to bring it into compliance with the configuration standard. Such products must also support:

- The simple customization of configuration standards to meet local security policies and requirements. This is necessary since security policies are not an absolute and requirements will vary by application, organization and risk level. These customizations should apply equally to the application of changes as well as the assessment of current product configurations.

- The safe reversal of configuration changes when problems are detected that require a specific set of changes must be backed out. No product is perfect, so there may be times when changes that have been applied need to be reversed due to unexpected or unintended failures.

- The detection of dependencies, where possible, so that changes made to a product leave it in a consistent, working and supportable state.

There exist very few security configuration management tools on the market today that meet each of these requirements. As a result, often users must perform each of these steps manually, with a collection of assembled programs and tools that may or may not work well together, or using custom programs developed by the local organization or user group.

In addition, recent regulatory forces are also driving the emergence of an IT security policy compliance market. The Federal Information Security Management Act of 2002 [FISMA] levied policy compliance requirements on government agencies. Similarly, the U.S. Public Company Accounting Reform and Investor Protection Act of 2002 [SOX], better known as the Sarbanes-Oxley (SOX) Act, is driving public sector and market demand for security policy compliance tools and capabilities.

SOX aims to reduce fraud and conflicts of interest by regulating all financial processes. Since businesses have come to depend on IT as the backbone of their operations, including financial processes, SOX will have a dramatic impact on IT. Security policy management tools that can implement and validate IT-based financial processes to comply with SOX requirements will be in high demand as U.S. publicly held companies come to grips with the new law.

Until SOX, managers had no direct incentive to implement strong security practices on a wide scale, other than to avoid often indefinable costs related to failed audits, intrusions or compromises. An IT organization configured to comply with known recommended practices will be more likely to comply with SOX requirements, averting known and specific legal and monetary penalties.

5.6.2 Ongoing and Related Work

Certainly, to combat this problem, tasks associated with the implementation and evaluation of security configurations should be simplified, automated and make easily reproducible and auditable. While there are very few tools capable of meeting all of these new challenges in a flexible, scalable and effective way, market forces are driving the emergence of a security policy compliance market.

There are many tools available on the market today, however, that are able to meet some subset of the requirements discussed above. Most of these products have typically fallen into the vulnerability management category. The Gartner Group defines vulnerability management as "a set of processes and technologies that establishes and maintains a security configuration baseline; discovers, prioritizes and mitigates exposures; establishes security controls; and eliminates root causes."

The majority of IT security policy and vulnerability management products available today are based on one or more of the following sources of information:

- Consensus-derived recommended practices such as those provided by CIS and SANS
- Vendor specific recommendations such as Sun Microsystems' Security BluePrints, IBM's Redbook Security Supplements, Oracle's Security Configuration Guide, or Microsoft's Security Operations Guide.
- Government recommendations such as those developed by NIST, NSA and DISA

Note that some security product vendors also employ research and development staff who are also responsible for developing security configuration recommendations for their product and clients.

The following is a small sample of security policy and vulnerability management tools. There are many products in this space with a vast array of capabilities. While there is overlap among some products, the sheer depth of this space focuses many vendors on subsets of the policy and vulnerability management problem.

Organization	***Product***
BindView	bv-Control
Computer Associates	eTrust Policy Compliance
NetIQ	Security Manager
Symantec	Enterprise Security Manager
Internet Security Systems	Site Protector

These tools represent a growing understanding that IT security must be a continual process and integral to system configuration management. All of these products offer customization capabilities, and most provide configurations based on a selection of peer-reviewed, consensus-based, vendor-specific or government recommendations. Many more tools are available to manage configurations and patch distribution across the enterprise, but do not apply specific recommendations.

5.6.3 Gaps and Recommendations

While there are a number of products currently in the security policy and vulnerability management space, very few offer the complete range of capabilities needed to provide comprehensive security management to user communities. To be successful, cooperation between vendors, user communities, and government organizations is required to ensure that products in this space are able to meet the range of security, performance, scalability and reliability requirements of these diverse user populations.

Recommendation: Vendors, user groups, consumers and government organizations should collaborate closely on identifying requirements and capabilities needed to improve security policy management practices and tools in the enterprise.

Recommendation: The U.S. Government as well as user groups and consumers should encourage independent evaluation and/or certification of security management products. Users must have confidence in the tools they choose to deploy in their environments. It is important that these tools not only work as advertised, but they must also not be responsible for introducing new vulnerabilities or undocumented risks into the user's environment.

Recommendation: Vendors should provide baseline security assessment or management capabilities with their products. Individual products should, either natively or in conjunction with another tool, evaluate the deployed configuration of a product against a set of baseline recommended practices reporting any inconsistencies detected. Such tools can be very useful in detecting common product configuration errors or baseline product-specific security risks. Organizations looking for more comprehensive capabilities could then deploy a security policy and/or vulnerability management product.

Recommendation: Vendors should provide stable and documented interfaces for managing the configuration of their products. As part of this effort, users should encourage the use of standard protocols and formats where possible so that a given vendor's product is able to easily integrate into an organization's security and policy management infrastructure.

6.0 REFERENCES

[FIPS199] National Institute of Standards and Technology, Federal Information Processing Standards (FIPS) Publication 199, "Standards for Security Characterization of Federal Information and Information Systems", Draft – Pre-publication Final, December 2003. http://csrc.nist.gov/publications/drafts/draft-fips-pub-199.pdf

[SCIP] National Institute of Standards and Technology, "NIST Security Checklists for IT Products", Draft, November 2003.

[FISMA] 108th Congress of the United States, "Federal Information Security Management Act of 2002", H.R. 2458, Title III, January 2003. http://csrc.nist.gov/policies/HR2458-final.pdf

[CSRDA] 107th Congress of the United States, "Cyber Security Research and Development Act", H.R. 3394, December 2001. http://www.house.gov/science/cyber.htm

[HNP2001] The Honeynet Project, "Know Your Enemy: Statistics", July 2001. http://www.honeynet.org/papers/stats/

[CSI2003] Computer Security Institute, Federal Bureau of Investigation, "8th Annual, 2003 CSI/FBI Computer Crime Survey", June 2003. http://www.gocsi.com/forms/fbi/pdf.jhtml

[XCCDF] Ziring, Neal, et al., "XCCDF – An Extensible Configuration Checklist Description Format for the Security Community, Version 0.5, December 2003.

[SOX] 107th Congress of the United States, "U.S. Public Company Accounting Reform and Investor Protection Act of 2002 ", H.R. 3763, January 2002.

[X.805] International Telecommunication Union – Telecom Standardization (ITU-T), Recommendation X.805 – Security architecture for systems providing end-to-end communications, September 2003. http://www.itu.int/itudoc/itu-t/aap/sg17aap/history/x805/x805.html

7.0 RECOMMENDATIONS SUMMARY

The following is a summary of the recommendations included in this document.

Documented Security Recommendations

Recommendation: Vendors, user groups, and government organizations to should take a more proactive role in the development of and collaboration on product security recommendations. The U.S. Government can play an important role by encouraging such collaboration.

Recommendation: Vendors should perform more realistic functional and security testing of their products in real-world situations. All too often, product testing is done in a lab setting that almost never reflects how the products will actually be deployed in a user's environment. The results from this testing can be used to determine what security features and capabilities may be missing that should be added to the product. This information is also useful for the development of product security recommendations. The U.S. Government as well as user groups and consumers should actively participate in this testing by contributing their use cases, usage and deployment considerations and other feedback.

Recommendation: Vendors should provide more substantive security recommendations, configuration checklists, best practices, assumptions, dependencies, and considerations in their product documentation. Vendors are generally in the best position to provide much of this information. Vendors should leverage feedback from user groups and government organizations to improve their security documentation based on actual deployment and usage.

Recommendation: Vendors should work with their ISVs, IHVs and OEMS to better certify common security configurations impacting a set of products rather than developing secured configurations in isolation. This includes documenting any shared assumptions, dependencies or requirements. As a result of this collaboration, vendors may be able to participate in logo or certification programs.

Recommendation: The U.S. Government should encourage organizations to develop security recommendations that apply to one or more specific risk profiles. Recognizing that security is a spectrum and not an absolute, it is both appropriate and necessary to provide common set of recommendations based on a selection of pre-defined thresholds for risk. Similarly, encourage organizations to develop baseline security recommendations (if applicable) that apply to all user communities or environments. These could serve as the foundation for more comprehensive sets of recommendations that may apply only to specific risk profiles or product combinations.

To support this recommendation, risk profiles and security objectives such as those defined by the FIPS 199 publication [FIPS199] should be better promoted to academia and industry in addition to government for the purpose of building baseline recommendations and consensus. Such agreement, if achieved, would help promote the development and collaboration of security recommendations based on such models. In addition, the NIST draft publication titled “Security Checklists for IT Products” [SCIP] provides additional examples that highlight a baseline set of environments for which security recommendations could written. Note that FIPS 199 was developed in response to tasking to NIST under the Federal Information Security Management Act of 2002 [FISMA].

Collaboration on Security Recommendations

Recommendation: Vendors, user groups, and government organizations to should take a more proactive role in the development of and collaboration on product security recommendations. The U.S. Government can play an important role by encouraging such collaboration.

Recommendation: Vendors, user groups, consumers and the U.S. Government should encourage groups developing product security recommendations to make every attempt to ensure that products that are configured in accordance with their recommendations are left in a vendor-supported state (unless clearly declared at the beginning of the recommendation).

Recommendation: Vendors, user groups, consumers and the U.S. Government should encourage groups developing product security recommendations to clearly delineate the product versions for which the recommendations apply.

In addition, reinforce the need for these organizations to ensure that their recommendations are reviewed and corrected as the product is patched, updated or enhanced. Vendors should maintain product security recommendations as products are patched, updated or enhanced.

Recommendation: Vendors, user groups, consumers and the U.S. Government should encourage groups developing product security recommendations to work closely with product developers to ensure that security recommendations are available at or near the actual product launch date. Many times such recommendations are provided well after the product has been deployed in many environments leaving those users in a potentially vulnerable state for weeks or even months.

Recommendation: Vendors should leverage heightened forms of collaboration with user communities and government organizations, where possible, to improve the security capabilities and out-of-the-box security posture of their products.

Recommendation: Vendors should endeavor to provide both secure and supported product configurations. Similarly, vendors should not hide behind claims of unsupportability but instead actively participate in the development of supported baseline security configurations and recommendations for their products.

Coordination of Security Recommendations

Recommendation: The U.S. Government should complete the development of the NIST central repository for security recommendations and checklists based on a common description language, format and framework. This portal should include appropriate security mechanisms to greatly assist in locating and retrieving relevant security configuration information as well as comparing checklists that may be available for the same or similar products.

Recommendation: Vendors, user groups, consumers and the U.S. Government should work with NIST to develop standards and requirements for checklists, baseline policies for specific environments, and peer-reviewed or consensus-based checklists. Checklists, submitted by vendors, user groups and other organizations could be used as input for the creation of consensus-based checklists. NIST can serve as a neutral third-party to industry and facilitate the coordination between vendors, agencies, academia, industry, and other organizations such as consortia. Vendors should consider certification of their products against these checklists, to ensure that products configured per the checklists do not break other products that depend on them.

Recommendation: The U.S. Government as well as user groups and vendors should promote the use of the completed NIST central repository for security recommendations and checklists. Promote the existence and use of this portal as a common source for submitting, collecting and developing agreement on security recommendations and checklists.

Secure by Default

Recommendation: Vendors should collaborate more directly with their user communities to better determine what changes are commonly made to their products during or immediately after installation to improve upon their out-of-the-box security posture. Using this information, vendors may be able to change default configuration parameters to make products more secure by default. Note that in some cases the inverse of this recommendation is also true. Some user communities appear to feel that too much vendor involvement will compromise their actions. Only with true involvement from both parties will an effective and complete set of changes be developed and integrated into products. The U.S. Government, user groups and consumers have a key role to play in encouraging and participating in such collaboration.

Vendors should make secure by default a product release requirement. In the short term, vendors may elect to adjust default security settings so that dependent products will continue to function. However, vendors should improve (i.e., harden) default security settings from major product release to major product release, so that product defaults become more secure over time.

Recommendation: Vendors should provide stronger out-of-the-box security configurations and/or provide supported capabilities and tools that simplify and automate the process of securing their products.

While strong out-of-the-box security configurations are preferred, it is recognized that updating existing products to comply with this requirement can be costly, time-consuming and can result in various incompatibilities with current and supported versions of the product. As a result, it may not be possible for a vendor to transition a product to a more secure out-of-the-box state for several years, depending on product release cycles. To mitigate this gap, vendors are strongly encouraged to include software tools, scripts, or wizards to guide users through the process of securing their product post-installation.

Ideally, these tools would leverage vendor-provided, peer-reviewed or consensus-based security recommendations while also allowing users to configure the product to meet their specific security requirements and needs. These tools should always default to a secure setting.

Recommendation: Vendors that deliver products supporting multiple installation or risk profiles should provide and support at least one configuration profile that implements a baseline level of security. This option should be the default. A user installing the product should be able to override this option based on specific site policies and requirements.

It is recognized that there are scenarios where security requirements for products will vary significantly so it is important that users be given the choice to install a product in a manner appropriate for them.

Recommendation: Vendors should more clearly document the out-of-the-box security risks and assumptions for their products including any external dependencies that may exist such as requirements for the device to exist only on a "private network." Vendors should provide recommended (secure) deployment scenarios as part of product documentation.

Recommendation: Vendors should develop awareness plans to educate users and vendors about the risks of out-of-the-box security configurations and the need to tune the security configuration of products for their specific security policies, requirements and risk profiles.

Recommendation: Vendors should encourage vendors to respect the installed security configuration of products when patches are applied or upgrades performed. Where possible, such user configurable settings should not be overwritten thereby possibly degrading the security posture of the upgraded product.

Recommendation: Vendors should include with their products, a tool or capability that allows a user to quickly and easily report on the security posture of the installed product. This information can then be used to identify common security configuration changes and to help simplify ongoing security administration and management. Additionally, third party vendors are encouraged to leverage these tools (and their respective APIs), to extend upon the baseline level of functionality to provide more sophisticated security assessment solutions. For example, third party tools could be developed to deliver a more thorough, targeted or even profile-based security assessment. Similarly, such tools could be used to evaluate groups of related or integrated products in an attempt to provide a more complete security assessment.

Secure in Deployment

Recommendation: Vendors should work with their ISVs, IHVs and OEMs to ensure that security assumptions and dependencies are well known and documented.

Recommendation: Vendors should perform quality assurance and functional testing of their products using baseline security configurations commonly used by their customers. To be effective, however, consumers, user groups and the U.S. Government should collaborate with vendors on the development of these common security configurations.

Recommendation: Vendors, user groups, consumers and the U.S. Government should work together on standard protocols and methods for documenting and validating compliance with security requirements and dependencies. One such early draft in this area is "XCCDF - An Extensible Configuration Checklist Description Format for the Security Community" [XCCDF]. This proposal seeks to establish a common, uniform way of representing security benchmark or checklist criteria.

Management of Secured Configurations

Recommendation: Vendors, user groups, consumers and government organizations should collaborate closely on identifying requirements and capabilities needed to improve security policy management practices and tools in the enterprise.

Recommendation: The U.S. Government as well as user groups and consumers should encourage independent evaluation and/or certification of security management products. Users must have confidence in the tools they choose to deploy in their environments. It is important that these tools not only work as advertised, but they must also not be responsible for introducing new vulnerabilities or undocumented risks into the user's environment.

Recommendation: Vendors should provide baseline security assessment or management capabilities with their products. Individual products should, either natively or in conjunction with another tool, evaluate the deployed configuration of a product against a set of baseline recommended practices reporting any inconsistencies detected. Such tools can be very useful in detecting common product configuration errors or baseline product-specific security risks. Organizations looking for more comprehensive capabilities could then deploy a security policy and/or vulnerability management product.

Recommendation: Vendors should provide stable and documented interfaces for managing the configuration of their products. As part of this effort, users should encourage the use of standard protocols and formats where possible so that a given vendor's product is able to easily integrate into an organization's security and policy management infrastructure.

8.0 ACKNOWLEDGMENTS

The following is an alphabetical list of those people who participated in or contributed to the Common Configuration Working Group and the development or review of this report.

Name	***Organization***
Brian Andersen	Phoenix Technologies, Ltd.
John Banghart	Center for Internet Security
Chris Benjes	NSA
Glenn Brunette (Working Group Champion)	Sun Microsystems, Inc.
Tim Grance	NIST
Theresa Grant	The Dow Chemical Company
Brian Henderson	NSA
Clint Kreitner	Center for Internet Security
John LaCour	Zone Labs, Inc.
Alex Noordergraaf	Sun Microsystems, Inc.
Joseph Petragnani	St. Joseph's University
Hal Pomeranz	Deer Run Associates
Frank Reeder	Center for Internet Security
Murugiah Souppaya	NIST
John Wack	NIST

Appendix B

National Cyber Security Partnership
Technical Standards and Common Criteria Task Force

Research Working Group
RECOMMENDATIONS REPORT

April 19, 2004

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

The National Cyber Security Summit held in Santa Clara, CA on December 3, 2003 created the Technical Standards and Common Criteria Task Force. This task force formed the Research Working Group. This working group's objectives were to develop recommendations for areas of research in furtherance of support of the Common Criteria (CC).

This report is the output of the Research Working Group with recommendations for specific actions to fulfill the stated needs.

1.1 Problem Statement

The CC has a substantial ability to help validate the security claims of software products. However, at commercially-viable assurance levels (Evaluation Assurance Level 4[1] [EAL4] and below), there is no mechanism for verifying that a product is free from defects that weaken overall product security, e.g., bugs of any type that introduce security vulnerabilities. Independent (third party) testing for security faults after products have shipped does not help vendors produce better software, since it is far more expensive to remediate faults after product shipment than during development. (In fact, some faults that are discovered after the product has shipped may be impossible to remediate without major architectural changes.)

Vendors need tools that they can use during development to find the types of flaws in code that weaken overall security. Currently, there are few such tools available that meet the needs of vendors from "infrastructure providers" to small start-ups. There appears to be few incentives to invest in such technology (e.g., by venture capitalists) because the security software market has in part evolved based on protection of information technology (IT) against the consequences of poor quality code, rather than improving the code itself. The market for products that protect against attacks (that exploit defects in software) is far larger than the market for vulnerability analysis tools, just as there is more money to be made on selling bandages than on a vaccine that cures the underlying illness.

1.2 Recommendation

The U.S. Government should fund research into the development of better vulnerability analysis or "code scanning" tools that can identify software defects. The vulnerability analysis tools should be able to operate on code developed in a variety of programming languages, handle millions of lines of code daily, to support development of large, complex applications, and run on many operating systems, to support multiple development environments. They must be suitable for products ranging from IT infrastructure to business applications, as well as security products themselves.

The U.S. Government should require vulnerability analysis of products as a condition of procurement. This can best be achieved by first, providing vendors with the tools to do automated code scanning in-house and second, using the evaluation process to validate vulnerability analysis (through directly rerunning code scans or by verifying that a vendor has done so).

---

[1] Assurance levels higher than EAL4 are not considered by industry to be commercially viable for multiple reasons. So-called EAL4+ evaluations are not mutually recognized under the Common Criteria Mutual Recognition Arrangement (CCMRA), meaning that the entities that ask for them generally require at least those parts of the evaluation not subject to the CCMRA to be done by a lab certified by the local certification body. That is, the local lab would do the "plus" elements of the EAL4+ evaluation, and there would potentially be some revalidation of the base EAL4 evaluation, as well. EAL4+ evaluations tend to be significantly more expensive than EAL4 and below evaluations, both because of the higher assurance requirements and because they may have to be done in a relatively expensive venue, such as the U.S. Furthermore, since other signatories of the CCMRA do not accept an EAL4+ evaluation, a vendor may have to repeat the evaluation under other countries' evaluations schemes. EAL4+ evaluations thus suffer from the same defects that doomed the pre-Common Criteria evaluation world: companies have to evaluate the same product numerous times, against multiple countries' requirements, at considerable expense. While many companies are willing to do a single evaluation to substantiate their security claims, doing the same evaluation three, four or five times can also be three, four, or five times as expensive without any significant increase in security of the product. The insistence upon EAL4+ evaluations is a recipe for the failure of worldwide assurance efforts, once and for all.

2.0 DISCUSSION

Evaluation against the CC at commercially viable assurance levels (EAL4 and below) may do much to validate that claimed security mechanisms work as advertised, but they do not go far enough to establish that software is free from defects that may lead to "unintended consequences." While faults in software may not be errors in the security functionality itself, they may nonetheless result in a significant weakening of overall product security. For example, many products (even evaluated ones) are vulnerable to buffer overflows, which represent a significant proportion of all overall security vulnerabilities in software. Buffer overflows may allow an attacker to gain control of a machine, or mount a classic "denial of service" attack, thus bypassing security checks.

The stated desire of some proponents of EAL4+ evaluations (i.e., the National Security Agency [NSA], who has written "medium robustness" Protection Profiles [PP] at EAL4+) is the ability to perform vulnerability analysis of the software; that is, to do more intrusive analysis of a product to ensure that it is largely free from defects that would weaken security.

However, even if the goal of higher assurance evaluations is laudable, it does the vendor little good to have an outside entity perform vulnerability analysis as part of a security evaluation. A product may already be most of the way through the product development cycle if, indeed, it has not already shipped, which is more likely the case. (Evaluations are seldom done on products during product development for multiple reasons.) It is far more expensive to fix vulnerabilities in products that have already shipped, than it is to do so in products that are in development. For example, a product that has been ported to run on 10 operating systems now requires 10 separate patches to remedy a defect that affects all versions of product. Vulnerability analysis done by an outside firm after the product has shipped is thus "too little, too late." Having a third party discover vulnerabilities in software as part of an evaluation is like having a structural engineer review building plans only after the house has been built and occupied: defects are expensive to remedy after-the-fact, if they can be remedied at all.

Both customers and vendors are far better served by vulnerability analysis done by the vendor during software development, rather than during a product evaluation. Any vulnerability analysis done by evaluation labs that is desired could be a validation – providing assurance, if you will – of the vendors' own vulnerability analysis work. Either the lab could, as part of the security of the development environment portions of an evaluation, validate that vulnerability analysis is done during development. Or, the lab could rerun the (automated) vulnerability analysis tools.

Why isn't code scanning done already? In part, because even those vendors who want to build better software have few suitable automated tools that enable them to find more defects in software before the product ships. A culture of security, a formal development process, developer training on secure coding practice, code reviews and the like, however necessary, are insufficient without automated tools. For example, if a buffer overflow can be prevented by input validation, and to do so thoroughly requires 21 conditions to be validated, code that validates only 20 conditions is just as insecure (and just as costly to fix) as code that does no validation. "To err is human," and to rely on developers to validate their own secure coding practice by hand is to invite errors.

Furthermore, because of the breadth of the code base in commercial software (millions of lines of code in large infrastructure products) and the difficulty of accurate manual review of all code, automated tools are absolutely necessary to be able to validate that a product is free – or largely free – of defects that weaken overall security. Large products under development literally have changes every day to the code base, even during the final phase of development, when the development team may be focused on fixing "show stoppers" prior to shipment. Code scanning for security faults needs to be done often, during development, not once, after development is finished.

Some, mostly academics, argue for the development of "safe" programming languages that make common vulnerabilities much less prevalent. However laudable the goal of developing more secure programming languages, it is years away from fulfillment and does nothing to address vulnerabilities in products that are already in production, and will be used for years to come. The IT industry needs code scanning tools that can help identify and remediate defects in products that are currently shipping or under development.

The fact that there is not more code scanning tools readily available is, in part, a market failure. Many venture capitalists would rather support bandage companies than vaccine companies. That is, treating the symptoms of bad or insecure coding practice (for example, through specialty firewalls, risk-based patch management, and anti-virus

tools) of a problem that is never "solved" is a license to print money through repeatable revenues; fixing the underlying problem cuts off the revenue stream from customer use of "technical band-aids." While the IT industry may never get away from the requirement for defense-in-depth that some products can provide, the industry can significantly reduce customers' security exposure simply by writing better code. Under any cost/benefit analysis, customers and vendors will both benefit from better code through lower risk, lower cost to produce and apply patches, and stronger security.

The code scanning tools currently on the market are generally insufficient for large-scale software development, meaning that the large "infrastructure providers" of the IT industry lack the fundamental tools that would help them build better software. To be effective, the tools need to be able to scan source code, rather than object code (vendors obviously have access to source code if they developed it). They may need to work on very large code bases (e.g., many million of lines of code in an enterprise class product). They need to scan code in common programming languages, including C, Java, Perl, and others. They need to "scale" — to be able to run against these large code bases daily without becoming a development bottleneck through slow performance. The tools need to run on multiple operating systems, since software is developed in many different platforms and needs to be validated on many different platforms. The tools need to be delivered as products, not services (development organizations need to be able to use the tools themselves for code scanning to be economically viable and – more importantly – embedded into the development process). The error rate (false positive and false negative) needs to be acceptably low, and the error messages sufficiently descriptive that the non-security expert can understand what the problem is, diagnose and repair it.

These tools need to be usable by the nimble software startup as well, and economically priced for them. While the infrastructure providers need to improve their code, those providing the next generation of products — including the next generation of security software — also need to ensure that their code is robust and largely free of security-weakening defects.

There are other classes of code scanning software that work on object code, typically on applications software by mimicking attacks. There are a number of small startups in this sector, though it must still be explored for further research, for the same reasons cited above: the need to address the needs of many vendors, not merely the small niche IT vendors, nor merely the large IT infrastructure providers.

The ability to establish assurance (e.g., through evaluations) would benefit greatly from enhanced testing that the software is largely free of the kinds of defects that introduce security flaws that weaken product security, and thus system security. If the CC is to "catch on" broadly as a measure of security worthiness, it needs to address the fundamental question of reducing security faults in commercial software.

As a final note, if the U.S. Government provides these tools to industry and requires them to be used as a condition of procurement, industry can have no excuse for not producing better software, in fact, "provably secure" software. The benefits of improved products will accrue to all customer sectors, not merely the U.S. Government. It would be a worthy accomplishment indeed if the IT industry saw its last buffer overflow within 18 months, which accounts for over 50% of significant reported security vulnerabilities.

3.0 CONCLUSIONS

Recommendation: The U.S. Government should fund research into better code scanning tools that will help software development companies (both large and small) weed out more defects in software.

Recommendation: The tools should be made widely and/or freely available to companies to enable them to scan their code during the development process.

Recommendation: The CC can be amended to require vulnerability analysis at lower assurance levels (by a third party validating that a vendor does code scanning during development and remediates significant faults accordingly, or by the evaluation lab rerunning the scan separately). Alternatively, the U.S. Government can require vulnerability analysis by vendors, as a separate condition of procurement, if requiring vulnerability analysis at lower assurance levels is not accepted as a change to the CC.

Recommendation: In conjunction with the above recommendations, the requirement for medium or higher assurance evaluations (EAL4+) for commercial products should be dropped, since the stated reason for higher assurance evaluations by the proponents is the ability to do vulnerability analysis. Higher assurance evaluations for commercial software impose a cost burden that even the largest IT vendors cannot bear or should not bear, they do not substantially improve product security, but may result in vendors paying multiple times for the same evaluation in different markets. Furthermore, finding faults in software that has already shipped is far more expensive and less effective than giving vendors the tools to be used during the development process.

4.0 GLOSSARY

CC	Common Criteria for Information Technology Security Evaluation. Established as ISO 15408.
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCMRA	Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of IT Security
EAL	Evaluation Assurance Level
NIST	U.S. National Institute of Standards and Technology
NSA	U.S. National Security Agency
PP	Protection Profiles

5.0 ACKNOWLEDGMENTS

The following is an alphabetical list of those people who participated in or contributed to the Research Working Group and the development and review of this report.

Name	***Organization***
Mary Ann Davidson	Oracle Corporation (Working Group champion)
James Norris	Sprint
Shaun Lee	Oracle Corporation
Jack Suess	University of Maryland, Baltimore County

Appendix C

National Cyber Security Partnership
Technical Standards and Common Criteria Task Force

Best Practices for Technical Standards Working Group
RECOMMENDATIONS REPORT

April 19, 2004

1.0 EXECUTIVE SUMMARY

National Cyber Security Summit held in Santa Clara, California, on December 3, 2003, created the Technical Standards and Common Criteria Task Force. This Task Force formed several working groups including one focused on Best Practices for Technical Standards.

The Working Group focused its efforts on assembling a compilation of existing sources of best practices. The Group believed this was an important and useful contribution to the cyber security debate because the breadth and depth of existing sources of guidance and direction were not as well known as they should be. Failure to recognize the variety and specificity of such sources could lead to mistaken conclusions that the government needed more standards or that the Common Criteria (CC) process had to be used by default.

2.0 MISSION STATEMENT

The mission of the Task Force was "to respond to current technical vulnerabilities and risks, analyze the security requirements including at industry-specific and general infrastructure-wide level, associated 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 for the existing testing activities, including the CC standard and NIAP testing program in support of the 'NIAP review.'"

The Best Practices Working Group was to review, assess, and amend if necessary existing checklists of recommended best technical cyber security practices. Within the group's charter was to possibly look at current gaps as well as to examine alternative approaches to testing and ways to obtain assurance that may not be testing-based.

3.0 COMPILATION OF BEST PRACTICES

The Working Group focused its efforts on assembling a compilation of existing sources of best practices. There had been significant discussion at the Summit that not enough was known about the extensive work that has been already undertaken. Without such knowledge, there were significant risks that: (1) duplicative and unnecessary work would be undertaken in the private sector; (2) an inaccurate presumption might arise that additional government standards were necessary to fill the "void"; or (3) there would be a belief that the CC process had to be used by default.

The compilation organizes and characterizes existing guidance in the following areas:

- Information security management models that are principles-based
- General (not just information) control models
- Information security management models that are controls-based
- Comprehensive models – capability maturity
- Product security models
- Board governance guidelines
- Guidelines for senior managers
- Sector specific guidelines
- Legal/regulatory requirements
- Security checklists
- General management guidelines
- Risk management models
- Guides for home and individual users
- Higher education guidelines
- Configuration/patching guides

While the compilation is thorough, given constraints of time and resources the Working Group does not believe it is exhaustive. Additional sources can and should be easily added to the various lists. Figure 1 shows how best practices and standards can be used to help protect the critical resources.

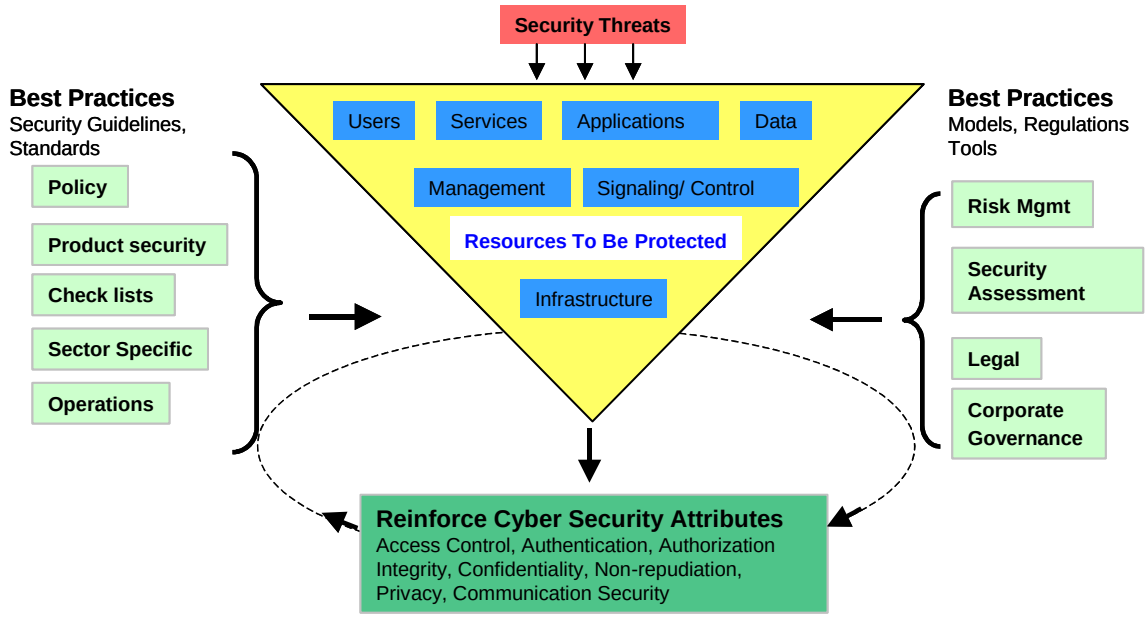

Figure 1 – Best Practices View to Protect Critical Resources

4.0 RECOMMENDATIONS

The Working Group believes that for organizations large and small, governments and business and non-profits, as well as individuals, there are significant sources of guidance and direction on what to do, and how to do it, to improve cyber security. Other Task Forces are addressing how to better educate about the threats and problems and to motivate organizations and individuals to pursue such improvements. But where there is the will, this compilation shows that there is definitely a way.

Best Practices for Technical Standards Working Group Compilation

Document	URL	# Pages
Information Security Mgmt Models – Principles Based		
OECD Guidelines for the Security of Information Systems and Networks (Nine pervasive principles for information security upon which several other guides are based.)	www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html	30, English & French
GAPP – "Generally Accepted Principles and Practices" NIST SP 800-18, "Guide for Developing Security Plans for Information Technology Systems" December 1998 (Marianne Swanson & Barbara Guttman), ". Eight generally accepted principles (see OECD) and "Common IT Security Practices."	http://csrc.nist.gov/publications/nistpubs/index.html www.issa.org/gaisp.html http://web.mit.edu/security/www/gassp1.html	55
GAISP – Generally Accepted Information Security Principles Currently available are the Generally Accepted Systems Security Principles (GASSP) consisting of Pervasive Principles (PP), and Broad Functional Principle (BFP), June, 1999. Detailed Principles are under development (ISSA)	www.issa.org/gaisp.html http://web.mit.edu/security/www/gassp1.html	PP 10 BFP 57
NIST 800-26 Self Assessment Guide for IT Systems	http://csrc.nist.gov/publications/nistpubs/index.html	
NIST 800-27 Engineering Principles for IT Security	http://csrc.nist.gov/publications/nistpubs/index.html	
IFAC International Guidelines on Information Technology Management—Managing Information Technology Planning for Business Impact: International Federation of Accountants, New York, 1999.	www.ifac.org	20
NIST 800-14 Generally Accepted Principles and Practices for Securing IT Systems, 1996	http://csrc.nist.gov/publications/nistpubs/index.html	60
Basel II – The New BASEL Capital Accord – Bank for International Settlements	http://www.bis.org/publ/bcbsca.htm	126
ITU-T X.805 Security Architecture for Systems Providing End-to-end Communications	http://www.itu.int/publications	28
General (not just information) Control Models		
CoCo: Guidance on Control (CICA) 1995	http://www.rmgb.ca/index.cfm/ci_id/3092/la_id/1.htm	32
COSO: Internal Control—Internal Control – Integrated Framework (Treadway Commission) 1994	www.cpa2biz.com/CS2000/Home/default.htm	118
Information Security Mgmt Models – Controls Based		
BS 7799 – Parts 1 & 2, Code of Practice for Information Security Management (British Standards Institute)	www.bsi.org.uk	Part 1, 77 Part 2, 11
CobiT – Control Objectives for Information and Related Technologies (ISACA)	www.isaca.org	148
FISCAM - Federal Information Systems Controls Audit Manual (GAO)	www.gao.gov	
ISO 17799 – Information Technology – Code of Practice for Information Security Management	www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=33441&ICS1=35&ICS2=40&ICS3=	71 English

Trust Services Criteria; formerly SysTrust/WebTrust (AICPA)	www.cpa2biz.com/ResourceCenters/Information+Technology/SysTrust/None_00_aicpaorg_assurance_systrust_index_systrust_in_09914.htm	68
Standard of Good Practice for Information Security (Information Security Forum)	www.isfsecuritystandard.com/index_ie.htm	224
ITCG: Information Technology: Control Guidelines 1998 (CICA)	www.cica.ca	414
ISO TR 13335 "Guidelines for the Management of Information Security", Parts 1-5	www.iso.org/iso/en/StandardsQueryFormHandler.StandardsQueryFormHandler	18, 14, 47, 61, 31
ISO TR 13569 "Banking and Related Financial Services – Information Security Guidelines, 9/9/2003	http://www.iso.org/iso/en/stdsdevelopment/techprog/workprog/TechnicalProgrammeProjectDetailPage.TechnicalProgrammeProjectDetail?csnumber=37245	100
ISO 15408 "Information technology -- Security techniques -- Evaluation criteria for IT security" – aka Common Criteria (available in English only) Part 1: Introduction and general model Part 2: Security functional requirements Part 3: Security assurance requirements		Pt 1: 53 Pt 2: 343 Pt 3: 213
IT Baseline Protection Manual - P BSI 7152 E 1, BSI - Bundesamt für Sicherheit in der Informationstechnik	http://www.bsi.bund.de/gshb/english/menue.htm	1600 in 3 binders
NIST 800-53 - Recommended Security Controls for Federal Info Systems (draft)	http://csrc.nist.gov/publications/nistpubs/index.html	229
NIST 800-12 The Computer Security Handbook, 1995	http://csrc.nist.gov/publications/nistpubs/index.html	
NIST 800-37 Guide for The Security Certification and Accreditation of Federal Information Systems	http://csrc.nist.gov/publications/nistpubs/index.html	55
NIST 800-55 Security Metrics Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/index.html	91
ITU-T X.805 Security Architecture for Systems Providing End-to-end Communications	http://www.itu.int/publications	28
Systems Auditability and Control (SAC) – IIA RF	www.theiia.org/eSAC	1600+
Canadian PIPEDA		
EU Data Protection Directive		
FFIEC		
BITS FRAMEWORK: MANAGING TECHNOLOGY RISK FOR INFORMATION TECHNOLOGY (IT) SERVICE PROVIDER RELATIONSHIPS		
FDA 21 CFR Part 11		
DTI Code of Practice for Information Security Management: Department of Trade and Industry and British Standard Institute. A Code of Practice for Information Security Management, London, 1993, 1995.		
Comprehensive Models – Capability Maturity		
ISO 21827 System Security Engineering Capability Maturity Model		
SSE-CCM: Model Description Document, Version 2.0 April, 1999	http://www.sse-cmm.org/	322

Product Security Models		
ISO 15408 Common Criteria	http://csrc.nist.gov/cc/ccv20/ccv2list.htm	618
Board Governance Guidelines		
Board Briefing on IT Governance (IT Governance Institute)	www.itgi.org http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&CONTENTID=6658&TEMPLATE=/ContentManagement/ContentDisplay.cfm	63
Information Security Governance: Guidance for Boards of Directors and Executive Management", 2001 – IT Governance Institute	www.itgi.org http://www.itgi.org/template_ITGI.cfm?Section=Recent_Publications&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=43&ContentID=6579	28
Information Security Management and Assurance – Three report series from IIA, NACD, CIAO, et al	http://www.theiia.org/esac/index.cfm?fuseaction=or&page=rciap	Rpt 1 – 20 Rpt 2 – 28 Rpt 3 - 66
Information Security Oversight: Essential Board Practices (Nat'l Assoc of Corporate Directors)	http://www.nacdonline.org/publications/pubDetails.asp?pubID=138&user=6158BBEB9D7C4EE0B9E4B98B601E3716	14
Information Security Oversight: How to Reduce the Board's Legal Exposure (NACD)	http://www.nacdonline.org/publications/dmdetails2.asp?dmID=6&user=DE7DA2F9D3C8485A807E0CADC7761E95	10
IT Governance Implementation Guide	http://www.isaca.org/Template.cfm?Section=Browse_By_Topic&Template=/Ecommerce/ProductDisplay.cfm&ProductID=503	58
Turnbull Report - Internal Control - Guidance for Directors on the Combined Code		
Guidelines for Senior Managers		
Common Sense Guide for Senior Managers (Internet Security Alliance)	http://www.isalliance.org	21
Electronic Systems Assurance and Control (eSAC) – IIA RF	www.theiia.org/eSAC	
Building Security in the Digital Resource: An Executive Resource – Business Roundtable, Nov. 2002	www.businessroundtable.org	
Information Security Assurance for Executives: An International Business Commentary on the 2002 OECD Guidelines for the 'Security of Networks and Information Systems: Towards a Culture of Security' - Business Industry Advisory Council/International Chamber of Commerce, April 22, 2003	www.iccwbo.org www.iccwbo.org/home/news_archives/2003/stories/e-tools.asp	
ICC Handbook on Information Security Policy for Small to Medium Enterprises - International Chamber of Commerce, April 11, 2003		
Automated Information Security Program Review Areas – NIST, July 27, 2002		
Corporate Information Security Evaluation for CEO's (TechNet)	www.technet.org/cybersecurity	16

Sector Specific Guidelines		
Electronic Security: Risk Mitigation in Financial IT Transactions - The World Bank, (Thomas Glaessner, Tom Kellermann, and Valerie McNevin), June 2002		
Interim Security Guidelines (NERC)	ftp://ftp.nerc.com/pub/sys/all_updl/standards/Urgent-Req-CyberStnd-3-3121.pdf	
NRIC VI Best Practices for Telecom	http://www.nric.org/	600+ BPs
Legal/Regulatory Requirements		
Sarbanes-Oxley Act (SOX)		
Gramm, Leach, Bliley Act (GLBA)		
Health Information Portability and Accountability Act - HIPAA		
Federal Information Security Management Act of 2002 (FISMA) – U.S. Congress, 2002		
CA SB 1386 (the "You've Been Hacked Act)	http://info.sen.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.html	4
Security Checklists:		
BSA: Mid/Large Businesses Small Businesses Government Agencies Consumers	http://global.bsa.org/usa/policy/security/checklists.phtml	1 each
NIST Security Checklists	http://csrc.nist.gov/checklists	various
NRIC VI Best Practices for Telecom	http://www.nric.org/	600+ BPs
General Management Guides		
CERT Guide to Systems and Network Security Practices (May 2001)		
The 60 Minute Network Security Guide (NSA SNAC)	www.nsa.gov/snac/support/download.htm	35
NIST 800-50 Building an Information Technology Security Awareness and Training Program	http://csrc.nist.gov/publications/nistpubs/index.html	
NIST 800-26 Security Self-Assessment Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/index.html	87
NIST 800-60 Guide for Mapping Types of Information and Information Systems to Security Categories	http://csrc.nist.gov/publications/nistpubs/index.html	
Risk Management Models		
NIST 800-30 Risk Management Guide for Information Technology Systems	http://csrc.nist.gov/publications/nistpubs/index.html	
SEI's OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation)		128
RMI – Risk Measurement Index from the American Security Consortium (work in progress)	Not yet publicly available	
Guides for Home and Individual Users		
Common Sense Guide for Home and Individual Users (Internet Security Alliance)	http://www.isalliance.org	26
StaySafeOnline (FTC/NCSA)	www.staysafeonline.info	

Cyber-Safety for Everyone: From Kids to Elders	http://www2.norwich.edu/mkabay/cyberwatch/cybersafety.pdf	82
Internet & Computer Ethics for Kids: (and Parents & Teachers Who Haven't Got a Clue.)	www.amazon.com	
Top Ten Security Steps for Kids	http://www.iisw.cerias.purdue.edu/k-12/top10_kids.php	
Security Procedures for Educators	http://www.iisw.cerias.purdue.edu/k-12/top10_educators.php	
Higher Education Guides		
EDUCAUSE/Internet2 Effective Security Guide	http://www.educause.edu/security/guide	
Configuration/Patching Guides		
Consensus Benchmarks	www.cisecurity.org	various
DISA Security Technical Implementation Guides	http://csrc.nist.gov/pcig/cig.html	various
NIST Configuration Guides	http://csrc.nist.gov/pcig/cig.html	various
NSA Configuration Guides	www.nsa.gov/snac	various
SANS Step-by Step Guides	https://store.sans.org	various
Vendor Configuration Guides		

Organizations:

AICPA – The American Institute of Certified Public Accountants, www.aicpa.org
ANSI – American National Standards Institute, www.ansi.org
BRT – Business Roundtable, www.businessroundtable.org
BSA – Business Software Alliance, www.bsa.org/usa
BSI – British Standards Institute, www.bsi.org.uk
BSI - Bundesamt für Sicherheit in der Informationstechnik, www.bsi.bund.de
CERT – Computer Emergency Response Team, www.cert.org
CIAO – Critical Infrastructure Assurance Office (formerly U.S. Dept. of Commerce, now IAIP of DHS)
CICA – Canadian Institute of Chartered Accountants www.cica.ca
CIS – The Center for Internet Security, www.cisecurity.org
CMU – Carnegie Mellon University, www.cmu.edu
COSO – Committee of Sponsoring Organizations for the Commission on Fraudulent Financial Reporting (Treadway Commission), www.coso.org
DHS – Department of Homeland Security, www.dhs.gov
DISA - Defense Information Systems Agency, www.disa.mil
GAISPC – Generally Accepted Information Security Principles Committee, www.issa.org/gaisp.html
IAIP – Information Assurance and Infrastructure Protection Directorate of the DHS, (See www.dhs.gov.)
ICC – International Chamber of Commerce, www.iccwbo.org
IFAC – International Federation of Accountants, www.ifac.org
IIA – The Institute of Internal Auditors, Inc. (and IIA Research Foundation), www.TheIIA.org
ISA – Internet Security Alliance, www.isalliance.org
ISACA – The Information Systems Audit and Control Association, www.isaca.org
ISF – Information Security Forum, www.securityforum.org
ISO – International Organization for Standardization, www.iso.org
ISSA – Information Systems Security Association, www.issa.org
NACD – National Association of Corporate Directors, www.nacdonline.org
NERC – North American Electric Reliability Council www.nerc.com
NIST – National Institute of Standards and Technology, www.nist.gov
NRIC – Network Reliability and Interoperability Council, http://www.nric.org/
NSA – National Security Agency, www.nsa.gov
OECD – Organization for Economic Cooperation and Development, www.oecd.org
PCAOB – Public Company Accounting Oversight Board, www.pcaobus.org

SANS – Systems Administration, Audit, and Network Security Institute, www.sans.org
SEC – Securities & Exchange Commission, www.sec.gov
SEI – Carnegie Mellon University Software Engineering Institute, www.sei.cmu.edu
SNAC – Systems and Network Attack Center (NSA), www.nsa.gov/snac

Appendix D

National Cyber Security Partnership
Technical Standards and Common Criteria Task Force

Equipment Deployment & Architecture Guidelines Working Group
RECOMMENDATIONS REPORT

April 19, 2004

TABLE OF CONTENTS

EXECUTIVE SUMMARY

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 in conjunction with the U.S. Department of Homeland Security (DHS), was directed to identify gaps and develop recommendations to promote the adoption and implementation of the President's *National Strategy to Secure Cyberspace*. These recommendations will be presented to the DHS and other stakeholders for consideration in planning next steps.

WORKING GROUP MISSION STATEMENT

To accomplish its goals, the Technical Standards and Common Criteria Task Force established five working groups, each focusing on a specific technical area or challenge. 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.

PROBLEM STATMENT

The other working groups focused on technical security standards for individual, commercial products - from configuration and documentation to deployment, vulnerability testing, certification and maintenance. This working group recognizes that these products do not operate in a vacuum. Technical standards are needed to guide users in deploying products in real and complex architectures.

RECOMMENDATIONS

The Equipment Deployment & Architecture Guidelines Working proposes two recommendations:

Recommendation 1: It is recommended that the industry work together to develop a set of standards for using recommended security equipment as well as best practices for understanding, designing and implementing secured IP network infrastructures.

Recommendation 2: It is recommended that the industry work together to develop a defined set of standards for determining the security level, or security status, of cyberspace.

1.0 TASK FORCE 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 (CC) standard and National Information Assurance Partnership (NIAP) testing program in support of the "NIAP review."

2.0 WORKING GROUP MISSION STATEMENT

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.

3.0 INTRODUCTION

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 in conjunction with the U.S. Department of Homeland Security (DHS) was directed to identify gaps and develop recommendations to promote the adoption and implementation of the President's *National Strategy to Secure Cyberspace*. These recommendations will be presented to the DHS and other stakeholders for consideration in planning next steps.

To accomplish the goals set forth in its Mission Statement, included in Section 1 above, the Technical Standards and Common Criteria Task Force divided its work among six working groups, each focusing on a specific technical area. Each working group was asked to:

1. Identify the current practice and any related works in their respective area of focus;
2. Describe the gaps and challenges facing individuals and organizations today; and
3. Develop actionable recommendations for improvement.

The working groups created by this Task Force include:

- WG1 – Common Configuration
- WG2 – Research
- WG3 – Inventory Awareness Materials[1]
- WG4 – Best Practices for Technical Standards
- WG5 – Equipment Deployment & Architecture Guidelines
- WG6 – Common Criteria, NIAP Review and Metrics

This report focuses on the current practice, gaps and recommendations developed by Working Group 5 – Equipment Deployment & Architecture Guidelines.

4.0 PROBLEM STATEMENT

The other working groups focused on technical security standards for individual, commercial products - from configuration and documentation to deployment, vulnerability testing, certification and maintenance. This working group recognizes that these products do not operate in a vacuum. Technical standards are needed to guide users in deploying products in real and complex architectures.

Cyberspace is a collection of Transmission Control Protocol/Internet Protocol (TCP/IP) network infrastructures. Network infrastructures, in turn, are comprised of individual pieces of equipment. Even when recommended,

[1] The Inventory Awareness Materials Working Group was integrated into the Common Criteria, NIAP Review and Metrics Working Group.

"secure" equipment is used at the 'box,' or device level, it may not be evident to users how to deploy this equipment together in a network in a secure manner.

In addition, there is a need for a method, or process for determining if the charter of the five task forces has been achieved. This means a method of determining, at any given time now or in the future, if a network is actually secure and at what level, or "Defense Condition."

5.0 RECOMMENDATION 1.0 - SECURING NETWORK ARCHITECTURES

It is recommended that the industry work together to develop a set of defined standards for using recommended security equipment, as well as best practices for understanding, designing, and implementing secured IP network infrastructures. Frameworks such as the recent standard ITU-T X.805 *Security architecture for systems providing end-to-end communications* help identify the minimum-security requirements that need to be fulfilled.

This recommendation recognizes that work is being done to improve the process for certifying equipment thru organizations such as the National Institute of Standards and Technology (NIST) with Common Criteria Certifications (CCC), and therefore improving the ability for certain types of IP network security equipment to be selected against a fair comparison of others for a particular security task, or tasks.

This recommendation also recognizes that there is a lack of standards and understanding on the proper use and implementation of recommended and selected security equipment.

This recommendation attempts to draw on the expertise of other Task Force Working Groups such as Task Force 4, Working Group 1, Common Configuration; and Task Force 4, Working Group 4, Best Practices for Technical Standards. Other input and recommended standards are also invited from any source including other standards organizations such as NIST, the International Telecommunication Union (ITU), the 3rd Generation Partnership Project (3GPP), 3GPP2, the European Telecommunications Standards Institute (ETSI), the Internet Engineering Task Force (IETF), and the Telecommunications Industry Association (TIA).

To accompany this recommendation, a starting point is supplied for consideration in the development of new standards. Specifics can be found in the "Reference" section of this paper under "Security Network Architectures."

Recommendation 1.1 – Security is a Philosophy: It is recommended that discussion of "security as a philosophy" be further developed and expanded so that industry may gain a more complete understanding of security. This topic is more complex than many realize. Creating a completely secure IP network calls for more than good equipment and a secure architecture; it calls for an understanding of its users and its business practices.

Details can be found in the "Reference" section of this paper under "Security is a Philosophy."

Recommendation 1.2: - Network Security-Specific Resources: It is recommended that the following list of IP network security-specific resources be utilized and expanded upon as a reference for determining the types of equipment and functions required for implementing and planning a secure IP network infrastructure.

It is also recommended that this list be expanded upon and continually updated, as technology and security devices and services are continually being improved, and introduced:

- Firewalls
- Network Address Translation (NAT)
- Authentication Systems
- Intrusion Detection Systems (IDS)
  - Network Based
  - Host Based
- Intrusion Prevention Systems (IPS)
- Encryption
- Host Based / Gateway Anti-Virus

Details can be found in the "Reference" section of this paper under "Network Security Specific Resources."

Recommendation 1.2.1 –Network Security-Specific Resource Requirements: The devices selected in recommendation 1.3 by any given individual, or organization for security use in an IP infrastructure should meet all the requirements and be selected in accordance with the findings of

Task Force 4 equipment recommendations, including basic system hardening and configuration as outlined by Task Force 4 Working Group 1 (Common Configuration).

Recommendation 1.3 – Network Security Auditing: It is recommended that a method or process for determining the importance of individual network devices, elements, services, and/or equipment be developed so that a proper level of security can be established for each resource in the network infrastructure.

It is currently recommended that the NIST FIPS PUB 199 (Standards for Security Categorization of Federal Information and Information Systems) be used as either the recommended method of categorizing information systems, or that it be used as a starting point for developing a categorization system for auditing network security. Additional information on other aspects of security auditing can be found in the "Reference" section of this paper under "Network Security Auditing."

Additional input on prioritizing systems, functions, or services for determining security requirements is required as there are many different methods and viewpoints on what is considered important or critical. These viewpoints may be dependant upon the infrastructure owners' use of the network.

Recommendation 1.4 – Planning Security Domains, De-Militarized Zones (DMZ's), and other applicable perimeter security measures: It is recommended that all network architectures be planned and implemented in a secure manner. To accompany this recommendation, we suggest several possible layouts, or topologies that utilize recommended equipment and practices to secure infrastructures against illegal or unintentional penetration, or attack. The use of techniques such as DMZ's, defense-in-depth, and restricted directional communications combined with the proper use of recommended equipment and best practices, can be used to create a secured IP architecture. It is recognized that not all network infrastructures may be suitable for protection via security domains and DMZ's; therefore additional research should be conducted and recommendations should be developed to accommodate network architectures that are not suitable for protection via these discussed techniques.

Details can be found in the "Reference" section of this paper under "Planning Security Domains, De-Militarized Zones, and other applicable perimeter security measures."

It is also recommended that ongoing research in to these types of security deployment scenarios and their benefits become a regular event so that standards may be properly updated as security technology evolves. The industry as well as organizations, such as NIST, ITU, 3GPP, 3GPP2, ETSI, and TIA for example; should update relevant standards and proposed standards such as this one, to constantly include new security advancements in technology, or technology based security layouts and tactics.

6.0 RECOMMENDATION 2.0 – SECURING CYBERSPACE

It is recommended that the industry work together to develop a defined set of standards for determining the security level or security status of cyberspace.

This recommendation recognizes that it is the charter of the five (5) task forces to put together standards and practices that facilitate the securing of cyberspace. There is currently no work on a method or process of determining how well these proposed standards and recommendations are working as they relate to the current or ongoing security of cyberspace. These recommendations attempt to offer a proposed solution that provides a useable feedback mechanism.

This recommendation attempts to draw on the expertise of other Task Force Working Groups such as Task Force 4, Working Group 1, Common Configuration; Task Force 4, Working Group 4, Best Practices for Technical Standards, and Task Force 2, Early Warning. Other input and recommended standards are also invited from any source including other standards organizations such as NIST, ITU, 3GPP, 3GPP2, ETSI, IETF, and TIA.

A starting point for this recommendation can be found in the "Reference" section of this paper under "Securing Cyberspace."

Recommendation 2.1 – Grading the Security of Individual Network Infrastructures: It is recommended that a feedback mechanism be created to test and rate, or grade the security and practices of individual networks and their operators.

Two ideas are proposed here. Either, or both may be utilized. It is recommended that a set of criteria be established and then utilized in either of both of the two methods.

First, the recommended criteria may be created and made available to everyone participating in 'cyberspace' with the intent that the 'Cyberspace Sector' (everyone participating in cyberspace, financial, residential, commercial, etc.) be self-policing and constantly continuing to improve upon its own performance and security for the benefit of the whole. A standards body (similar to any other) should be created to oversee the current and ongoing recommendations in this area.

Second, the recommended criteria may be created and made available to a created independent organization that is responsible for determining the overall security of cyberspace on a network-by-network basis. This independent organization is not intended to be a government institution or a body with any limiting powers. It is simply intended to be a clearinghouse for gathering statistics, providing rating, and sending out feedback, that assists in determining the overall and ongoing security of cyberspace.

This independent organization, and/or standards body should be composed of personnel from all sectors of cyberspace, similar to any other standards body, and be responsible for defining, managing, updating, and executing this testing and rating system for determining the ongoing security level of cyberspace.

Details can be found in the "Reference" section of this paper under "Grading the Security of Individual Network Infrastructures."

Recommendation 2.2 – Security Classifications or 'DefCon' Levels: It is recommended that a series of grades, or classifications, be developed that can be used to determine the level, or amount of security (Defense condition) an individual network has, or maintains. These security classifications state the tested networks ability to repel, or defend against illegal, or unwanted intrusions and attacks. These classifications are ultimately used to grade the overall level of security of cyberspace, since cyberspace is a collection of individual networks.

Currently there are five (5) proposed classification levels. Details can be found in the "Reference" section of this paper under "Security Classifications or 'DefCon' Levels."

It is also recommended that further development of these testing procedures be developed by organizations, such as NIST, ITU, 3GPP, 3GPP2, ETSI, and TIA for example; so that the resulting guidelines will be able to serve as a more complete model to determine the actual level of security of cyberspace.

Recommendation 2.2.1 - Security Classifications or 'DefCon' Levels Requirements: It is recommended that these classification levels include the guidelines and recommendations of Task Force 4, Working Group 1, Common Configuration and Task Force 2, Early Warning where appropriate.

Details can be found in the "Reference" section of this paper under "Security Classifications or 'DefCon' Levels."

7.0 REFERENCE – RECOMMENDATION 1.X

7.1 Introduction

One of the purposes of this paper is to propose recommendations and guidelines in architecting secure network infrastructures in which recommended security equipment and components are deployed.

The initial task discussed here is to suggest initial seed ideas to be used by the security community to develop guidelines in architecting secure network infrastructures in which recommended security equipment and components are deployed. As these are developed, fleshed out, and subject to peer review, the resulting guidelines will be able to serve as a generic base reference model for creating a secure network topology. Our initial suggestions, which follow, are intended to be generic to most types of network topologies without respect to their individual purposes, functionalities, or intended operations.

Note: There are additional security precautions that may be put into place that may be dependent upon a networks specific purpose; for example, banking, education, and ISP specific networks. These purpose specific precautions, as well as protocol level security issues, are outside the scope of this paper.

Reference material on design and implementation of network architectures in a secure method is typically a difficult task and not readily available to the public. There is an abundance of information available on specific components used to secure networks, such as firewalls and IDSs. There is ample information available, and best practices for these common systems to secure existing networks. The dilemma is that there is little availability of information on how to architect a communications infrastructure from the ground up so that the given infrastructure is inherently more secure from the start than a network that is backward engineered with firewalls and IDS added to plug holes that are later found after the infrastructure has been compromised.

This paper endeavors to educate the reader on how to engineer an IP communications infrastructure that, by its very nature of the architecture and layout, is inherently more secure than most networks today that have security added as an afterthought. Total security is something that must be designed into the very foundation of the network architecture and not something that is thrown on after the fact. This is not to say that existing networks cannot be secure, this is simply stating that there are architectural issues to consider in creating secure networks, and that these issues are applicable to both existing and planned infrastructures.

Following is discussion, and some basic architectural lessons and recommendations (in an informal whitepaper format) on two of the most commonly overlooked and least publicly understood issues facing network security. They are the ‘Human Firewall’ and secure architectural design.

7.2 Security is a Philosophy

One of the most important things to remember about security, all security, regardless of whether were securing a network infrastructure or a house, is that security is not a ‘box’ that you purchase, it’s a philosophy, a way of doing things, and to some extent it’s also a way of life. When securing anything, specifically a network infrastructure, it’s important to know how to implement security practices and equipment (boxes). If implemented improperly, even the best designed security boxes, or devices, can be rendered useless.

The Human Firewall

In keeping with the idea that security is a philosophy we also have to understand that like philosophy, security comes in layers. When properly layered, each of these layers reinforces the others; and compromise of one layer does not compromise the other layers. One aspect, or layer of security that is overlooked is what is sometimes referred to as the ‘Human Firewall’. Much like the hardware version of the firewall that protects networks today, the human firewall is also intended to block improper information flow.

This improper information flow can come in many forms, and is typically the result of human behavior. The most common forms of information leaks that result in information being revealed that attackers can use to penetrate networks come from:

- Support web sites: Knowledge-base type articles that are intended to allow customers to service themselves with network access problems. These sources of information can sometimes provide key information such as IP addresses, vendor equipment types, and configurations that can give hackers just the bit of information they need to take advantage of a known, or even un-known weakness in the sought after infrastructure.

- Phone-based tech support personnel: The same issues apply here as with support web sites with some possible additional security issues. Phone-based support personnel are in the business of helping people resolve some technical issue, a lot of the time these support personnel do not actually know the people they are talking to, this creates a personnel authentication issue. There have been many instances in corporate history where a hacker has simply placed a phone call to a corporate help desk acting as though he or she is a new employee, or newly hired consultant and for some reason has not yet been given access to the network and must have access to get a newly assigned project completed. In the spirit of assisting, as help desk do, access is often granted to someone unknown by assigning him or her a username and password. This is the ultimate form of hacking: the 'human firewall.'

- Press Releases: Often times a service provider, whether it's a Telco, or a bank offering new on line services, will make it publicly known that they have just finished implementing a public, or publicly accessible infrastructure. Often times as part of a joint marketing venture between the purchaser, and the supplying vendor, a press release will be sent out stating the availability of this new infrastructure and that the equipment is supplied by vendor X and utilizes the vendors new whiz-bang XXXX model products capable of offering XXX services. This is information that is valuable to hackers, as this information details the equipment used, how it's used in a general sense, and the fact that it's new brings the possibility that there are unknown and yet unfixed security vulnerabilities just waiting to be exploited.

These are just a few examples of ways that seemingly innocent information and people can be taken advantage of in ways that are not typically considered when laying out security policies and practices within an organization. As we mentioned before, security comes in layers, and the human layer is often the most important and the most overlooked.

Human security specifically, is outside the scope of this papers expertise. The above description, and discussion is supplied solely for information reasons to present one of the most commonly overlooked and important security vulnerabilities. 'Human Firewall' security will not be covered in any detail in the remainder of this paper.

7.3 Network Security-Specific Resources

The following is a listing of and definition of the most commonly used, and new IP networking security-specific tools, or resources. These resources are defined here, and later discussed as to their proper placement and use in securing most common IP network infrastructures.

- Firewalls
- Network Address Translation (NAT)
- Authentication Systems
- Intrusion Detection Systems (IDS)
  - Network Based
  - Host Based
- Intrusion Prevention Systems (IPS)
- Encryption
- Host Based / Gateway Anti-Virus

Firewalls

A firewall is a combination of hardware and software used to implement a security policy governing the network traffic between two or more networks. A network firewall serves as a primary line of defense against external threats to an organization's computer systems, networks, and critical information. Because the firewall is a primary line of defense, the administration of this system must be carefully scrutinized. Segregation of duties, logging, auditing, and change control processes must be in place and continuously reviewed.

There are three firewall types. In order of increasing security, they are:

- Packet Filtering Routers/Firewalls –Restricts network traffic by looking at the sources and destinations of individual network packets. There is no consideration of packet content or authorized use. Basic packet filtering can be implemented on many network routers, most commonly known as Access Control Lists (ACL). An enhancement to basic packet filtering is stateful inspection. This technology keeps tracks of "conversations" outside is in response to traffic from the inside.

- Proxy/Circuit Level Gateway Firewalls –Acts as an intermediary for user requests at the connection level by requiring each user to first connect to the firewall. The firewall then establishes a second connection to the user's final destination.

- Application Proxy Firewalls –Extends the concept of Proxy/Circuit Level Gateway firewalls to the application level. Each application proxy inspects the traffic it is relaying to ensure that it conforms to that particular application's protocol. For example, an FTP application proxy examines the user's requests to verify conformance to the FTP protocol specification.

There are also hybrids of these technologies available, for example, a firewall that uses stateful inspection in combination with application proxies.

Proxy/circuit level gateways and application proxy firewalls may also require individual users to authenticate themselves (e.g., with a password) to the firewall before they establish the connection to the final destination. In addition, some firewall vendors offer hardened or secure operating systems as their firewall platform. These features can, in some circumstances, provide an even greater level of security and better protect the firewall should a security breach occur.

Regardless of the type of firewall selected, the controls it should implement are basically the same:

- Permitted Services - The services allowed to traverse the firewall should be restricted to the smallest set required to implement the particular application or function. This restriction should be applied separately for each of the networks that the firewall interconnects.

- Restricted Communications Flow - The direction of communications should be restricted and controlled between the networks the firewall interconnects. As a result, a clearly defined and limited communication trust model can be documented and monitored. For example, while it may be necessary for internal systems to initiate connections with a server on a DMZ network, it should never be necessary for a server residing on a DMZ network to initiate connections with internal systems. Therefore, the firewall should not permit such connections. As a result, if an attack occurs, the scope of the attack is limited to the networks and systems controlled within this trust model.

- Access Control - The particular set of systems or users allowed to use each service should also be restricted. For example, access to a database server on a DMZ network should be restricted to a) the web servers that retrieve information from the database and b) the internal system(s) used by the database administrator(s).

- Control Messages –To make it more difficult to scan the firewall and determine what protocols may pass through it, the firewall should not return any protocol control messages such as "host unreachable," "port unavailable," "time exceeded," etc.

- Network Address Translation (NAT) – described below.

Network Address Translation (NAT)
NAT allows internal network topology and addressing to be hidden from external users by using one set of addresses to access the external network, a different set of addresses to access the internal network, and a mapping between the two.

Authentication Systems

Authentication provides a means for identifying an object (e.g., user, application, system, etc.). As a result, the object can then be granted access to only those services it requires and its activities can be monitored. A variety of authentication mechanisms are available, ranging from simple password-based systems to token-based systems and biometrics. The particular authentication technology selected is dependent upon the classification assigned to the data, system, or network. For example, as a primary line of defense, a firewall would be classified as critical. Therefore, minimally, a token-based system should be used to authenticate with administrator privileges to the firewall.

In addition, an organization may extend the authentication mechanism to ensure that a particular transaction(s) can be traced back to a particular user (e.g., brokerage transactions). This is commonly known as providing non-repudiation capabilities.

The most common authentication protocols used are:

- Remote Authentication Dial-in User Service (RADIUS)
- Kerberos
- Lightweight Directory Access Protocol (LDAP)
- Windows NT Domain Services
- Novell EDS
- Windows Active Directory

Intrusion Detection Systems (IDS)

IDSs search for signs of unauthorized access or use. Network-based intrusion detection examines the types and contents of network packets; host-based intrusion detection examines system audit trails and activity logs. Unauthorized access and use can be detected in one of two ways: misuse detection searches for known attack "signatures," much in the same way that anti-virus software searches for viruses; anomaly detection searches for unusual behavior based on profiles of expected user and application activity. Network-based IDS has the advantage of being able to monitor and alert on attacks of all systems on an entire network segment. This capability generally makes network-based IDS easier and less expensive to deploy. However, network-based IDS's are limited because it cannot "see" what is happening on individual hosts. For this reason, a complete implementation will make use of both network-based and host-based solutions.

Network-Based IDS: An IDS should be deployed on each DMZ network, extranet segments, as well as on the internal network segment that is connected to the firewall. Optionally, an IDS may also be deployed on the "Internet side" of the firewall; however, this system must be carefully configured to avoid unnecessary alarms.

In all cases, the IDS should be configured with two network interfaces: one for receiving traffic to be analyzed and the other for reporting alarms to an IDS management console(s). The interface used for receiving traffic should be configured without a network address (in what is known as "stealth mode"), making it almost impossible for attackers to identify its location or existence.

For IDSs that are monitoring the activity of external networks (e.g., DMZs), the reporting interface should be connected to an isolated IDS segment, and communication between the IDS and IDS management console(s) must be controlled by the firewall. This approach has several benefits and should hold true with all security systems management interfaces. First, it uses the firewall to restrict access to the IDSs. Secondly, it improves the performance of the IDS' analysis and reporting functions by segregating these duties between the two interfaces. Thirdly, keeping IDS traffic on a separate network avoids any reduction in available bandwidth afforded to the Public and Private DMZs. Finally, because the IDS traffic is flowing on separate network, it will not be interrupted should a bandwidth-consuming denial of service attack be directed at the Public DMZ.

Like the IDSs deployed for external network monitoring, IDSs that are monitoring internal networks require segregation of receiving and transmitting interfaces. An organization can use the same architecture as described above, if desired. An alternative is to have the reporting interface connected to the internal network, but internal switching and routing would restrict access.

In either case, the communication between the IDS and the management console(s) must be strongly authenticated and encrypted. In addition, the system clocks of all systems that are monitored or play a role in the monitoring of intrusions (e.g., IDS, management consoles, firewalls, routers, DMZ systems, etc.) should be synchronized to a common time to allow for correlation and auditability of log data from multiple systems. This configuration may require the installation of an additional network interface on the firewall and/or additional firewalls/ routers.

Host-Based IDS: Host-based IDS should be deployed on all critical systems. In order for host-based intrusion detection to function effectively, these systems must be configured to enable full auditing and activity logging. This may require that the systems be configured with additional memory and/or disk space to avoid adversely impacting their performance. All IDS data and management must be strongly encrypted and authenticated.

Host-based security specifically is outside the scope of this papers expertise. The above brief description is supplied solely for information reasons to present all usable resources. Host based security will not be covered in any detail in the remainder of this paper.

Intrusion Prevention Systems (IPS)

Intrusion Prevention is quickly becoming the newest security resource, and the 'next generation' firewall technology so to speak. Intrusion prevention, in essence, combines the abilities of firewalls and IDS. IPSs typically sit in-line in the main traffic stream in a similar fashion to firewalls. IPSs perform most if not all functions a firewall performs as far as managing traffic that flows through it. Intrusion prevention takes firewalling a step farther by also being capable of mitigating several types of intrusions or penetration attempts that standard firewalls cannot detect. Also, IPSs look for incorrect, or non-typical behavior in traffic patterns and take action appropriately to protect the network.

Some IPSs are designed in a manner that allow them to be placed outside the network they are protecting in a manner that does not interfere with traffic routing, or addressing, since the IPS device is not detectable in the infrastructure and does not participate in network activities the way a normal firewall or proxy device would.

Encryption

Encryption is an essential part of security and should be implemented wherever confidentiality is a concern. However, in many cases, encryption only protects the data while it is in transit. A more secure implementation would also encrypt the data once it is stored at its final destination.

Encryption specifically is outside the scope of this papers expertise. The above brief description is supplied solely for information reasons to present all usable resources. Encryption based security will not be covered in any detail in the remainder of this paper.

Host based / Gateway Anti-Virus

Anti-virus software should be implemented on all desktops or email servers and should be updated regularly for the latest signatures. Additionally, given the number of users within any network that have external POP email addresses, such as Yahoo or Hotmail, organizations have begun to deploy gateway anti-virus solutions that could otherwise bypass the email server.

Anti-virus, specifically for email security, is outside of the scope of this paper. The above brief description is supplied solely for information reasons to present all usable resources. Anti-virus will not be covered in any detail in the remainder of this paper.

7.4 Network Security Auditing

The first step in creating a secure IP architecture is to know and understand what you're securing. This may sound trivial, but you can't secure what you don't understand. Every resource that is a part of, or is connected to, the network must be analyzed and categorized so that they may be properly laid-out, accounted for, and architected into the security scheme.

Prioritizing Systems
These network resources, as mentioned above, may follow under the headings of:

- Servers
  - Web-based publicly accessible (i.e., extranet, services, etc.)
  - Web-based internally accessible (i.e., intranet)
  - Application-based publicly accessible (i.e., on-line banking)
  - Application-based internally accessible (i.e., Corporate email)
- Databases
  - Publicly accessible (i.e., on-line bill retrieval)
  - Internally accessible (i.e., customer database)
- Network Management Systems (NMS) (incl. servers/databases, non-security related)
- Networking Equipment (switches, routers, etc., non-security related)

The list of resources generated and categorized by a close examination of each networks individual use, or service requirements should then be cross-referenced by three additional topics:

- Accessibility – How accessible does this specific resource need to be, and who will be accessing it? Is this resource to be publicly accessible, or only privately accessible?
- Functionality – What purpose does this resource serve? How critical is it to the overall service offering of the network infrastructure?
- Vulnerability – How vulnerable is this resource? Is this vulnerability acceptable given its function? How replaceable is this resource?

7.5 Planning Security Domains, De-Militarized Zones (DMZ's), and other applicable perimeter security measures

The second step in creating a secure IP architecture is plan out your security zones. This is done using the matrix created by the network resource audit described above with modifications for geographical, departmental, financial, and/or political issues.

In most situations one DMZ, or security domain, should be implemented in the network infrastructure. This DMZ should be positioned between the trusted (internal) network and the untrusted (typically the Internet) network. Typically this initial DMZ will contain only resources that are required to be publicly available, such as web servers, mail servers, and domain name servers (DNS).

Given the specific functions and services that may be offered and required by different networks, it may be desirable to create two or even three security domains to provide maximum protection to all resources. Each set of systems or applications that require different levels of accessibility, or access requirements should be implemented in its own DMZ or security domain. Subnets work best to separate different security zones with security-specific equipment demarking each zone. Each security zone may also be set up with individual subnets according to function. Having FTP servers on one subnet and restricting that subnet to FTP traffic only, and web servers on another subnet while restricting that subnet to HTTP traffic only, in the same DMZ is a good way to be sure that any FTP weaknesses aren't used to exploit your web servers.

Another suggestion is to place similar equipment or resources on common switches divided by virtual local area networks (VLAN). For example, place untrusted subnets or zones on the untrusted switch, DMZ resources on the DMZ switch, and trusted internal resources on the internal switch. Cabling from each of these specific switches, or VLANS should be running to security specific demarcation equipment such as firewalls, or IPSs.

Architectural Design
The reference diagram below details one possible architectural deployment scenario designed to provide a light to moderate level of network security. Note that there are many other areas that can be addressed to enhance security such as deploying Host-Based Intrusion Detection, Virus Scanning gateways, and proxy servers. These additional security measures, or layers, are outside the scope of this paper as we are concentrating on the secure architectural layout of networking infrastructures at a higher level.

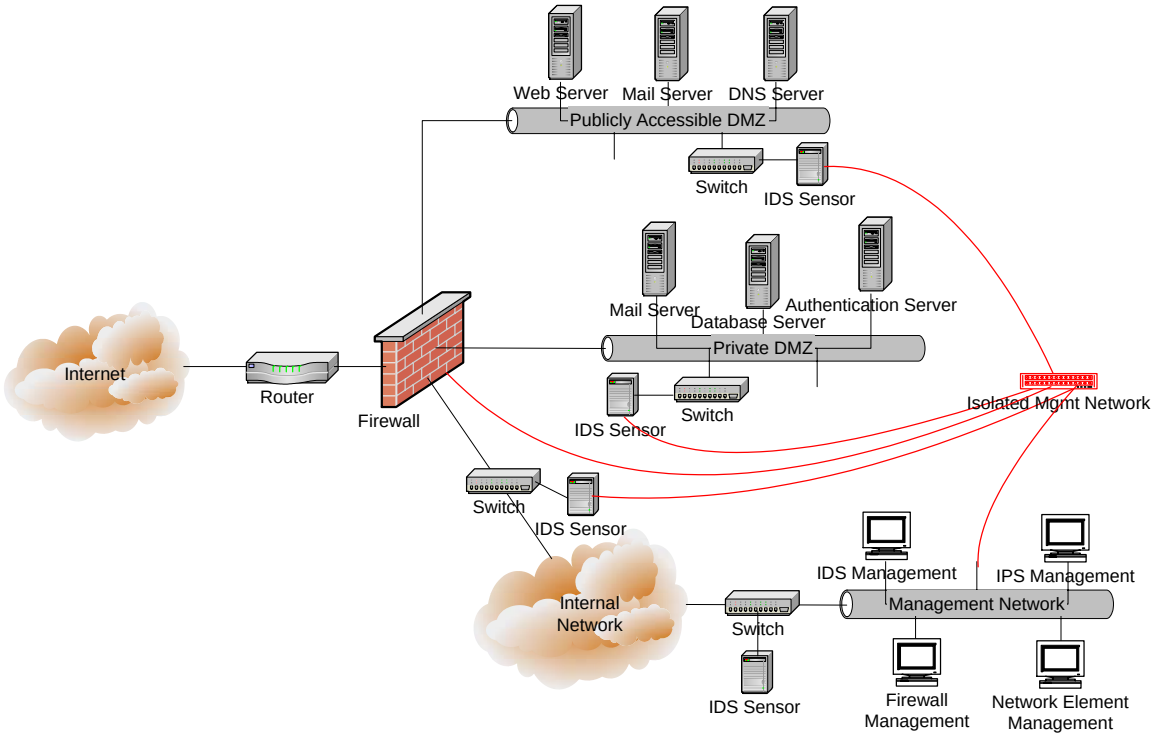

Figure 1: Architectural Deployment Scenario

This reference network does not take into consideration equipment redundancy, or additional equipment for load sharing, or performance issues. Adjustments may be made accordingly.

Note: This and the following diagrams also show two mail servers. Two mail servers are not normally the case in a standard network deployment. The placement of the actual mail server in real deployment would be at the discretion of the security architect. Since the mail server serves as both a publicly- and privately-accessible device, placement of the mail server in one DMZ or the other is not mandatory, but must reside within a DMZ. One thought is that by placing the mail server in the private DMZ, the internal company could continue to run if the public DMZ was compromised and brought down by an attack or other destructive event.

This network employs a standard firewall for external protection between the trusted and untrusted (Internet) network IDS sensors are used to monitor and detect attacks and improper traffic behavior should an attack make it past the firewall or if an attack should be generated from inside the trusted network. Each of these security zones is attached to an individual port of the main firewall.

Three different security zones are configured in this scenario:

- A publicly-accessible DMZ
- A Private DMZ
- Internal network / Management Network

Connections from hosts from the Internet are controlled as follows:

- Hosts on the Internet may initiate connections to the servers on the Public DMZ using only those protocols needed by the particular application(s) offered. For example, the Web server may only be reached with valid HTTP and SSL requests, the mail server may only be reached with valid SMTP requests, and the Name server may only be reached with valid DNS queries.

- Access to any other network in the architecture is prohibited.

- Hosts on the Public DMZ are permitted to initiate connections to hosts on the Private DMZ. Again, these connections are restricted to only the particular hosts and protocols required.

- Hosts on the internal network may initiate connections to the servers on the Public DMZ using required protocols and the protocols necessary to administer the servers. Access using administrative protocols is limited to the particular systems used to perform administrative functions (e.g., the Web server may only be accessed by the Web administrator's system, the mail server may only be accessed by the mail administrator's system, etc.)

- No connections may be initiated from this network directed to the internal network.

Connections to and from the Private DMZ network are controlled as follows:

- No connections may be initiated from the Internet/extranet to the Private DMZ.

- Hosts on the Public DMZ are permitted to initiate connections to hosts on the Private DMZ. These connections are restricted to only the particular hosts and required protocols.

- Hosts on the internal network may only initiate connections to the private DMZ for administrative purposes. Access using administrative protocols is limited to the particular systems used to perform administrative functions (e.g., the database administrator is permitted to perform maintenance and administration and the primary database server can perform data uploads and downloads).

- No connections may be initiated from this network directed to the internal network.

- Connections to and from the isolated Management network are controlled as follows:

- No connections may be initiated from the Internet, Public DMZ, or the Private DMZ to the isolated IDS segment. However, if the monitoring of the IDSs is outsourced, authenticated, encrypted, and restricted to a specified IDS management console, then connections may be allowed and initiated from the outsource company to the isolated segment.

- Depending on the alerting mechanism, the isolated IDS segment may initiate connections with the Public DMZ (e.g., the mail server) for the purpose of intrusion alerts (e.g., email/ pager).

- No connections may be initiated from this network directed to the internal network.

- Connections to and from the internal network are controlled as follows:

- No external network (including the Internet, Public DMZ, Private DMZ, or isolated IDS segment) may initiate connections directed to the internal network.

- The internal network may initiate connections to any external network. However, this access should be limited to the particular systems and protocols necessary to perform a specified function.

- The firewall should perform NAT for all networks it inter-connects. Other than as described in this section, all connections traversing the firewall are prohibited using the firewall strategy commonly referred to as "that which is not expressly permitted, is denied."

<u>The Public DMZ</u>

Each application provided to the public is implemented on a separate server attached to the DMZ. This segregation of duties limits the amount of damage and disruption that can be caused by a security breach. It also allows the configuration of the privileges on each server to be as restrictive as possible. This includes configuring each server to only accept connections that are required for the particular application they offer.

Each server on the Public DMZ should implement full auditing and activity logging. If possible, a dedicated log server on the internal network should retrieve logs from these systems in a timely manner. This log server protects

the logs from unauthorized modification and/or deletion. In addition, each host should run system-level vulnerability assessment and host-based intrusion detection applications. The data generated by these applications should be encrypted to ensure confidentiality and employ strong authentication to mitigate the risk of forgery.

Hosts on the Public DMZ should not be permitted to establish connections to the internal network. Therefore, all system administration, security management activities, and data transfers should be initiated from the internal network. This includes, but is not limited to, Web content changes, invocation of assessment tools, retrieving assessment data, retrieving log data, and host-based intrusion alarms.

Because the servers on the Public DMZ are accessible to the public, it should be assumed that they are likely to be attacked. Therefore, these systems should only contain data that originates from systems not on the Public DMZ.

The Private DMZ

Each application provided to the hosts on the Public DMZ must be implemented on a separate server attached to the Private DMZ. This segregation of duties limits the amount of damage and disruption that can be caused by a security breach. It also allows the configuration of the privileges on each server to be as restrictive as possible. This segregation includes configuring each server to only accept connections that are required for the particular application they offer.

Each server on the Private DMZ should implement full auditing and activity logging. If possible, a dedicated log server on the internal network should retrieve logs from these systems in a timely manner. This log server protects the logs from unauthorized modification and/or deletion. In addition, each host should run system-level vulnerability assessment and host-based intrusion detection applications. The data generated by these applications should be encrypted to ensure confidentiality and employ strong authentication to mitigate the risk of forgery.

Hosts on the Private DMZ should not be permitted to establish connections to the internal network. Therefore, all system administration, security management activities and data transfers should be initiated from the internal network. This includes, but is not limited to, database changes, invocation of assessment tools, retrieving assessment data, retrieving log data, and host-based intrusion alarms.

The Isolated Management Network

The isolated segment provides for secure and controlled communication between all security systems and its associated management console. Essentially, this is an additional external network that is connected and controlled independently by security administrators, accessed only by security administrators.

Each IDS or security device should be configured with at least two network interfaces: one for receiving traffic to be analyzed and the other for reporting alarms to a management console(s). The interface used for receiving traffic should be configured without a network address (“stealth mode”), making it almost impossible for attackers to identify its location or existence.

The reporting interface should be connected to this isolated IDS segment for the purpose of communicating only with the associated management console. This communication should employ strong authentication and encryption (e.g., point-to-point encryption with public -private key authentication) to mitigate the risk of forgery. This protection has several benefits. First, it allows the act of segmenting the network to restrict access to the IDS, allowing communication from only the associated management console(s). Secondly, it improves the performance of the IDS’ analysis and reporting functions by segregating these duties between the two interfaces. Thirdly, keeping IDS traffic on a separate network avoids consuming bandwidth in the Public and Private DMZs. Finally, because the IDS traffic is flowing on separate network, it will not interrupted should a bandwidth-consuming denial of service attack be directed at the Public DMZ.

The Internal Network

The firewall should restrict all external systems (e.g., the DMZ networks and the isolated IDS segment) from initiating connections with the internal network. The internal network may initiate connections with these external networks as described in previous sections. Additionally, a network-based intrusion detection sensor should also be deployed on the internal network segment that is connected to the firewall (also with a stealth mode interface). This sensor provides “last-resort” monitoring for any inappropriate traffic entering through the firewall, as well as for

traffic leaving the internal network. A filtering router should be used to limit access to the sensor's alarms/administration interface; only the IDS Management console(s) should have access to the sensor. Within the internal network, all IDS and Security Management Consoles should reside on a dedicated network segment(s). Access to this segment should be restricted to appropriate personnel/systems using firewalls or filtering routers and strong authentication.

7.6 Additional Architectural Security Options

Below are some additional architectural diagrams displaying other options for architecting networks in a secure manner in the order of increasing security. The above diagram is representative of a star, or spoke and hub configuration, of laying out a secure network infrastructure. Other options such as the 'layered' approach are also available.

Inherently the 'layered' approach tends to be more secure, as the infrastructure is created in layers that must be penetrated in order to reach the internal network segment, as opposed to the spoke and hub approach which places each network segment at equal distance from the untrusted perimeter.

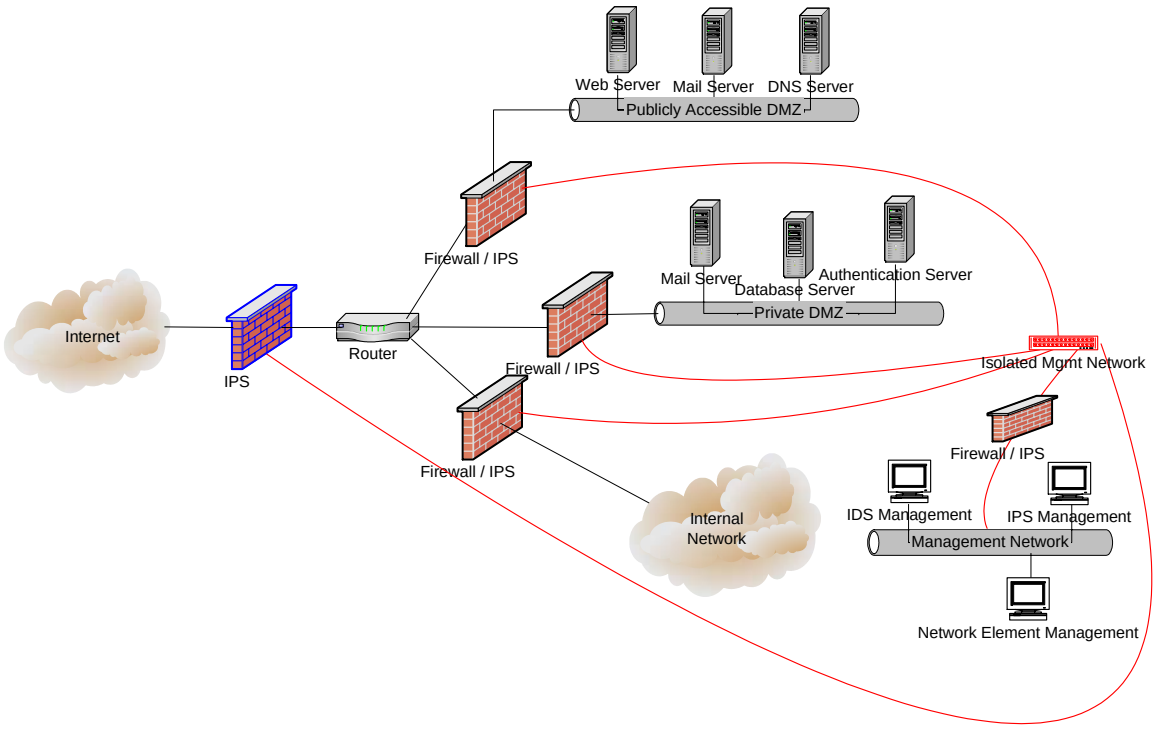

Figure 2: Spoke and Hub 'Heavy' Security Architecture

This star, or spoke and hub approach, is built in a manner that offers heavy security as opposed to the previously shown configuration that offers light to medium security. The major differences here are that IPSs may be utilized with, or in place of Firewalls. Some IPSs may also be deployed 'outside' the network in front of the main router and they operate in-line invisible, and undetectable.

Inside the network, additional IPSs or firewalls may be used to segment off each security zone independently. Also, not that there is no direct connection from the internal network to the management network, and also note the additional firewall or IPS that is present on the management network. This created additional security for the all-important management network as it is now completely stand-alone, and contains it's own protection.

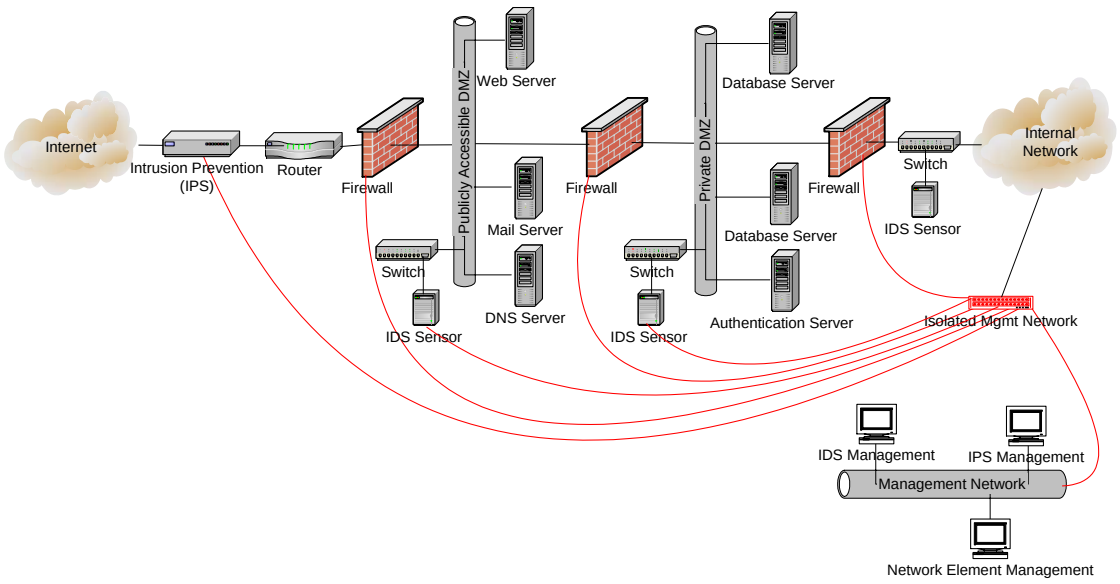

Figure 3: Layered 'Light to Medium' Security Architecture

The above 'layered' security approach is inherently more secure that the spoke and hub architecture in that it places each network in-line and therefore the most sensitive network is protected behind one or more additional networks. Instead of each network being placed equal distance from the untrusted perimeter as with spoke and hub architectures, the more sensitive, or important networks, are hidden behind the other less important networks.

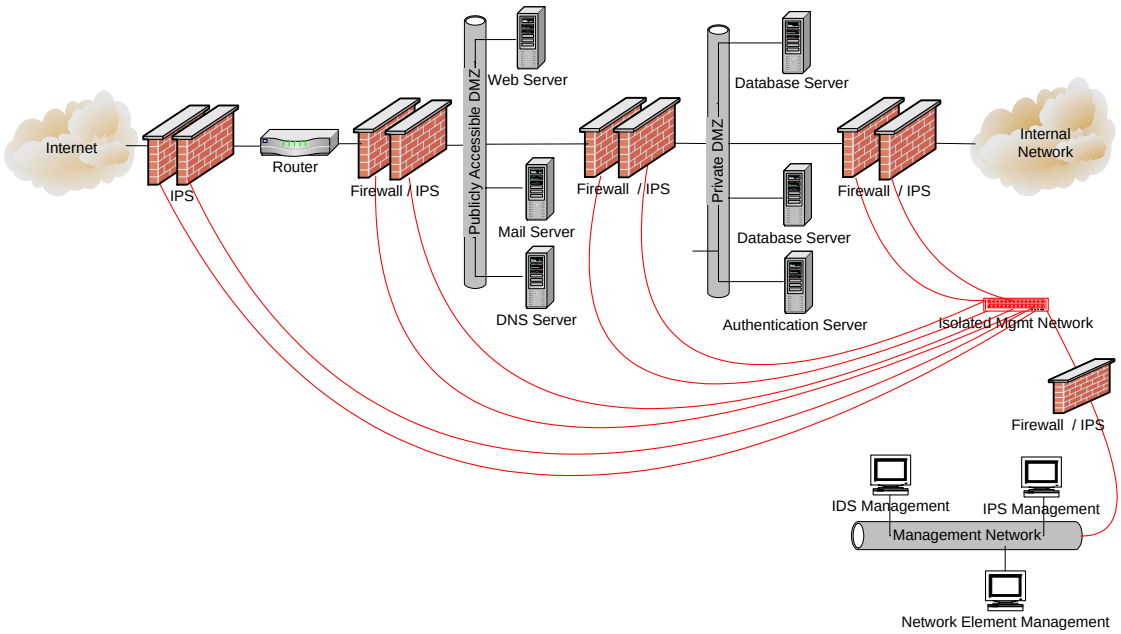

Figure 4: Layered 'Heavy' Security Architecture

This layered approach may be considered the most secure of all shown approaches. Not only does this approach utilize the layering method of security architecture, but also it utilizes multiple firewall or IDSs at each segment or security boundary.

The best approach to this method is to use multiple devices, one firewall and one IPS, or two IPSs at each boundary with each device at the given boundary utilizing a different operating system, and security software load. This method ensures that a security weaknesses in one operating system, or security software load, will not likely not be an issue in the next device in line since the next device will utilize a different operating system, and security software load.

As a final note, be sure that all unused and unneeded ports and services in each security device is disabled, and/or removed or uninstalled. Also, security systems, like all other systems, should always be kept up to date with the latest software version and patches. These actions keep the devices themselves more protected and 'hardened' against weakness and attacks.

It is recognized that not all network infrastructures are suitable and lend themselves to these types of protection schemes. It is recommended that additional work be done in the area of this research to develop or recognize architectural designs and plans that encompass architectures that cannot be secured via these discussed techniques.

8.0 REFERENCE – RECOMMENDATION 2.X

8.1 Introduction - Securing Cyberspace

The goal of this, and the cumulative work of the other DHS Task Forces and working groups is to secure cyberspace, in relation to the boundaries of the U.S. This is indeed a monumental task. The aim of this working group is to educate and recommend network level architectural issues that can lead to this noble purpose.

Essentially, the Internet, or 'Cyberspace', is NOT a collection of boxes performing individual tasks. Cyberspace IS a collection of networks performing functions, and should be treated as such. Cyberspace is essentially one large network made up of smaller individual networks, each adding to the whole. Each network, no matter how large or small, plays a part in making up cyberspace. Since each of these networks are individually owned and operated, they cannot be secured as a whole against outside attack, especially since some of the attacks are likely to originate from somewhere inside the network (as a whole). Therefore, we are faced with protecting these individual networks that make up cyberspace, from other networks inside cyberspace, as well as protecting cyberspace (as it exists in the U.S.) from malicious activity outside North America. So, we must create a plan for protecting cyberspace one network at a time.

Any engineer will tell you that each network is different, and that is a very accurate statement. There are however, commonalities to all networks regardless of their purpose, be it on-line banking, Internet Service providers, or a simple home network. As far as security is concerned, there are also commonalities; the most common security device is the traditional firewall. Firewalls can be, and are implemented in just about ever type of network ever built, even the small home network. There are also other issues that are typically overlooked that are common, or should be common, to all networks, one of these issues is secure design, meaning a network architecture that was built, or re-built with security, as well as function in mind.

Most networks today were not originally designed with security as one of the top issues; network security for the most part had traditionally been an afterthought. There is good reason for this. It's only been in the last decade or two that serious security threats have begun to commonly arise in cyberspace and many network owners have scrambled to install firewalls, Intrusion Detection, and other associated devices to plug these previously unknown security weaknesses.

The industry has recently discovered the need for enhanced security, and has invested billions in hardening its architectures. One thing that is often overlook in this process, and in the process of designing new networks is that the layout of the architecture itself needs to be secure. In other words, a well laid-out network with no security devices can be inherently more secure that a poorly laid out network with an abundance of security devices. Therefore a few minutes spent learning how to securely architect networks would be time well spent, and this is what part of this paper aims to do.

If we, as an industry, or as a country, are to claim that our portion of cyberspace is secure, then we must have some method of making this determination. We need some grading format that is common to all networks, that allows us to grade the security of the individual networks so that we can determine the overall security of the U.S. portion of cyberspace, as our President has required us to do.

8.2 Grading the Security of Individual Network Infrastructures

One suggestion or recommendation for grading the security level of each individual network infrastructure is to implement a publicly known and accepted rating system that is generic enough to encompass all networks, but detailed enough to ensure their security on many different levels. After all, security is a philosophy, and a way of life, or a way of doing business in this case; and any grading or rating system should take this into account.

The following proposed recommended rating system divides ratings, or certifications, up into five levels. Level 1 thru level 5 certifications is based on tested infrastructure security. These certifications can be analogized to the U.S. Military's DefCon 1-5 rating system for defense condition. For example, a network with a security classification of 5 has been tested and deemed more secure than a network with a security classification of 1. These certifications state not only the graded networks 'Defense Condition,' but also the defense condition of the operator, and their business and response practices as it relates to their networks security. This certification also demonstrates

the operator's ability to accurately and timely communicate information to the rest of the industry on lessons learned from dealing with IP or network infrastructure security issues.

In order to properly implement a system like this, it is recommended that the cyberspace sector either police itself based upon developed criteria of a standards-like organization, or have an independent organization created that defines, manages, updates and executes the delivery of these recommendations. Either or both of these groups should be made up of industry and government security experts at all levels from firewall/device experts, management level subject matter experts on incident response, and technical support directors, just to name a few.

8.3 Security Classifications or 'DefCon' Levels

The following five classification levels provide a means for rating, or grading an individual infrastructures security level. The word 'infrastructure' in this context refers to the network, and the network owners' security practices as it relates to the network and the information it contains.

The security classifications are listed and discussed in the order of increasing security requirements.

Level 1 Security Classification Recommendations:
The level 1 classification of network security is the first rating and has the most basic requirements of the five. They are:

- The network to be certified undergoes an external vulnerability assessment of all perimeter systems. These systems may include Internet gateways, web servers, email servers, name servers, modem dial-in connectivity, etc. This means that all systems or network components that are exposed to any other network not owned by the same owner must be tested.

- The results of the testing must not return any vulnerabilities that are exploitable.

- The vulnerability assessment must conclude that it is not possible to 'see,' or identify components or systems, inside the tested network any farther than its security perimeter.

- Vulnerability assessment to be carried out using the most up-to-date recognized industry assessment tools that are certified by the independent organization.

Other details of these level 1 recommendations are to be addressed by the standards body and/or independent organization.

Level 2 Security Classification Recommendations:
The level 2 security classification includes all the requirements of the level 1 classification plus:

- An internal examination of the perimeter security equipment to ensure that the latest and most secure software loads, patches, and updates are installed; and that the perimeter equipment is configured in the most secure manner in accordance with the guidelines and recommendations of Task Force 4, Working Group 1, Common Configuration.

- A review of the network owner's security practices regarding upgrade and patch management procedures and processes. This includes the use of 'staging' servers or other appropriate equipment to test patches and software upgrades before they are implemented on production networks systems.

- Results of this examination must return conformance with TF4, WG1 recommendations, and show adequate procedures and processes to properly implement upgrade and patch management.

Other details of these level 2 recommendations are to be addressed by the standards body and/or independent organization.

Level 3 Security Classification Recommendations:
The level 3 security classification includes all the requirements of the level 2 classification plus:

- A vulnerability assessment of the 'Human Firewall'. This may include researching all publicly available information (press releases, knowledge bases, etc) of an organization to determine if any information is unintentionally provided that can be used to compromise the owners network. This may also include unannounced questioning via phone, or personal visit to support staff by unknown personnel asking questions that could reveal security weaknesses if answered, or answered improperly. For example, information that can be used to compromise a network's integrity may be as simple as revealing information on equipment types, software versions, IP addresses, maintenance window times, etc…

- It is also recommended that personnel in positions of holding this type of knowledge be required to sign non-disclosure agreements detailing the types of information that is and is not allowed to be discussed, and who they are, and are not allowed to discuss this information with.

- The results of the assessment of the 'Human Firewall' should not return any information that can be used to compromise the owners network.

Other details of these level 3 recommendations are to be addressed by the standards body and/or independent organization.

Level 4 Security Classification Recommendations:
The level 4 security classification includes all the requirements of the level 3 classification plus:

- A review of the network owner's internal security practices as they relate to:

  - Incident Preparedness
  - Incident Investigation
  - Incident Response
  - Incident Alerting and Notification
  - Incident Recovery

Recommendations on these practices may fall under the standards and recommendations of Task Force 4, working Group 4, Best Practices for Technical Standards.

Other details of these level 4 recommendations are to be addressed by the standards body and/or independent organization.

Level 5 Security Classification Recommendations:
The level 5 security classification includes all the requirements of the level 4 classification plus:

- Subjecting the network being tested to professional ethical or 'whitehat' penetration attempts, or other activities designed to improperly effect the tested networks equipment or services. These attempts should be carried out at a time unknown to the network owner.

  These ethical or whitehat hackers should be sanctioned and certified by the standards body and/or independent organization.

- Also, the network owner should be able to demonstrate that they comply with the recommendations laid out by Task Force 2, Early Warning. This demonstrates that the network owner is able to share information and lessons learned with the rest of the industry for the benefit of the whole. The fact that the owning organization has reached the level 5 classification, means that this information should be accurate and reliable.

- The results of these whitehat attacks should not result in an actual penetration beyond the security perimeter, and the network owner should be able to report the following minimum information to the independent organization (if utilized) via TF 2 recommendations within a given acceptable time frame:

  1. Time of attack
  2. Type of attack, penetration attempt of X device, Denial of Service Attack, etc….

3. Was attack successful in penetrating the infrastructure, or disabling equipment or services?
4. Attack target. What gear was affected?
5. Source of attack, or at least the operators best guess of the source of the attack. This may include IP and/or geographical information.
6. Are any adjustments required by the network owners procedures or processes to deal with future attacks of these types?

Other details of these level 5 recommendations are to be addressed by the standards body and/or independent organization.

The goal of these security classifications is to be as detailed and hard as possible while being open and generic enough that anyone owning a network, regardless of size, can achieve any level classification desired. This dictates that the details of the requirements of each classification level must be appropriate to the network being certified. For example, it is much easier for someone in a home office to demonstrate perimeter security, and security practices, than it is for a large organization with a nation-wide network infrastructure to demonstrate the same requirements.

It is recommended that the determined security certification level of each certified network be kept confidential and only be made publicly known by the network owner/operator. Public knowledge of each networks certification level may lead to attempted penetration attempts of networks holding lower certification levels.

As networks receive certifications, ongoing testing must occur to maintain certification levels. Many times a network can be implemented today that is secure, but will be vulnerable tomorrow due to updated hacking techniques, network expansion or modification, and ongoing device software upgrades. It is recommended that each network be tested and re-certified at least once a year.

It will be up to the cyberspace sector, standards body and/or the independent organization to determine what levels are required of what networks before we can make the statement as a country and say, “Cyberspace is secure.”

9.0 CLOSING STATEMENT

As this document proposed some constructs to enable a secure network equipment deployment as an architectural model, we do not suggest being a complete reference on building a secure model. This document is to emphasize the criticality of implementing a hardware configuration that will allow for the maximum benefit of the best practices of software and management of networks.

Network security has become a pivotal role in the extremely fast moving and complex business environment which can be the most fragile place for malicious invasion. By understanding the network topologies and how they inter-relate to the software and management best practices, an understanding of a secure architectural model can be realized.

IP communication infrastructures, by their very nature are open, and can be as secure or vulnerable as is needed or mandated. When securing an existing network, the effort to increase security can be a very difficult task depending on the legacy of the network. Risk analysis has to be completed and a realistic overview of reconfiguration options should be weighed to the networks mandate for security. When architecturally designing a network from the ground up, there is far less short falls to overcome. As the network expands and more elements are introduced to the topology there must be a clear path to growth with security as a key element of future assimilation of new technology.

There is an ongoing effort from software and hardware vendors to create products that are tested for exploits and vulnerabilities, however there is nothing set in stone as of now regarding how this testing is done. Companies that implement secure architectures today must continue vulnerability testing from both the inside and outside, stay current on fixes and patches, and keep up to date on existing or upcoming threats.

Once the effort has been made and the deployment has been completed, the best-laid plan can be failed by the “Human Factor.” The philosophy of security must become a cultural issue that everyone who is associated with the

network must adhere to. Policies that inform staff of how they are to use the network in great detail is not an effort to be minimized. The "Human Factor" is one of the hardest to manage and should be addressed early and often.

10.0 ADDITIONAL RESOURCES

These resources may be consulted and implemented to supply, or create additional levels of security that are not covered in this recommendation.

ITU x.css

Draft Recommendations [1] T01-SG17-030910-C, draft, new ITU-T Recommendation X.css. Security Architecture for Systems Providing End-to-End Communications, ITU-T, July 2003.

ANSI T1.276

ANSI T1.276-2003, American National Standard for Telecommunications Operations, Administration, Maintenance, and Provisioning Security Requirements for the Public Telecommunications Network: A Baseline of Security Requirements for the Management Plane.

ANSI T1S1

ANSI T1S1/2003-285, American National Standard for the next generation network control and signaling plane security.

NIST FIPS 199

NIST FIPS PUB 199, Standards for Security Categorization of Federal Information and Information Systems.

11.0 ACKNOWLEDGEMENTS

The following is a list of those people who participated in or contributed to the Equipment Deployment & Architecture Guidelines Working Group and the development and review of this report.

Name	***Title***	***Organization***
Victor Rychlicki (Working Group Chairman)	Senior Security Systems Engineer	Marconi Wireless
Uma Chandrashekhar	Advanced Network Reliability, Security & Service Assessment & Optimization	Bell Labs Lucent Technologies
Mary Ann Davidson	Chief Security Officer	Oracle Corporation
Lawrence G. Dobranski	Senior Network Security Architect	Nortel
Greg Jackson	Vice President	DeepNines Technologies
Ron Knode	Director, Global Security Service Definition and Deployment	Computer Sciences Corporation (CSC)
Steve Macke	Senior Consultant	Georgia Tech Research Institute
Ron Mathis	Director Security Infrastructure and Planning	Intrado
Edward Roback	Chief of Computer Security Division	NIST
Marty Schulman	Chief Technologist	Juniper Networks
Jack Suess	Chief Information Officer	University of Maryland, Baltimore County

Appendix E

National Cyber Security Partnership
Technical Standards and Common Criteria Task Force

Common Criteria, NIAP Review and Metrics Working Group
RECOMMENDATIONS REPORT

April 19, 2004

TABLE OF CONTENTS

1.0 EXECUTIVE SUMMARY

The National Cyber Security Summit held in Santa Clara, CA on December 3, 2003 created the Technical Standards and Common Criteria Task Force. This task force formed the Common Criteria, NIAP Review and Metrics Working Group. This working group is composed of representatives from the customer, vendor and evaluation lab communities. This working group's objectives were to develop recommendations for how to define better security metrics, develop a mechanism to express consensus-based requirements and to provide inputs to the "National Information Assurance Partnership (NIAP) Review."

This report is the output of the Common Criteria, NIAP Review and Metrics Working Group with recommendations for specific actions to fulfill the stated needs.

The national and international information infrastructure includes civilian systems and networks and commercial products from U.S. and non-U.S. companies. In order to ensure the security of the information infrastructure we need to improve the security of the Commercial Off-the-Shelf (COTS) products used within it.

The Common Criteria (CC) offers a number of advantages that make it an excellent starting point toward meeting the objectives of the working group. CC is internationally recognized and provides a standard framework for product evaluations. It also provides a rich language through which customers can articulate their security requirements. It is generally agreed that the working group objectives can be met with more education about the CC capabilities and improvements to the process and implementation.

There are several issues with the CC and the U.S. Scheme that need to be addressed in order for the CC to be truly effective. The working group makes the following recommendations and encourages the sponsors of the Cyber Security Summit (ITAA, BSA, TechNet and U.S. Chamber of Commerce) and their member companies to support these recommendations.

1.1 Increase NIAP effectiveness

The stated objectives of NIAP are to meet the needs of government and industry for cost-effective evaluation of Information Technology (IT) products and to improve the availability of evaluated IT products. Currently, NIAP has failed to accomplish these objectives. NIAP has been focused on meeting the needs of the government intelligence community. It needs to re-focus its efforts on the security needs of other government agencies and the needs of the private sector. Getting the National Institute of Standards and Technology (NIST) re-engaged fully will be critical to the future success of NIAP by representing the security interests of the private sector and the rest of the government.

NIAP would greatly benefit its government as well as private sector communities if it adopted a more open process in developing national standards and in providing inputs to the international standards. NIAP should include customers, vendors and evaluation labs in the development of government Protection Profiles (PP), interpretations and recommendations to the international CC community.

NIAP can greatly increase the demand and availability of evaluated products by providing more training and guidance to customers and vendors. Through greater awareness and education of CC benefits, customer demand for evaluated products will increase. The broader customer base will give vendors justification to compete with evaluated products and to compete on the basis of security features.

1.2 Make Government COTS procurement policies realistic

NSTISSP #11 and DODI 8500 direct Department of Defense (DOD) agencies to procure only those COTS products that have undergone CC evaluation. There are major flaws apparent today with these directives.

First, many of the U.S. Government-approved PP requirements are not realistic for COTS products. These PPs assume product architectures that do not reflect COTS product realities making it impossible for certain classes of products to claim conformance to the PPs.

Secondly, depending on the assurance level, the complexity of the product itself, and the underlying product dependencies (i.e. for all components an application relies on to be evaluated), it may take months or years to evaluate a product. DOD procurement practices demand that only evaluated product versions may be procured.

Finally, these policies are not implemented consistently across the agencies. For example, some agencies and contracts allow procurement of products still "in evaluation" while others have no requirement for evaluation. This is due to lack of understanding of the directives and the fact that the directives are not practical.

The U.S. Government needs to make its procurement policies for COTS products realistic and to administer them consistently.

1.3 Reduce costs of Common Criteria evaluations

Typical evaluation lab fees will run hundreds of thousands of dollars and up to millions of dollars. Development of product evaluation submissions can take hundreds of person-hours. These high costs coupled with the fact that CC evaluations are not in broad demand force vendors to choose which products to evaluate and for some not to evaluate at all.

Once a product has gone through an evaluation, it needs to maintain its evaluated status. There is currently no nationally or internationally recognized evaluation maintenance program. In fact, ratings maintenance as it has been done in the past simply does not work. The cost and complexity of evaluating every change to a product, for example, may make it cheaper to do an entirely new evaluation. However, re-evaluation cost, time and effort can be reduced with effective reuse of product evaluation evidence.

The U.S. Government should encourage CC evaluation by helping to reduce the impact of evaluation costs. NIAP should provide vendors with more information on how to minimize costs and effort and how to effectively reuse evidence documentation. NIAP should examine alternative evaluation and testing paradigms to identify ways of reducing time and effort and yet improve product security and assurance.

1.4 Increase customer demand for Common Criteria evaluated products

In the U.S., there has been very little interest and adoption of the CC in the private sector. Vendors have little incentive to undergo the costly and time-consuming evaluation effort without larger private sectors markets embracing CC. Much of the reason for duplicated efforts and lack of customer demand for certifications is the lack of awareness of the capabilities and benefits of CC evaluations.

Customers need more training, education, and information about CC capabilities and benefits. Customers need to understand the role they play in ensuring security of the international information infrastructure. They also need to understand how they can articulate their requirements effectively using PPs.

As customers become more aware of security issues and better able to articulate their security needs, vendors will be better able to compete to meet those needs. Market forces will drive security as a competitive issue and catalyze a cultural change in the IT industry to become more secure.

NIAP should help educate customers on the benefits of CC and how they can articulate their security requirements using PPs. Customers depend on NIAP to provide current and accurate product evaluation information

1.5 Improve the use and utility of Protection Profiles

NIAP and the Department of Homeland Security (DHS) should encourage the establishment of customer and vendor consortia to develop PPs. PPs offer customers the ability to articulate their security needs in a standard language. Coupled with improving the evaluation process to enable products to be "graded" against several PPs simultaneously, this represents the first step toward being able to doing "apples-to-apples" comparisons of products.

Currently, the NIAP interprets the CC narrowly so that a given Target of Evaluation (TOE) cannot utilize support of its environment in meeting requirements. Requiring that the TOE to solely meet some requirements pose significant problems for products especially application software products that are developed on top of operating systems,

networks, and other products. Allowing requirements to be met by the TOE and the Environment greatly increases the utility of PPs.

Customer consortia should be encouraged to create more PPs, especially for application products. Vulnerability assessment is recognized as a very important aspect of CC evaluations. Vulnerability assessment should be made a requirement in all PPs regardless of Evaluation Assurance Level (EAL).

1.6 Increase product security through Common Criteria

Today, CC evaluations are generally (in the U.S.) treated as a "checkbox" procurement item. There is a tremendous opportunity to help vendors recognize the value of evaluations to improve the effectiveness of their internal processes and product security. This can be a catalyst for cultural change in the product development (especially software) industry and improve the overall security of the critical information infrastructure

Those vendors that have experienced several product CC evaluations have attested to security improvements in their product development processes. Vulnerability assessments, testing strength of function, assuring secure delivery and other CC assurance tests help vendors improve the security of the features of their products and their development, delivery and support processes. All of these activities contribute to reducing security defects and vulnerabilities and thus reduce support costs.

NIAP and the vendor community can improve vendor education on the impact of CC evaluations by sharing vendor CC experiences. NIAP can provide more outreach and education to vendors.

DHS should support research into quantifying the benefits of security process improvements.

2.0 TASK FORCE MISSION STATEMENT

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 U.S. Department of Homeland Security (DHS) was directed to identify gaps and develop recommendations to promote the adoption and implementation of the President's *National Strategy to Secure Cyberspace*. These recommendations will be presented to the DHS for consideration in planning next steps. There is a meeting planned for September 2004 to check the status of these recommendations. The Task Force mission statement is as follows:

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 CC standard and National Information Assurance Partnership (NIAP) testing program in support of the "NIAP review."

3.0 WORKING GROUP MISSION STATEMENT

Out of the Technical Standards and Common Criteria Task Force, the Common Criteria, NIAP Review/Metrics working group was created. This working group consists of members from product vendors, customers and international CC evaluation labs. The stated objectives of this working group are to address the following:

- There is a need for better security metrics to give consumers a means by which they can compare products against their requirements and compare security claims among vendors.
- There is a need for consensus-based requirements for infrastructure components expressed in a standard language.
- Provide inputs to the "NIAP review" to be conducted by the Administration in early 2004 to improve current processes based on past experiences.

4.0 INTRODUCTION

The national and international information infrastructure is composed of civilian systems and networks and commercial products from U.S. and non-U.S. companies. It is clear that ensuring the security of our information infrastructure is a priority. We can begin to achieve this by developing and deploying more secure computing products. The members of this working group believe that Common Criteria evaluations can help us develop more secure products and provide a higher level of assurance for the information infrastructure[1].

Improving product security is not the only thing needed to secure our computing infrastructure, but it is recognized as an important component. And while improving product security may not have been an original objective of the Common Criteria, this working group believes it is a good basis or catalyst for achieving this goal. It is recognized that the Common Criteria and the implementation of its processes is not perfect, many believe it is a good place to start if we can address some of the issues.

Articulation of customers' security needs and increased focus on security have given vendors motivation to pay more attention to security features, secure development, delivery, installation and configuration. Evaluation of products and processes by an independent third-party lends credibility to vendor claims. An internationally recognized standard evaluation methodology gives customers a level of assurance no matter where in the world a product is produced or where it is evaluated. The Common Criteria has these attributes.

In the past, demands on product engineering have increased as customers' awareness and demand for more reliable and user-friendly products have increased. The same thing is happening now with security. As customers become more aware of security issues and articulate their security needs, vendors compete to meet those needs. The Common Criteria holds the promise for providing a way to measure the relative security of products against the

[1] IBM strongly disagrees at the present time with the view that CC should be expanded. IBM believes it must first be demonstrated that the issues raised with CC are being addressed, and that it can be shown that CC is cost-effective.

customers' requirements. As this trend grows, the information technology (IT) industry will develop a culture of becoming more secure.

The NIAP has been tasked with improving the security of the U.S. Government's information infrastructure. Congressional staffs are planning a review of NIAP's effectiveness and have asked for input from parties that have interacted with NIAP. This task force welcomes the opportunity to relate first-hand experiences and offer recommendations for helping NIAP achieve its goal of improving the security of our information infrastructure.

5.0 ADVANTAGES OF COMMON CRITERIA

The CC offers a number of advantages that make it an excellent starting point toward achieving the stated objectives. It is generally agreed that the stated objectives can be met with more education about the CC capabilities and improvements to the process and implementation.

5.1 Internationally recognized standard

The CC is an internationally recognized common language to express security requirements, product features and product development, delivery and operation assurance. It has been established as International Standards Organization (ISO) standard 15408. Nineteen countries have signed the Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of IT Security (CCMRA). Certification by one of the certificate producing nations of the CCMRA is recognized by the other member countries that have signed the Arrangement. This helps eliminate the need for country-specific evaluations and certifications. Beyond the standard language is a standard evaluation methodology to assure customers that products are evaluated consistently around the world.

5.2 Designed to describe security requirements of systems and components

Application of the CC around the world has demonstrated its flexibility in addressing a wide variety of requirements. PPs define threat models, objectives and the environments into which the products will be deployed. These can be used to define metrics.

5.3 Helps improve security of vendor processes and products

The use of accredited, independent, objective evaluators serves to provide greater assurance that products meet their claims for security. Third-party evaluators are focused on providing objective evaluations using standard methods. CC evaluations test the vendor's processes as much as the product itself. Product security architecture, functional, design, and test specifications are reviewed and a secure development process has to be repeatable in order to achieve certification. Centralizing on a single evaluation process drives consistency within a vendor corporation. This addresses the issue raised by consumers that within a company there are inconsistent processes.

5.4 Standardized certification is an industry cultural catalyst for change

Institutionalizing evaluations as part of product development, and then repeating them over and over changes the corporate culture. Over time, it becomes an industry culture.

Security can only be built in from inception, not "bolted on" after the fact. Just as usability and reliability have been added to the requirements customers expect products to meet, security is now expected. The CC has been a catalyst for this change internationally.

6.0 FINDINGS AND RECOMMENDATIONS

The findings and recommendations are divided into seven core focus areas. Each focus area, discussed in more detail below, will include a brief overview along with a set of recommendations for improvement. The focus areas covered by this report are:

- Increase NIAP Evaluation Scheme effectiveness (NIAP Review Inputs)
- Make Government Commercial Off-the-Shelf (COTS) procurement policies realistic
- Reduce the costs of CC evaluations
- Increase demand for CC evaluated products
- Improve the use and utility of PPs
- Increase product security through CC

6.1 Increase NIAP Evaluation Scheme effectiveness (NIAP Review Inputs)

The overall finding is that NIAP is currently not addressing the full scope of the U.S. Government's information infrastructure. Rather, it is primarily focused on the Federal intelligence community. The NIAP and its Common Criteria Evaluation and Validation Scheme (CCEVS) claim the following objectives[2]:

- To meet the needs of government and industry for cost-effective evaluation of IT products;
- To encourage the formation of commercial security testing laboratories and the development of a private sector security testing industry;
- To ensure that security evaluations of IT products are performed to consistent standards; and
- To improve the availability of evaluated IT products.

However, as identified in more detail below, these objectives are not currently being met.

As identified above, the U.S. Scheme needs to address the entire U.S. information infrastructure. To that end, it should serve many communities of interest with very diverse roles and responsibilities. These communities include IT product vendors, value-added resellers, systems integrators, IT security researchers, acquisition/procurement authorities, consumers of IT products, auditors and accreditors. Close cooperation between government and industry is paramount to the success of the Scheme and the realization of its objectives. Furthermore, the Scheme needs to be run openly and in an unbiased and consistent manner.

6.1.1 Current Landscape

NIAP was created out of a partnership between the National Security Agency (NSA) and the National Institute of Standards and Technology (NIST). NIAP contains the U.S. Common CCEVS or U.S. Scheme. The CCEVS represents the U.S. in the international CC community. Today, due to budget limitations there is essentially no NIST representation in NIAP. The NSA-only driven NIAP lacks the balanced view of security to cover all U.S. interests, not just the Federal intelligence community. NIAP should address the question – how can we make CC evaluations viable for commodity products?

NIST should receive new appropriations to be used for the greater adoption of CC through supporting the development of "market appropriate" PPs. The majority of customers do not need the higher assurance or specific technical security features that so-called "higher assurance" evaluations (for classified systems) entail. In fact, many of the PPs developed by NSA (for higher assurance evaluations) are not appropriate or applicable to commercial products. NIST appropriations should also be used to develop greater standardization and higher quality of the evaluation work. Best practices and specific "how to evaluate against this protection profile" will make it easier for labs to do high quality, consistent work.

Customers (public and private sector), vendors, and evaluators need a greater voice in the international CC and ISO community to address issues such as:

- Continue the work to expand the CC standards to fully address system security requirements. ISO 15408 Working Group 3 is addressing this.
- Interpret or provide requirements that are more broadly applicable to evaluated products. For example, a number of important requirements have been interpreted so that they cannot be claimed by applications, such as firewalls and intrusion detection products.

[2] From the NIAP CCEVS website URL http://niap.nist.gov/cc-scheme/ccevs-objectives.html

- Improve the handling of interpretations such that there are appropriate national reviews and concurrence before they are submitted to the international Common Criteria Interpretations Board (CCIMB). Reduce confusion by evaluating products against the established ISO standard rather than mandating interim interpretations as they occur, which impacts comparability and re-evaluations.
- Support the efforts to establish FIPS-140-2 as an ISO standard.
- Improve the CC to recognize new methods to improve product security and development process assurance measures, such as the use of independent source code reviews and automated bug checkers.
- Improve the education and training of CC for customers and vendors.

While CCEVS validations, like evaluations are not completely objective, validations lack consistency due to the training, expertise and focus of the individual validators. Moreover, validators validate by re-evaluating the results of the evaluators. Validators are not offered training different from evaluators. Perhaps as a result of these factors, the CCEVS seems to distrust evaluators (and their own validators) and implement measures to check the work of the evaluators and validators during evaluations.

Many of the NSA-sponsored PPs were not created with the input of the consumer agencies; therefore, they don't always reflect the needs of these agencies except perhaps the intelligence community. These PPs also were not developed with input from vendors and evaluators. The result has been there have been very few products that have been certified against these PPs. NIAP should be working with vendors to encourage them to certify their products and develop requirements that are reasonable and achievable.

Recent PP developments are using the NSA-defined "medium robustness" standard or Evaluation Assurance Level L4-Augmented (EAL4-Augmented) that do not align with international mutual recognition. Evaluations against these PPs require custom evaluation work by the NSA. These effectively U.S.-only requirements may drive other countries to adopt their own country-specific requirements, thus defeating the CCMRA. The major component for the "plus" part of the evaluation is vulnerability analysis. This will not help improve product security because the product under evaluation has already shipped in most cases. Therefore, "vulnerability analysis" at that stage does nothing but slip the evaluation, as the vendor has to make product changes that cannot be made in current product.

Pushing vulnerability analysis down the assurance chain (i.e. requiring this at lower assurance levels), as was suggested earlier in the document, would resolve this issue. Furthermore, making it part of development process would improve overall product quality and security.

6.1.2 Gaps and Recommendations

Recommendation: Provide greater funding to NIST so that they can return to represent the interests of the majority of the U.S. Some efforts are underway by individual companies and some industry organizations and progress towards actual funding should be checked in September. NIST should receive new appropriations in the amount of $12 million upfront and $6 million per year thereafter for the purposes of developing non-classified PPs and developing best practices and methodologies to enable labs to evaluate products against these PPs.

Recommendation: Knowledgeable customers, vendors, CC consultants and evaluation lab personnel should be involved from the beginning in some standards development activities, such as CC revision and interpretation. This will lend perspectives to the standards that will make the standard more robust and account for the realities of the environment, product technologies and serve to improve the credibility and acceptance of the standards.

Recommendation: NIAP should provide standard training and guidance specifically for validators so that they are properly trained to validate results rather than re-evaluate. This training is expected to improve the consistency of validations. If a Security Target (ST) claims conformance with a PP, the CCEVS often consult the PP authors for their intentions. They are willing to allow STs that do not meet the literal words of the PP if the PP author indicates that is what they meant and conversely, a ST that meets the literal words of a PP might be disallowed if the PP author indicates that is not what they meant. This ambiguity needs to be addressed.

Recommendation: Knowledgeable vendors, consultants and evaluation labs should provide standard evidence templates or examples for vendors and have NIAP validate them to help vendors generate the proper documentation for evaluations. The existence of such templates or examples will also help evaluation labs and consultants to better understand thresholds of acceptability so they can provide better services.

Recommendation: NIAP can work with the National Voluntary Lab Accreditation Program (NVLAP) to create a Lab Accreditation Program (LAP) for commercial, commodity products to make CC evaluations viable for all commodity (COTS) products.

Recommendation: NIAP should recognize that the NSA-developed PPs do not apply to all U.S. Government agencies without proper vetting with agency customers and vendors. Other agencies, such as DHS should consider parallel initiatives to develop PPs for their respective users.

Recommendation: NIAP should support more sponsorship of the development of PPs vetted by customers and vendors for private sector markets. Customers (i.e. vertical market groups) and vendors should develop consortia to collect requirements, discuss technology, product and business realities toward the development of PPs.

Recommendation: NIAP needs to employ a more open process for the development and management of PPs they develop. Customers and vendors need to be better informed about new PP developments and timetables. Customers and vendors can express their needs to be consistent internationally and to meet Mutual Recognition requirements.

6.2 Make Government COTS procurement policies realistic

Procurement policies have been used historically to encourage the evaluation of products against available standards so that users can better understand what the products provide and whether they can address identified needs. To be most effective, procurement policies need to be practical, justifiable, reasonable and effective.

6.2.1 Current Landscape

The U.S. Department of Defense (DOD) has directed its agencies to comply with NSTISSP #11 and DODI 8500 requiring COTS products to be CC certified as a condition for procurement. These directives have been applied inconsistently or ignored by the purchasing agencies. CC certifications are treated as "checkbox" items by both agencies and vendors. Many DOD agencies have little understanding for how CC evaluations will help them improve the security of their environments. This lack of understanding undermines the real purpose for submitting products to CC evaluations.

The NSTISSP #11 was updated in July 2003 and includes the following paragraph:

> *(14) While COTS IA and IA-enabled products (non-encryption based) have been developed, evaluated, and are available for acquisition and implementation on national security systems, it is recognized that these products do not cover the full range of potential user applications. Rapid technologic changes and the amount of time it takes to successfully complete a product evaluation also affect compliance with NSTISSP No. 11. Therefore, full and immediate compliance with NSTISSP No. 11 may not be possible for all acquisitions.*

NSTISSP #11 now allows exemptions and deferred compliance. These policies may open the door for more inconsistency across the DOD and defeats the purpose of product evaluation.

The DOD directives allow for products still "in evaluation" to be procured by the DOD agencies. This practices drives vendors to enter the CC evaluation process prematurely and can mislead the customers. Entering the evaluation process prematurely can also drive the total evaluation costs up and ties up scarce evaluation and validation resources.

DODI 8500.bb requires that if a PP exists for a product type, that only those products that have been certified against that PP may be procured. Many of the NSA-sponsored PPs contain requirements that are too specific, assume monolithic product architectures and sometimes reflect archaic technologies thus excluding many modern COTS products from meeting these requirements. In these cases, the PP becomes a Request for Proposal (RFP) for a custom product.

Since the DOD through NSTISSP #11 and DODI 8500.2 require COTS products to certify against PPs when they exist, COTS application software intrusion detection system (IDS) and firewall products have been submitted for evaluation against their respective PPs only to find that in order to be certified the Target of Evaluation (TOE)

would have to include the underlying operating systems. There has to be a way in which application software vendors can meet PP requirements without having to include OS code into the TOE of the application. Specifically, some products rely on the OS to securely store the user and audit data. Some rely on the OS or LDAP for authentication and identification. These products cannot claim they meet the PP requirements. If the DOD continues to require products to meet PP requirements as currently stated and evaluated, there will be very few products that they can procure.

The authors of some of the U.S. Government-approved PPs believe they are including requirements to improve the security of current products. They have every right to do so, but when the requirements do not reflect the needs of the broader customer base for vendors, then the COTS product becomes a custom product for the government and the RFP process should be used. The government should then pay the costs for the development of a custom product and pay the costs for a custom evaluation.

There is no PP management process nationally or internationally. Since NIAP is the most prolific generator of PPs, it raises the greatest issues. The NIAP PP development process is closed and timetables are unknown to vendors or customers. Rumors of new PPs emerge and vendors, in the middle of evaluation against an older version of the PPs are expected to evaluate against the new PP requirements. Since the requirements within the new PP are not made public and the actual release date is unknown, the vendor is stuck. It needs to be made clear whether new PPs are expected to replace older ones.

6.2.2 Gaps and Recommendations

Recommendation: Experienced vendors, consultants, evaluation labs and NIAP should provide greater security education and training to DOD and other agencies to help them understand the role CC evaluations play in improving the security of their information infrastructure.

Recommendation: DOD procurement policies should be modified to encourage improved security rather than presenting barriers to procurement. This includes ensuring consistent application of the procurement policies and the elimination of exemptions and deferred compliance.

Recommendation: DOD agencies should review vendor ST claims and evaluated configurations as part of the purchasing process to ensure that the product will meet security requirements in the deployed environment. These practices should help eliminate the “checkbox” mentality.

Recommendation: Until PPs are properly vetted with realistic customer requirements and vendor inputs; the DOD should suspend the requirement for COTS products to meet PP requirements. Should the DOD choose to retain this policy, the RFP process should be used to provide DOD customers with custom products to meet their custom requirements. The RFP response costs will include costs for developing a custom product the costs for a custom CC evaluation.

Recommendation: Product evaluations against PPs should be “grandfathered” allowing vendors to complete evaluations against older PPs while newer ones are being developed. This should be reflected in government procurement policies.

6.3 Reduce costs of Common Criteria evaluations

While amortizing evaluation costs across a broader base of customers provides some vendors with a viable return-on-investment (ROI) argument, the costs are prohibitive for many. CC evaluation costs should be in reach of all vendors willing to invest in improving their products and processes. However, the key will be customer demand for evaluated products.

To be most effective, evaluations should be viable for all types of products and should accommodate a wide range of life-cycle models, release cycles, and product update methods and frequencies.

6.3.1 Current Landscape

Typical evaluation lab fees will run hundreds of thousands of dollars and up to millions of dollars. Creation of evaluation submission packages can take hundreds of person-hours. While these costs are considerable for larger vendors, smaller companies may find these costs prohibitive. Many of these companies introduce innovative new technologies to address security threats. These cost issues will force vendors to choose which products to evaluate rather than submitting all of them. Today, the preparation, evaluation and certification processes can take several months to a year or more to complete. In the fast-moving IT industry, certified product versions become obsolete by the time evaluations are complete. There must be ways in reduce the time it takes to complete the CC process

An effective evaluation maintenance program can help vendors provide certified or assured versions of products in a timely fashion. In fact, ratings maintenance as it has been done in the past simply does not work. The cost and complexity of evaluating every change to a product, for example, may make it cheaper to do an entirely new evaluation. A major reason why the Orange Book failed was because of the lack of a viable "ratings maintenance" mechanism. There needs to be some happy medium between requiring a brand new evaluation for every single release (and minor upgrade) of every product, and ratings maintenance of all changes to a product. Clearly, it should not be the case that a vendor does one evaluation that is "valid" for four years and four major product upgrades.

The evaluation maintenance program must address the issue that COTS product version update cycles are on the order of weeks, not months as the typical CC evaluation cycle. Products will also change (e.g. final QA, bug fixes) during the evaluation process and minor changes must not force a major reset in the evaluation process. Effective evidence reuse is critical to the success of such a program. Vendors need to become better educated about how to create reusable submission information.

6.3.2 Gaps and Recommendations

Recommendation: In order to promote the evaluation of more products, the U.S. Government should help offset the expenses of CC evaluation through research and development tax credits or paying part of the evaluation costs.

Recommendation: Vendors need more information and education from evaluation labs and perhaps other vendors on when to enter the evaluation process and what to expect and how to prepare. Some labs and consultants offer this as a service, but NIAP should also offer public guidance in this area:

- NIAP should provide a set of vulnerability assessment tools and evidence templates and/or samples to developers to help ease the evaluation process.
- NIAP should provide information and guidance to vendors regarding evaluation evidence reuse to help reduce time and costs of re-evaluations.

Recommendation: Vendors can greatly reduce the costs required to complete CC evaluations by integrating CC evaluations into their product development plans. This will require more education and organizational commitment to CC within the companies.

Recommendation: NIAP, NIST, customers and vendors should research alternative evaluation and testing paradigms (such as the so-called “Common Criteria Lite” concepts) to identify ways of reducing time and effort and yet improving product security and assurance. Testing models employed by the vendor community should be examined to understand how these tests add value at minimal additional cost and time.

Recommendation: Experienced vendors, consultants and evaluation labs with approvals from NIAP should provide guidance on how to maximize reuse of evaluation evidence to vendors and evaluators. This would benefit vendors whose products have already gone through evaluation.

Recommendation: NIAP and the other international CC Schemes should develop a mutually acceptable means by which minor product changes (e.g. typographical errors in documents, code version number changes, minor bug fixes) result in only minor disruptions in the evaluation process. Some flexibility must be accommodated for the fast-moving IT COTS industry.

6.4 Increase customer demand for Common Criteria evaluated products

The benefits of training and the availability of current and accurate information are crucial to the success and effectiveness of an evaluation Scheme. Such information exchange can help identify and alleviate redundant or misguided efforts ultimately reducing cost and maximizing the benefits of the Scheme.

6.4.1 Current Landscape

The process control industry is developing PPs for systems used in that industry. The financial industry decided to develop their own parallel BITS standards and have mapped their requirements onto CC. Aside from these few examples, in the U.S., there has been very little interest and adoption of the CC in the private sector. Vendors have little incentive to undergo the costly and time-consuming evaluation effort without larger private sectors markets embracing CC. Much of the reason for duplicative efforts and lack of customer demand for certifications is the lack of awareness of the capabilities and benefits of CC evaluations.

Customers need more training, education, and information about CC capabilities and benefits. Customer education should help reduce duplicating efforts and enhance the demand for CC certifications. Customers need to understand the role they play in ensuring security of the international information infrastructure. They need to understand how they can articulate their requirements effectively using tools provided by the CC such as PPs and functional and assurance packages.

As customers become more aware of security issues and better able to articulate their security needs, vendors will be better able to compete to meet those needs. Market forces will drive security as a competitive issue and catalyze a cultural change in the IT industry to become more secure.

Customers also need to have reliable, up-to-date, international sources of information related to the CC and associated Schemes, including available training and product evaluation statuses. The individual Scheme websites provide some valuable information. The former www.commoncriteria.org website is currently being re-worked. Some customers make their buying decisions based on what appears on these websites, so it is important that the information is complete and reliable.

It is important to minimize the number of evaluations a product must undergo in order to demonstrate how it meets the requirements from multiple vertical markets. That is, a product should not have to undergo X number of evaluations from X number of different markets. CC, coupled with strong mutual recognition, will reduce the number of different types of evaluations a product would need and create the critical mass necessary for vendors to be able to justify the cost and effort required to execute the evaluation.

6.4.2 Gaps and Recommendations

Recommendation: Vendors and NIAP must engage in increasing the recognition of CC into markets both vertically and horizontally in order to amortize evaluation costs and effort across a broader customer base.

Recommendation: Evaluation labs and consultants should promote their training services more to product purchasers to create more demand for evaluated products. Vendors should relate their experiences at sessions at the International CC Conferences or other public forums. DHS and NIAP should promote the benefits of CC to customers.

Recommendation: NIAP should be proactive in providing current and accurate information about its processes, policies, and international CC activities. New developments such as the evaluation maintenance program should be announced to all vendors that have products in evaluation or have certified products.

Recommendation: Customers should promote an environment of competition on security and assurance. Customers should learn to articulate their security needs in terms of CC language (PPs) and expect vendors to compete to meet those requirements. See recommendations for PPs.

Recommendation: The www.commoncriteria.org website should be reinstated and be developed into a clearinghouse of information and training for customers and vendors. The webmasters and sponsors of this website

should ensure that the information is up-to-date and complete. In particular, current and accurate product evaluation status is important.

Recommendation: BSA, ITAA and TechNet and their member companies should discourage the development and adoption of industry-specific and country-specific evaluations.

6.5 Improve the use and utility of Protection Profiles

The CC defines Packages and PPs to allow users to define their own requirements. The CC offers seven pre-defined assurance packages (EAL 1 through EAL 7) and many PPs have been and are being developed. In order to be useful, these constructs need to be both achievable and meaningful.

6.5.1 Current Landscape

PPs are developed to articulate customer requirements and compare products against those requirements. By comparing products against the same PPs, customers can do the "apples-to-apples" comparisons of products they seek. This also addresses the issue that vendor ST claims vary widely today. Standard metrics will emerge in PPs for customer groups with common environments, threats, objectives, policies and requirements. Some PPs today are too specific and reflect old technologies. This will lead to stifling innovation. Vendors should be given more flexibility to address threats and objectives in new, innovative and more secure ways. PPs should not over-specify.

Defining the TOE boundary is complex and prone to evaluation delays when not all of the TOE components are designed, developed, delivered from a single vendor. This requires more time to explain and clarify to the evaluators and sometimes it is impossible to meet a requirement when parts of the requirement are satisfied by these different components

The NSA developed many of the existing and emerging PPs. The issues related to these PPs are discussed in the NIAP Review inputs section of this report.

The CC was also designed to support component-level evaluations. This capability has been forgotten in the current implementations. We need to enable product "grading" against requirements rather than "all or nothing" evaluations against PPs. Grading allows market verticals to define their unique threats, objectives and requirements without creating an RFP for a custom product. Vendors can submit products for evaluation and compare it against PP requirements. This avoids the issue of X number of PPs and X evaluations for a single product.

Cross-industry customer and vendor forums need to be developed to define common threats. If commercial systems and COTS products will continue to comprise the bulk of resources employed in the national and international information infrastructure, these products need to meet standard requirements, not just industry-specific requirements. All systems deployed on the Internet are exposed to the same threats. These threats need to be clearly articulated across industries. Open forums and standard bodies will help to define and apply these standards. Technologists will be expected to weigh-in with innovations on how to meet old threats in new ways and how to meet new threats. This means there must be flexibility built into requirements to take advantage of these new technologies. There must be mechanisms for providing assurance that these new technologies indeed provide better security.

Currently, the NIAP interprets the CC narrowly, so that a given TOE cannot utilize support of its environment in meeting requirements. This limitation is being debated in the NIAP community, but requiring that the TOE solely meet some requirements poses significant problems for products, especially application software products that are developed on top of operating systems, networks, and other products. Allowing requirements to be met by the TOE and the Environment greatly increases the utility of PPs as long as the interactions between the product and the environment are clear and can be met when the product is deployed. Note that it remains to be seen how or whether the next version of the CC (version 3.0) will deal with this issue.

Alternative standards have already been developed to capture the requirements of some large vertical markets. We need to examine "BITS Program" (financial sector) and T1.276 (telecom sector) to understand how these articulated requirements can map to PPs and determine whether they "over-specify."

ICSA Labs, a division of TruSecure, and others develop and execute "performance" tests on products such as firewalls and anti-virus software. These tests are intended to check products against the common or standard set of attacks. In the anti-virus case, tests are run against the WildList set of viruses. These types of performance tests complement the tests conducted in CC evaluations. These established performance tests should be carefully examined before attempting to duplicate this effort to cover customers' performance requirements.

In addition to performance testing, interoperability testing is currently used to ensure system components work together securely. Security technologies such as virtual private networks (VPN) and authentication servers need to work with other devices in a secure manner. PPs for such technologies should not assume all implementations would interact identically. The security industry has created a number of tests for interoperability between products and customers have demanded that these tests be passed before they purchase.

Vulnerability assessment is a valuable part of evaluation. Vulnerabilities seem to be the root of many serious intrusions in today's systems. Customers can benefit from having all products evaluated for vulnerabilities. These tests should be against a standard set of tests and should be updated periodically.

6.5.2 Gaps and Recommendations

Recommendation: NIST, customers, vendors and CC consultants and/or evaluators should develop consortia to develop and vet PPs. The coalition of all of these parties will ensure that the requirements are realistic and that the appropriate technologies can be delivered to address the needs. The requirements and vetting models used by organizations such as ICSA should be examined. The status of this activity should be checked in September.

Recommendation: These consortia should develop more PPs for more product types especially application products. By having more people involved in the PPs development process, the more PPs can be developed. This, of course, means that participants need to be properly educated in developing solid PPs and applying the appropriate EAL requirements.

Recommendation: These consortia should investigate how "performance" and interoperability testing could complement PPs requirements to satisfy customers' security and assurance needs.

Recommendation: NIAP should support investigations into how CC requirements can be met by a combination of the TOE and the Environment can be made practical and include customers, vendors, and consultants in this exercise.

Recommendation: Investigate how products can be "graded" against multiple PPs simultaneously. This is needed to avoid having to evaluate the same product multiple times against multiple PPs.

Recommendation: DHS, NIAP, customers, and vendors should support investigation into research opportunities for system of components security. Investigation should be conducted to see if current research is adequate or whether additional research should be funded.

Recommendation: PPs at any EAL or assurance package should include vulnerability assessments against a standard set of vulnerability tests.

6.6 Improve product security through Common Criteria

While not a direct goal of the CC itself, it is generally believed that evaluations can result in the improvement of product security. In addition to product security improvements inherent in the market-driven competitive process, improvements happen when vendors enhance their products to meet specific demands of customers, such as those specified in a PP, and also occasionally when evaluators find problems with the products they are evaluating. As identified below, improvements also come in the form of improved development processes that can mitigate the introduction of errors in the first place.

6.6.1 Current Landscape

Many vendors do not understand and have not realized the benefits of CC evaluations to their own internal product development processes. Vendors can improve their development, delivery and support processes and products to be more secure and pass evaluations readily if they were given more training on CC. Today, CC evaluations are generally (in the U.S.) treated as a "checkbox" procurement item. There is a tremendous opportunity to help vendors recognize the value of evaluations to improve the effectiveness of their internal processes and product security. This can be a catalyst for cultural change in the product development (especially software) industry and improve the overall security of the critical information infrastructure

Those vendors that have experienced several product CC evaluations have attested to security improvements in their product development processes. Vulnerability assessments, testing strength of function, assuring secure delivery and other CC assurance tests help vendors improve the security of the features of their products and their development, delivery and support processes. All of these activities contribute to reducing security defects and vulnerabilities and thus reduce support costs. In a sense, these vendors are introducing the evaluation processes employed by the independent labs into their own processes. One can imagine that at some point, a self-certification program, subject to the same rigorous evaluation and audit requirements as the third-party evaluation program, may reduce the cost and time burdens of third-party evaluations and move the industry toward a cultural change.

It is difficult to find competent, experienced evaluators and knowledgeable consultants. There are only limited experienced and knowledgeable vendor resources to shepherd CC evaluations. There is a strong need to increase the pool of knowledgeable resources to maximize the improvement of vendor internal processes and to create a greater emphasis on security.

6.6.2 Gaps and Recommendations

Recommendation: Vendors need more reliable education and training on how to conduct effective CC evaluations. Moreover, vendors need to gain greater awareness of the impact CC evaluations can have on improving their organizational processes. NIAP and DHS can serve as a clearinghouse of information about reliable education, training and consulting resources.

Recommendation: Experienced vendors should share their experiences and how they have derived benefits from improved processes due to CC evaluations. They can share this information through articles and sessions at conferences.

Recommendation: There may be an opportunity for a university business school to conduct research on quantifying the benefits of process improvements and improved product security. DHS should consider providing funding for such research.

7.0 GLOSSARY

BITS	Technology arm of Financial Services Roundtable and manages the BITS Product Certification Program
CC	Common Criteria for Information Technology Security Evaluation. Established as ISO 15408.
CCEVS	Common Criteria Evaluation and Validation Scheme
CCIMB	Common Criteria Interpretations Management Board
CCMRA	Arrangement on the Mutual Recognition of Common Criteria Certificates in the Field of IT Security
COTS	Commercial Off-the-Shelf
DHS	U.S. Department of Homeland Security
DOD	U.S. Department of Defense
DODI 8500	Dept. of Defense Instruction on Information Assurance Feb. 2003
EAL	Evaluation Assurance Level
FIPS	U.S. Federal Information Processing Standard
GOTS	Government Off-the-Shelf
ICSA	Division of TruSecure Corporation
ISO	International Organization for Standardization
NIAP	National Information Assurance Partnership
NIST	U.S. National Institute of Standards and Technology
NSA	U.S. National Security Agency
NSTISSP #11	National Security Telecommunications Information Systems Security Policy #11
NVLAP	National Voluntary Laboratory Accreditation Program
PP	Protection Profiles
RFP	Request for Proposal
ST	Security Target
TOE	Target of Evaluation
WildList	WildList Organization

8.0 ACKNOWLEDGMENTS

The following is an alphabetical list of those people who participated in or contributed to the Common Criteria, NIAP Review and Metrics Working Group and the development and review of this report.

Name	***Organization***
Jim Arnold	SAIC
Dave Aucsmith	Microsoft Corporation
Glenn Brunette	Sun Microsystems
Richard Caliari	Harris Corporation
Diann Carpenter	Cable and Wireless
Denise Cater	Syntegra
Larry Coleman	Department of the Navy
Ruth Cowell	Department of Defense
Mary Ann Davidson	Oracle Corporation
Lawrence Dobranski	Nortel Networks
Murray Donaldson	Decisive Analytics Corporation
Daryl Eckard	EDS
Jeremy Epstein	webMethods
Eric Guerrino	Bank of New York
Tim Hackman	IBM
Duncan Harris	Oracle Corporation
Wesley Higaki	Symantec Corporation (Working Group champion)
Paul Hoffman	VPN Consortium
Katie Ignaszewski	Internet Security Systems
Wendi Ittah	Check Point Software Technologies
Matt Keller	Corsec Security
Chris Klaus	Internet Security Systems
John LaCour	Zone Labs
Shaun Lee	Oracle Corporation
Sheila McCoy	Department of the Navy
Simon Milford	Logica
Ann Patterson	BITS
Judy Petsch	Department of the Navy
Ray Potter	Cisco Systems
Doug Sabo	Network Associates
Marty Schulman	Juniper Networks
Ray Snouffer	NIST
Catherine Webb	IBM
Paul Zatychec	EWA-Canada