Response to Request for Information published in the Federal Register / Vol. 75, No. 144 / Wednesday, July 28, 2010 / Notices

AGENCY: Office of the Secretary, U.S. Department of Commerce; National Institute of Standards and Technology, U.S. Department of Commerce; International Trade Administration, U.S. Department of Commerce; and National Telecommunications and Information Administration, U.S. Department of Commerce. ACTION: Notice of inquiry.

SUMMARY: The Department of Commerce's Internet Policy Task Force is conducting a comprehensive review of the nexus between cybersecurity challenges in the commercial sector and innovation in the Internet economy. The Department seeks comments from all stakeholders, including the commercial, academic and civil society sectors, on measures to improve cybersecurity while sustaining innovation. Preserving innovation, as well as private sector and consumer confidence in the security of the Internet economy, are important for promoting economic prosperity and social well-being overall. In particular, the Department seeks to develop an up to- date understanding of the current public policy and operational challenges affecting cybersecurity, as those challenges may shape the future direction of the Internet and its commercial use, both domestically and globally. After analyzing comments on this Notice, the Department intends to issue a report that will contribute to the Administration's domestic and international policies and activities in advancing both cybersecurity and the Internet economy. DATES: Comments are due on or before September 13, 2010.

ADDRESSES: Written comments may be submitted by mail to Diane Honeycutt, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8930, Gaithersburg, MD 20899. Submissions may be in any of the following formats: HTML, ASCII, Word, rtf, or pdf. Online submissions in electronic form may be sent to cybertaskforce@doc.gov. Paper submissions should include a three and one-half inch computer diskette or compact disc (CD). Diskettes or CDs should be labeled with the name and organizational affiliation of the filer and the name of the word processing program used to create the document. Comments will be posted at http:// www.ntia.doc.gov/ internetpolicytaskforce and http:// csrc.nist.gov.gov.

atsec thanks Office of the Secretary, U.S. Department of Commerce; National Institute of Standards and Technology, U.S. Department of Commerce; International Trade Administration, U.S. Department of Commerce; and National Telecommunications and Information Administration, U.S. Department of Commerce for the in depth information provided in the Federal Register notice and wishes to respond with the comments below. We trust that this information will meaningfully contribute to meeting and furthering your goals for improvement.

atsec information security is a commercial company based in Austin, Texas. atsec maintains information assurance assessment laboratories under U.S. Government NIAP , NIST and GSA programs as well as the Payment Card Industry Security Standards Council and other national assurance programs and has assisted with the development of some national security assurance programs. atsec has completed close to one hundred Common Criteria evaluations, several conformance test reports within the NISTS's CMVP, CAVP SCAP program, PIV Program and in the GSA FIPS 201 Evaluation Program. atsec assists customers in preparation for ISO/IEC 27001 and ISO/IEC 27002 conformance, HIPAA and FISMA and in several other areas of consultancy including the provision of an independent physical security testing facility and in topics related to export controls.

atsec has worked with many leading IT developers, including Apple, Dell, Hewlett-Packard, Honeywell , IBM, , Oracle, , and Red Hat as well as mid-sized and a small businesses for over ten years.

We work also with formal IT security assurance assessment schemes in other countries including Germany and Sweden in our pursuit of service of supplying IT security assurance to the commercial sector.

atsec actively works with the INCITS CS1 committee contributing to the development and improvement of cybersecurity standards in the US and internationally through the ISO/IEC JTC1/SC27 committee.

General comments

We support the points outlined in the NOI but note that there is a lot of discussion and focus in on a reactive approach to cybersecurity in the language of the NOI. atsec believes that a two pronged approach is fundamental including not just reactive measure but also preventive activities.

In this response to the NOI atsec contributes information, based on our experience in the Commercial sector, on the topics of Quantifying the Economic Impact, Global Engagement, and Product Assurance.

Quantifying the Economic Impact

Prior to releasing this NOI, the Task Force conducted listening sessions with a wide range of stakeholders in order to understand the issues that have the greatest bearing on cybersecurity preparedness and continued growth of the Internet economy. During those conversations, the Task Force heard that while cybersecurity threats continue to pose challenges for Internet users and services providers, it appears difficult to assess the macro- and microeconomic impact of cybersecurity incidents with current tools. It is hard to manage that which one cannot measure. Losses related to Internet fraud (e.g., payment fraud, identity theft, credit card fraud) are collected and reported to various government and private entities. However, data that describe the economic impact of cybersecurity incidents more fully and completely, either at the firm or sector level, are not readily available. Not only are losses difficult to quantify with today's tools, but it appears to be difficult to assess in economic terms the return on investments achieved via security measures. Measures of business and consumer investment in security-related activities lack a common reporting entity or information aggregating mechanism. The availability of authoritative, aggregated data on cybersecurity investments and losses from cyber incidents might yield a quantitative picture of the economic impact of cyber intrusions and attacks. Such data would enable industry and the government to evaluate the severity of cybersecurity threats and emerging trends and to make informed decisions about the trade-offs of different cybersecurity strategies and investment options. We seek comment on the following questions: How should a data gathering and analysis system (or systems) be fashioned to facilitate the collection of well-defined, consistent metrics to measure the financial impact of cybersecurity incidents and investments in cybersecurity protection? What would be the implementation challenges? Are there adequate incentives for businesses to provide information about security breaches, data security losses, and cybersecurity investments? It would be beneficial from a national perspective to have a greater understanding of the financial costs and benefits of different cybersecurity practices. Does the private sector, however, lack incentives to share information at the firm level? What are reasonable means to acquire the data necessary for greater understanding? At what level of granularity should data be collected and analyzed? What would be the appropriate entity to perform collection and analysis of the data? Aside from assessing the known costs of cyber intrusions and attacks and of cybersecurity measures, what other data would be helpful to better understand the question of whether at the firm, sector and national levels enough is being done to adequately protect the nation's information and communications systems? Can the opportunity costs associated with inadequate security be estimated in some way?

"It is hard to manage that which one cannot measure" is a quote that is often attributed as having emerged from the Quality movement in the middle of the last century. There are several other principles that stem from that same movement including "Cease dependence on mass inspection to achieve quality. Instead, improve the process and build quality into the product in the first place." Dr Deming also said "*The most important things cannot be measured.*" With this statement Deming hoped to describe the concept that some important long term issues cannot be measured in advance.

Accordingly we would recommend that consideration be given to a suitable sampling system for obtaining metrics, if necessary promoting researches on this topic in order to obtain meaningful measures that are statistically relevant without relying on a "100% inspection" approach.

There are well-known and significant pitfalls in implementing measuring systems. One important consideration is that it is easy to focus only on those items that are easier to measure, and neglect those things that pose challenges in obtaining objective repeatable measures. It may be tempting to put in place "low hanging fruit" measures and then focus resource on those items (prioritized of course by using the metrics) whilst completely

forgetting that there may be more significant, harder to measure items that are now being neglected purely because they are difficult to measure.

Effective measurement and related statistics require capturing all relevant events. In the case of cyber security it would require the complete knowledge of all security related incidents in order to completely analyze them and determine their cause and potential impact. As pointed out in the NoI, most stakeholders are reluctant to talk about security incidents, believing that it puts a bad light onto them. Developers will not publish sufficient details of security flaws detected in their products allowing users to identify if that flaw has been exploited and consequently a user can not measure how the existence of the flaw has impacted his assets. Even in cases where companies or other organizations have detected attacks on their IT infrastructure, they usually are reluctant to release any information about the impact such an attack had. They fear a negative impact on their business if information about attacks on their IT infrastructure gets public.

On the other hand it is also hard to impossible to measure the cost-effectiveness of proactive security measures. Unlike in the safety world where one can work with statistics based on the assumption that the probability of a specific event to happen is independent of the measure being in place (the probability of a car being involved in an accident is independent from the car having airbags or not), such statistics can not be applied when it comes to security. As an example assume a corporation that uses expensive cryptographic techniques to protect their communication. Measurement shows that none of their communication links has been attacked in the past year. Naively one could assume that their protection measure is not cost-effective and therefore can be removed. The company can be sure that after some (usually quite short) time period potential attackers detect that they have dropped their protection measure and the number of attacks on the company's communication links will rise sharply.

Any model that attempts to measure the effectiveness of cyber-security measures has to take this problem into account. It has to model the behavior of potential attackers, including their ability to learn from their experience and feed this back into the model. This requires constant monitoring of attack patterns and methods and the determination of the potential impact of those attacks and how current security measures deal with them.

A number of initiatives are already in place to support such constant monitoring. Computer Emergency Response Teams (CERTs) as well as Mitre's CVE and NIST's National Vulnerability Database (NVD) program collect information about vulnerabilities and issue advices, Mitre's CAPEC initiative tries to identify common attack patterns, and NIST's Security Content Automation Protocol (SCAP) attempts to build a common language to address security problems for systems in operation. While all this helps to deal with the security problems and flaws in today's IT systems, little is done to have security and assurance being an integral part of IT systems and their architecture that is designed into the systems rather than added later on to compensate for security problems introduced by an inadequate architecture or the side effect of new "features". A major breakthrough can only be achieved when architectures, functions, communication protocols and features of IT systems are analyzed for their security impact starting at the early stages of the design and traced down to the implementation. We are currently on the track to restrict ourselves to the management of vulnerabilities rather than building secure systems from scratch. The level of security one can achieve with such an approach is limited and may not be sufficient for future systems operating in an environment that gets more and more distributed thereby increasing the attack surface and the number of people that may perform sophisticated attacks.

Global Engagement

Cybersecurity issues are global. Companies want to design, manufacture, and test their products to make them available for sale in a global marketplace. Many in industry have described fear about the potential for balkanization of the global marketplace due to a proliferation of mandated, sometimes unique cybersecurity standards and conformity assessment requirements among nations—leading to a diverse patchwork of national requirements that can inhibit trade. Such unique national standards and conformity assessment requirements illustrate one way in which some foreign governments seem to be deviating from international norms by using security standards as a de facto entry barrier to protect domestic interests from foreign competition.

We request comment on what other cybersecurity-related problems U.S. businesses may be experiencing when attempting to do business in foreign countries. Please specify discrete areas of concern, such as foreign governments requiring access to product source code.

Do U.S. businesses confront unfair competition when competing against nationally controlled companies?

The attempt to install trade barriers to favor national industries has always been attempted and the IT industry is no exemption. On the other hand areas related to national security always had their own rules where nations do want to have better control on the products used in those areas in order to avoid security problems.

With the Internet we now have a global infrastructure that is of high importance for the national security of many nations, not only the U.S.. As a result many nations attempt to pose restrictions on products used in what they regard as national security systems, ignoring that the Internet is global, not national.

This trend is larger in countries where the distinction between industry and government is weak and in those countries fair competition seldom exists.

If so, in which countries?

?

How can the U.S. Government better encourage the use of internationally accepted cybersecurity standards and practices outside of the United States?

The U.S. already shows a strong presence in international for a development such as ISO, IEC, and IEEE. The U.S. leadership in the development of such standards is clear.

The U.S. should promote the adoption of international standards within the U.S. For example ISO/IEC 27001, ISO/IEC 27002 could be used much more effectively in the U.S. and promoted by NIST.

Another example is the use of Common Criteria by the U.S. By supporting the CCRA and implementing its policies as intended the use of the Common Criteria and ISO/IEC 15408 standards would be encouraged throughout the world. Developing effective leadership in supportive items such as

The promotion of effective, reasonable, community accepted protection profiles that can be validated by a strong national scheme (i.e. the U.S.) and recognized as applicable internationally by developers based abroad would do much to encourage and develop the effective use of the standard around the world

- Provision within the U.S. of high quality evaluator and validators training would also promote the adoption of the standard and do much to increase the standards of evaluation/validation in the U.S.
- Improvement of the controls in place to ensure the flow of information required to trust assurance assessments performed in other countries. With the Common Criteria some controls are already in place, but improvements to those are required. With other standards such mutual recognition of assurance assessment does not exist and need to be established. Continuous supervision is the solution on the international level to establish trust into assessments performed.

The U.S. should promote the development and promulgation of internationally agreed recognition arrangements at suitable commercial levels. The CCRA has been seen to be successful and further development of this agreement, and the establishment and development of similar agreements should be considered.

Are there more effective ways for the U.S. Government to engage countries that deviate from international norms (i.e., bilaterally, multilaterally, through technical dialogues, at an overarching political level, all of these or through other mechanisms)?

Yes, in addition to the strong technical contribution the U.S. should:

actively promote and strengthen the use of internationally recognized standards within the U.S.

- effectively collaborate with those nations that already adopt international norms appropriately
- promote and support internationally agreed recognition agreements
- Actively work to ensure that existing schemes do not deteriorate or become stagnant which allows other nations to see an opportunity to develop their own nationalist agenda
- Actively work on schemes to assess for compliance with such standards, which includes active international monitoring of such schemes operated in different countries to ensure a comparable level of assessment.

This should be done at all levels including technical and political levels as well as within our own borders.

Would a set of internationally accepted ‘‘cybersecurity principles’’ in the area of standards and conformity assessment procedures be useful?

Yes, Items such as the OECD Principles of Corporate Government, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data provide well-accepted input from the highest levels to the development of standards and national policies.

Agreement on a simple set of “cybersecurity principles” would do much to guide the development and implementation of current and future norms in many key international organizations. Such principles would help reduce the risks of introducing unfair competition and trade barriers if standards are not internationally recognized or aligned. This strategy for promoting harmonization is seen in many areas of co-operation, not just in the cybersecurity domain.

Developing such a set of “cybersecurity principles” can only be the first step to establish a common baseline. Later those principles need to be supported more precise standards that detail and regulate the technical aspects as well as the operational (management) aspects expressed in those principles.

If so, what role should the Department of Commerce play in promoting such internationally accepted principles?

The Department of Commerce should play an important role in representing the U.S. interests in such international fora by not only promoting those principles but also define the areas for further standardization derived form those principles and actively participate in the development of such standards.

Product Assurance

As noted above, many cybersecurity issues are global, but product assurance is one global issue that warrants particular attention. In the course of conversations with hardware and software developers, the Task Force has heard repeatedly that current domestic and international government product assurance efforts for many products can contribute to costly time-to-market delays, as well as unnecessarily expensive products. Several companies felt that the current U.S. Common Criteria assurance scheme is incompatible with industry product development and maintenance schedules and practices, and that the security assurance derived from many national assurance requirements and evaluation schemes is highly questionable. Additionally, participation in international mutual recognition schemes is, reportedly, so limited that some in industry see themselves as expending very significant resources to satisfy a range of varying security requirements and processes among nations in order to compete in a global market. Industry members have expressed a desire for assistance in improving mutual recognition in the product assurance realm. We seek comment on the following matters.

Background

Product assurance is an important topic. Without product assurance every attempt to build and operate a system securely in cyberspace is bound to fail. With this process and the associated activities we seek to provide confidence that the products available meet their security objectives and don't have security critical side effects. This is a critical measure at all levels of abstraction within the cyber space. It is vital that the products that represent the components of our cyber system say what they do and do what they say. This allows the architect of a system operating in cyberspace to identify where the security critical components of his system are and determine the level of assurance required to ensure that those components can withstand the type of attacks that have to be expected.

This fact is important because not all IT products are equal in their contribution to the attack surface a system exposes. Also the effect of a security breach may be different depending on the component in which the breach occurs. In properly designed systems, a security breach in an application can well be confined to that application, not affecting the underlying platform or other key components and allowing other applications to continue their operation. Items such as operating systems, virtualization software, smartcards, key application software such as databases are widely used in a variety of IT operating scenarios and for the basis for the platform on which many of the applications are hosted. A security breach in the underlying platform or some key components has a significantly larger impact potentially affecting all applications in the system. Therefore the assurance required for the products building the underlying platform is usually significantly higher than the assurance required for a specific application software. In such a composition environment we cannot build an infrastructure based on low-assurance (confidence) fundamentals and then expect that the applications and services using them have anything other than a low-assurance.

Missing from this NOI is a discussion and questions relating not only to product security assurance, but also to systems and operational security assurance. As stated earlier, product assurance is a necessary but not sufficient requirement for building and operating systems that can securely be operated in cyberspace.

Similar concerns to those mentioned in the NOI are expressed about the assurance provided by programs such as NIST's FISMA implementation program requiring certification and accreditation for federal agencies' and their contractors' systems supporting agency operations and assets.

The requirements derived from U.S. legislation such as the Federal Information Security Management Act of 2002 (FISMA) etc. are promulgated through a variety of disjoint product assurance programs. This top level legislation has resulted in many and various derived policies given by various agencies and other executive bodies that contribute to an array of program-related issues and that those vendors must navigate in order to satisfy several customers. Sometimes these policies are conflicting.

Providing security assurance does impose additional costs and time. The higher the assurance required, the greater the costs and time needed to provide the assurance. The task force should be aware therefore that some costs and time delays are inevitable if assurance is required and that especially for vendors who are not accustomed to providing such assurance these costs represent new or additional costs to those applicable in the past. With the implementation of more assurance comes some pain. However, with a good product assurance process these overheads are reasonable and not excessive and pay off due to reduced effort for flaw remediation and distribution of ifxes.

Assurance is no property of a product that can be brought in by an after-the-fact assurance assessment. Assurance does not “just happen”. It has to be built into the product beginning from the early design stages allowing an assessment to confirm the assurance.

Delays caused by an assurance assessment process are inevitable when the assessment starts after the product development has finished. Problems identified during such an assessment, which include problems with missing information required to perform the assessment, are hard to fix at this stage and often cause the delay industry complains about. On the other hand there are examples of assurance assessments performed in parallel with the product development that finishes at the time or shortly after the product has entered the market. One of the most complex Common Criteria evaluations, the evaluation of IBM’s mainframe operating system z/OS is an example where the assessment usually finishes shortly after the evaluated version is available and probably long before customers have adapted their operational environment to the new version and start to use it for production. Nobody would expect a manufacturer of an airplane or a car to start the safety assessment of a new plane or car after development is completely finished. In the classical engineering areas it is common to have development and assessment been done in parallel and this is where we need to get to also in the IT sector.

The NIAP’s current strategy of reducing the security assurance required in order to reduce the costs and time involved addresses only the complaint about the costs and time to vendors. Costs and time ***will*** be reduced by this policy but as a result, of course, the confidence in the products evaluated is reduced. There is no incentive for vendors to include assurance measures in their development process. Such a policy is counterproductive to the goal of increasing product assurance. We are unsure how this contributes to national cyber-security. The statement from the NIAP at various communication meetings that some (low) security assurance for the majority of products is better than no assurance is only true if the basic platform on which they rely has high assurance. Reducing the assurance for the base infrastructure of cyberspace is a backward, detrimental, harmful policy. We want to point out that many key products like operating systems and database management systems today already provide a significant higher level of assurance than most application programs. They have been continuously evaluated at Common Criteria assurance levels of EAL4 and most vendors of those types of products have invested a significant amount of money and time to improve their development processes and products in order to increase assurance. As a result the assurance that can be placed in operating systems, firewalls, routers, and database management systems (most of which have been evaluated at EAL4) today is quite good.

On the other hand more and more security problems are detected in applications that directly establish communication links (e. g. browser or multi-media applications) or that interpret potentially hostile data downloaded from the Internet (e. g. multi-media viewer, word processors). Those applications often lack the security controls required and also have

implementation flaws that an attacker can easily detect and exploit. Many vendors of application are not aware of general attack patterns that may apply to their product and the technology they use to implement it, nor is their software development process mature enough to provide even a basic level of assurance that the product can withstand even simple attacks. Whenever such an application is configured to execute with almost unlimited access rights or with administrative rights on the underlying operating system, a vulnerability in the application can be easily used to attack the underlying operating system or database management system.

There has been no public discussion on what reasonable costs and time constraints for providing assurance would be acceptable, and no analysis in the "complaints" about the security-maturity of the vendors making the complaints. As stated above, assurance needs to be designed into a product. Some vendors have the false perspective of an assurance assessment being a substitute for missing elements in their development process, and in those cases the assurance assessment is very time and cost consuming and may still result in a "fail" verdict.

It is also important to remember that assurance costs to vendors not only components relating to U.S. government assurance schemes but may also include commercial schemes (such as the Payment Card Industry), customer related requirements to meet legislation for which there is not current formal government sponsored assurance program (e.g. HIPAA) and voluntary de-facto programs (such as those operated by ICSA) as well as for those vendors with products marketed and sold outside the U.S., other international assurance programs.

Do current U.S. Government product assurance requirements inhibit production of timely security components and/or security-enhanced IT products and systems?

Yes, U.S. Government product assurance requirements often inhibit production of timely security components and/or security-enhanced IT products and systems. This is often not caused by the requirements themselves, but the way they are implemented and handled by the U.S government agencies involved.

The requirements impose some constraints as an additional process is integrated into the product development cycle. However it is the programs and the associated processes and activities that are implementing the requirements that can affect items such as cost and time. What is a reasonable overhead in terms of time delays to product releases is determined by the market and the stakeholders.

Accreditation of labs to operate under the several programs imposes unnecessary time and cost constraints to the labs and the programs involved. For example ISO/IEC 17025 accreditation needs to be repeated by laboratories for each program with which they are accreditted even though the laboratory systems are the same within each laboratory. This is inefficient and a waste of program and laboratory resource and causes additional costs to be transferred to vendors.

By their nature different assurance paradigms bring different characteristics to the assurance process:

"Evaluation" paradigms such as Common Criteria, ITSEC, Orange book and the various criteria-based methods allow for more open-ended analysis of products security features. They are flexible and can be applied to a wide variety of IT products with security functionality at different assurance levels. We note that the nature of evaluation engenders a potential risk for local variation simply because the test vectors and specification is flexible for each evaluation project. This in turn means that the schemes must be managed (i.e. monitored and controlled) even more closely than is necessary in a conformance based model in order to ensure that quality results are obtained.

"Conformance" paradigms such as FIPS 140-2 and the FIPS 201 schemes are more restricted in the assurance given. Conformance schemes ensure that the product conforms to the cited standard or specification, but does not allow the flexibility of looking beyond that standard or specification to provide for evolution of the threat model or of technology. Conformance is good for primitive products or components such as cryptographic algorithms and random number generators that form the base level of the products and systems that we use. An example of a conformance scheme that shows excellence is NIST's cryptographic algorithm validation scheme. Certifications of conformance are managed quickly and cheaply and provide a lot in terms of assurance of the core components for which they form the base.

By making requirements, establishing programs only on the needs of some government agencies (i.e. omitting to establish schemes that serve the needs of those other entities that form the critical infrastructure) and then under-resourcing the established programs that are responsible for measuring, validating or certifying products to the various assurance schemes and standards mean long delays and increase the costs to product developers and vendors.

There is also a lack of co-operation with vendors, labs and user in most of the programs. The Common Criteria have been accepted and widely used in areas where all stakeholders have jointly developed Protection Profiles and corresponding evaluation methodologies for specific areas. The smart card industry is the most prominent example of such an area and usefulness of Common Criteria evaluations even at higher assurance levels (EAL5 and higher) is generally accepted by all parties involved. As a result almost all smart chips and operating systems as well as most critical smart card applications undertake a Common Criteria evaluation for each major release. This shows how an assurance assessment scheme can be successfully implemented providing all parties are actively involved in the definition of the scheme.

The printer manufacturers are another example of a group that developed a security standard for multi-function printers [5] and also developed Common Criteria Protection Profiles based on this standard [6]. The security functions have been derived from customer requirements and the group involved a Common Criteria lab to assist in the development of the Protection Profiles, ensuring that the security requirements are correctly expressed and can be evaluated using the Common Criteria. Since the standard and the Protection Profiles have been developed by an industry group involving all major manufacturers of multi-function printer devices, acceptance of the Protection Profiles and the security requirements defined there is given.

Operating systems have always been the target of assurance assessments, because they are a key component within any IT infrastructure where security requirements need to be enforced. The security functions of operating systems have evolved significantly over the last 30 years, extending from pure centralized user management and access control to protecting data and communication links within a highly distributed environment where management functions and security decisions are performed based on information stored in separate repositories. Protecting communication links using cryptographic functions as well as firewall, filtering and intrusion detection capabilities are also now standard functions provided by operating systems. This major shift in the functions and architectures had not been reflected in the Common Criteria Protection Profiles at all until the major vendors of general purpose operating systems decided to participate in a group formed to develop a Common Criteria Protection Profile that reflects today's security requirements for server and client operating systems. This Protection Profile has been recently published and one vendor already has performed an evaluation based on this new Protection Profile with several others starting to follow. Again this seems to be a good start where the different stakeholders cooperate with the mutual benefit for all of them and their customers.

In the U.S. such common efforts by all parties have not been promoted. U.S. government Protection Profiles have usually been developed by NIAP or NSA without involvement of the vendors, labs or a wider user community. The result are Protection Profiles with

requirements that are sometimes unrealistic and often do not address the security problems users have. It is not surprising that those Protection Profiles are not well supported by industry and often vendors look for other schemes where compliance to those Protection Profiles is not mandatory to get into evaluation.

Also the development of FIPS140-2 lacks proper cooperation with the stakeholders. Drafts of the new version of FIPS 140-3 have been published for comment, but it is unclear if and how such comments will be addressed. There is little to no opportunity to discuss the comments with the developers of the standard. As a result the current draft of FIPS 140-3 has significant deficiencies with respect to software modules and hybrid modules (which will come up more and more in the near future).

In some cases delays in the development and publishing of standards (eg Common Criteria and FIPS 140-2) detriments the evolution and innovation in product security.

For example:

The CMVP is in charge of certifying information security products under the FIPS 140-2 standard and as such it plays a vital role in protecting the federal government against ever-increasing cyber security threats. After the Federal Information Security Management Act (FISMA) of 2002 removed the statutory provision that allowed agencies to waive mandatory Federal Information Processing Standards (FIPS), there has been a steady growth of the demand for information security product certifications under FIPS 140-2 standard. Currently, all information security products with cryptographic functionality used by the federal government must be FIPS 140-2 certified. Therefore, the CMVP is the effective gatekeeper between the federal consumers and the commercial providers of products. Thus, it is very important that the gatekeeper is not a bottleneck that prevents the smooth and efficient flow of products from the providers to the federal government consumers.

Unfortunately, the CMVP is in a crisis, unable to respond in time to the increased demand for product certifications. It is not the competency, the professionalism, or the dedication of the CMVP staff that results in this situation. The program is simply badly understaffed and it takes extremely long periods of time to certify products that have been independently tested by qualified labs, such as atsec's CST Lab, under the NVLAP charter.

As a result, all stake holders in the CMVP charter get hurt: the federal government cannot obtain in time the products it needs to protect the security of information circulating in its civilian and military branches; the commercial vendors of these products are affected badly since their engineering and marketing organizations cannot get a timely return from the investment they have made into improving the security and performance of their products to meet the letter and the spirit of the FISP 140-2 standard; the qualified testers at the CST Labs around the country are feeling de-motivated by seeing so much of their hard work aimed at meeting aggressive testing schedules of complex products get wasted by the prolonged wait; the CMVP staff feels frustrated and overworked.

In fact, the situation is so dire that if left unattended, the CMVP risks failing the very goals it was set to fulfill and ultimately going into oblivion.

NIST is looking into ways of improving the situation with the CMVP. NIST hired consultants to look into the problems with CMVP and atsec were canvassed for input. However we were left with concerns that the consultants are only looking into improving the existing internal processes and the adoption of tools as the means for improving the productivity of the CMVP staff. Although useful, these measures are addressing secondary issues and fall short of solving the core staffing problem affecting the CMVP performance.

The NIAP

The NIAP was established as a joint partnership between the National Security Agency and NIST. Conflicting objectives and draining of NIST resource in support of this scheme meant that non DoD stakeholders were effectively barred from entry in the U.S, scheme. Eventually NIST withdrew any technical involvement with the operation of the program, although they have maintained a role in ensuring that the basic quality standards of laboratories are maintained in accordance with the requirements of the CCRA.

The scheme fails in several areas to promote competency amongst evaluation facilities, formal training for validators and for evaluators, already established for many years in prominent schemes such as Canada and Germany have never been established, resulting in competency concerns about the standard of some U.S. evaluations. Proficiency in some technologies key to the U.S. national infrastructure, such as smart cards, have not been evolved in the U.S. assurance scheme.

Current NIAP policies severely undermine the intent of the assurance program in the US.

By implementing restrictive policies on entry into evaluation, delays in co-operatively producing and maintaining relevant protection profiles, restrictions on the assurance level (i.e. confidence) obtainable in IT products have caused not only time-delays but denial of service to vendors wishing to have their product assessed for assurance. It increases costs to US vendors as they must perform such assurance assessments in schemes operated by other nations. This causes resource issues in those other national schemes and engenders a poor reputation and frustration with the US product assurance scheme around the globe as the US seeks to take advantage of the CCRA recognition without contributing effectively.

Currently NIAP fail to listen effectively to their stakeholders, often requesting feedback and input as an afterthought. Whilst delays in the final validation are mitigated through the establishment of the VOR process, the delays are transferred to the beginning of the process in establishing a viable project for evaluation with the NIAP.

FIPS 201 EP

The service run for by the GSA for establishing conformance to the FIPS 201 standards is operated in a bureacratic fashion. It is so under resourced that when key staff take leave the effective operation of the scheme is put on hold.

An additional factor is that several programs exist within the U.S. Vendors who need to comply with the requirements implemented by several programs have additional costs and time factors involved. The risks of conflicting requirements are evident and composition of assurance when evaluations and tests are performed independently is a process fraught with problems.

Similarly accreditation of labs to operate under the several programs imposes unnecessary time and cost constraints to the labs and the programs involved. For example ISO/IEC 17025 accreditation needs to be repeated by laboratories for each program with which they are accreditted even though the laboratory systems are the same within each laboratory. This is inefficient and a waste of program and laboratory resource and causes additional costs to be transferred to vendors.

Do current assurance processes inhibit innovation?

The relationship between security assurance and innovation is complex and several factors need to be properly considered.

The individual specifications within Conformance assurance schemes by their nature tend to inhibit innovation. By this we mean that in order to meet a specification the product must comply with it precisely. Thus by regulating conformance to particular technical

specifications innovation is by definition stifled at that level. This is not necessarily a drawback, since innovations may have security critical side effects and therefore they first need to be analyzed for their security impact before being allowed in critical areas.

However, with proper knowledge and management of the security posture then innovation can still be properly accommodated within the scheme managing the specifications. As long as specifications are adapted to allow for innovations that have been analyzed for their security impact and found to not undermine security, the introduction of innovations in critical areas is just delayed, but not prohibited, This is standard practice in other engineering areas where innovations are first analyzed in depth for their impact before they are allowed to be used in critical systems.

In order to cope with innovations a process needs to be established that allows all stakeholders to identify where existing standards need to be adapted to deal with innovations. A formal process needs to be established where those stakeholders can discuss potential deficiencies of existing standards and come to an agreement how to evolve the standard to overcome those deficiencies. Standards developed by just one stakeholder without active participations of all other stakeholders are bound to fail.

The task force should also consider that there is a fine balance between rapid innovation and security and also note that there are differences in incremental innovation and disruptive innovation resulting in a radically-new technology.

A good example of this is the evolution of the cryptographic specifications managed by NIST. (i.e. the phasing out of DES, and the specification of new algorithms and modes such as the planned and reasonably well-executed transition from integer factorization cryptography (RSA) to elliptic curves over finite fields cryptography in order to keep pace with the evolution of the assurance required.) Adhering to vetted, provably-secure (in theoretical sense) technologies/algorithms is what allows correct balance between standardization and incremental innovation in these cases of primitive functions.

However if the specifications are not able to evolve in line with the evolution of technology and an evolving security ecosystem then the result can include an inhibition of useful innovation but may also cause a more disastrous built-in insecurity that emerges over time. For example the FIPS 140-2 specification has had difficulties in keeping pace with the evolution of smart-card technology and in allowing for the emergence of more complex hybrid modules (for example computer systems that have multiple hardware and software implementations of cryptographic functions).

There are concerns that the current FIPS 140-2 specification is stifling security technology innovation and may even be resulting in the specification of cryptographic modules that could be much more secure.

An example is the expected increase in the number of hybrid modules. In those modules the management functions (user management, key management, access management, system configuration), user authentication, and access control will be performed by software while the basic cryptographic algorithms will mainly performed in hardware. Today a pure software module can achieve a FIPS 140 Level 2 validation. If the vendor decides to just drop the software implementation of an algorithm (e. g. AES) and instead use the more efficient hardware implementation of this algorithm (which makes his module hybrid module), he can no longer achieve FIPS 140 Level 2, since hybrid modules are restricted to Level 1 only. With the current trend to extend to instruction sets of general purpose processors by cryptographic functionality, most cryptographic modules currently implemented purely in software will make use of the cryptographic functions in hardware (because they are usually significantly faster) and become hybrid modules. This obvious trend should be reflected in the FIPS-140 specification where hybrid modules are currently nor well represented and the restriction of the Level those modules can achieve to Level 1 is counterproductive.

We note that some disruptive innovations can be much more difficult to handle and unless they are theoretically proven to benefit security, slow adoption may be prudent allowing time to vet the potential and undiscovered new vulnerabilities these technologies may bring.

Evaluation paradigms are designed deliberately to ensure that innovation is not inhibited and provide recognition that product evolution is a key defense in protecting against evolving threats. In particular the Common Criteria has a built in flexibility through the specification of each product's security functionality in a security target that is individually specified for each "product" evaluation. On the other hand, the Common Criteria and especially the Common Evaluation Methodology define an assurance assessment process that initially has been developed without much interaction with vendors and users and has not been significantly changed despite of the criticism expressed for many years.

Comparability in the assurance of product types comes through the use of protection profiles. With proper management of the overseeing evaluation scheme inhibition of innovation should not be an issue. With poor management, lack of support for protection profiles, inappropriate security targets, and lack of focus on the true goals of assurance innovation is stifled.

The NIAP's CCEVS scheme is currently providing service **only** to those vendors who provide low-assurance products to US defense related customers. This effectively means that commercial product vendors who do not have a defense related customer, or who have products with high assurance requirements cannot enter the US scheme. Without the requirement to formally demonstrate assurance leads to commercial pressures to do nothing. This is a very bad situation for the rest of the US infrastructure.

Further demonstration of security assurance related innovation is observed in the improvement of development processes of vendors who have a mature security assurance strategy by ensuring that the product security architecture is considered and assessed at early stages of development and that assurance activities occur alongside development. This leads to early identification of vulnerabilities, leading to cost savings in their early resolution, and process improvements such as certification strategies that reduce the time to market of the security assurance associated with a particular product line but also reduction in the costs of assurance and the effort involved.

Failure of NIAP to promote evaluation and assurance processes and in standards evolution is detrimental.

A key point in allowing for innovation and evolution is the inclusion in the scheme of an effective certificate maintenance strategy allowing for the continued product

If so, what would be the best way to improve the current U.S. product assurance scheme?

Keep conformance paradigms to small well-defined components of products.

Ensure that all the U.S. product assurance schemes are improved to

- Be adequately funded and resourced to meet the needs of the U.S. cyber security posture
- Be resourced to allow timely validations and certifications
- Be proactive in improving the programs, and the related standards
- Provide trained and educated staff in a variety of product types
- Considers the goal of the U.S. security posture (i.e. the whole critical infrastructure as well as commercial concerns) as a key objective instead of just attempting to satisfy a few defense agencies

- Consider commercial aspects of U.S. industry wishing to export their products & services to other nations
- Is funded and educated to encourage information security, scheme and process innovation.
- Evolve with technology and the threats to technology and the infrastructure.

In particular regard to the Common Criteria evaluation paradigm - product assurance scheme

- Allow for appropriate higher assurance especially for core infrastructure components such as smartcards, network devices, operating systems, and core software such as databases
- Improves the knowledge and skill of validators to include all key technology types
- Encourage industry groups to develop suitable protection profiles at assurance levels that are appropriate for the type of product
- Have effective and meaningful dialogue as well as actively listen to all their stakeholders
- Cooperate with industry to identify and promote methods that allow for building products with higher and verifiable assurance
- Improves the scheme processes within the CCRA specifically
    - Support and promote **predictive assurance** in which the vendor's development and update process is assessed in order to predict ongoing assurance
    - Support and promote **evidence based evaluation**, in which the evidence "naturally" produced by a developer is assessed and that does not require the creation of evidence purely to support the evaluation process.
    - Offer an effective **certificate maintenance** strategy allowing for product evolution to be efficiently assessed for continued assurance
    - Support and promote an **attack based analysis** in which evaluators develop a hypothesis based on the strengths and weaknesses of the product, its development environment and design gained by them throughout the evaluation. The hypothesis can then be tested.
    - Provide the end user with a much more detailed and useful report about the assurance they gain than just a pass/fail result.

What, if any, changes need to be made with respect to international product assurance institutions, standards, and processes (e.g., the Common Criteria Recognition Arrangement)?

The Common Criteria Development Board (CCDB) was initially convened as a means to harmonize the various national government criteria into a single set of agreed criteria. The main drivers for this initiative was to address vendor concerns about the time and costs associated with certification under several national product assurance schemes, the time involved, and the varying criteria. Other problems with certifying under various schemes included the need to divulge source code and other sensitive assets to a variety of nations because there was no mutual recognition. Initially intended as an ISO standard the CCDB's initial mandate was to produce harmonized standards that could be published under the ISO "fast-track" process thus enabling their adoption by the nations on the timeliest basis. Hence a harmonized standard of Common Criteria (ISO/IEC 15408) was achieved and the CCRA was put in place to ensure comparable, repeatable evaluations as well as provide

mutual recognition for the certificates issued up to the commonly accepted assurance level for commercial products at that time, EAL 4.

Since then the CCDB has maintained control of the standards. The group operates on a closed basis, with only government agencies from the CCRA signatory nations represented. The group has notoriously failed to provide timely or public feedback to stakeholders other than the government agencies (i.e. the schemes) and have paid little attention to comments from other stakeholders who are not represented such as vendors, experienced evaluation facilities, end users and even the relevant ISO committee. This has resulted in the failure of several initiatives to evolve the standards with notable failures including the CC version 3, alternative assurance processes like the CDA and with the purported CC V4 now well over two years overdue and with little progress to demonstrate to stakeholders today.

Accordingly we support substantial change to the CCDB organization allowing for effective dialogue with all stakeholders, not just the government agencies that are signatories. A more open process would allow for effective change to occur. An international strategy of returning control of the development of the standards to ISO or a group with substantial industry involvement should also be considered.

The Common Criteria recognition arrangement (CCRA) is a useful vehicle for allowing commercial exchange of assurance at levels appropriate for commercial grade products. It is demonstrably successful with 997 certificates issued in the last 4 years with 507 at EAL4 or EAL4+. We refer to a recent paper “From Chaos to Collective Defense” [i] published in IEEE Computer magazine, [1]which illustrates some key points such as the dual purpose nature of much ICT and the need for collective defense.

The CCRA should be supported by the U.S. and consideration given to allowing a higher assurance level to be mutually recognized. For example much good would be achieved if the NIAP was able to make a positive statement confirming their continued endorsement of the CCRA and by working to ensure that this knowledge is passed effectively to U.S. Government procurement personnel. The current agreement allows recognition at EAL 4 (including flaw remediation) and was set over a decade ago. Allowing recognition of products to EAL5 would send a clear message to producers of commercial product developers that the assurance bar is being raised in line with increasing threats in Cyberspace and also promote innovation and re-architecture through competitive mechanisms. As pointed out earlier, the trust required for mutual recognition needs to be based on the supervision and control of the individual schemes by all the others. Currently this control is just based on periodic “shadowing” involving just a single evaluation; a process that is clearly not sufficient to establish the mutual trust required for accepting certifications at an EAL4 level, not to mention higher levels. Therefore we suggest reworking the CCRA to a more staged approach, defining an “entry level” with mutual recognition up to EAL2, a “medium level” up to EAL4 and potentially a “high level” up to EAL5. Each level needs to come with additional obligations for mutual supervision and the expertise that needs to be demonstrated by the schemes and labs. Nations that do not accept the additional obligations coming with higher levels may decide to stick with a lower level for mutual recognition. Strengthening the mutual supervision while also protecting the intellectual property of vendors that undergo an evaluation, is a challenge that needs to be addressed in a revised CCRA.

Some national schemes have been so underfunded that they are moribund and several are new and do not have advanced experience in evaluation, others are stressed by the volume of evaluation projects including those from other countries whose national schemes are restrictive to commercial products.

Sadly, the U.S. scheme has implemented restrictive policies that are failing to meet the requirements of the CCRA to which they are signatories. We support that the U.S. should promote for commercial recognition and actively promote the objectives of the CCRA abroad i.e.

- Support the CCRA and meet the U.S. obligations to it
- Ensure that evaluations of IT products and protection profiles are performed to high and consistent standards and are seen to contribute significantly to confidence in the security of those products and profiles;
- Improve the availability of evaluated, security-enhanced IT products and protection profiles;
- Eliminate the burden of duplicating evaluations of IT products and protection profiles, through being pro-active and co-operative with other national schemes in regard to the development and acceptance of protection profiles. This benefits all of the schemes involved and makes more efficient use of the product assurance resource pool available on an international basis;
- Continuously improve the efficiency and cost-effectiveness of the evaluation and certification/validation process for IT products and protection profiles in cooperation with vendors, labs and users.
- Consider changing the CCRA allowing for different trust levels.
- Offer an effective certificate maintenance strategy allowing for product evolution to be efficiently assessed for continued assurance, taking the developer's assurance activities into account.

Without this strategy the U.S. CCEVS scheme will continue to fail on home-ground in support of U.S. industry to

- Support the needs of securing cyberspace abroad (which also affects cybersecurity in the U.S.)
- Meet the commercial development needs of US industry abroad and operate on the same level as competitors from other nations.
- Demonstrate leadership and innovation to the rest of the world through operating a proactive, successful, and effective scheme demonstrating the U.S.'s leadership in this area. Instead we see other nations currently outside the CCRA forging ahead with developments in this area.

Should the Common Criteria Recognition Arrangement, the basis for international mutual recognition of cybersecurity product assurance, be expanded to include some of those countries which increasingly stray from international norms?

This question is not entirely within the control of the U.S. as CCRA membership is subject to the unanimous consent of the existing participating nations. We assume that the answer to this question will guide the U.S. position on admitting other nations to the CCRA.

Currently the U.S. product assurance scheme (CCEVS) policy is straying from the international norms by not complying with the agreements whole heartedly, as described above. In particular through very restrictive entry policies, failure to properly maintain and validate protection profiles, imposition of restrictions on evaluation assurance levels and so undermining the spirit of the agreement, which in turn encourages some key nations to be dubious about merits of joining the CCRA. If the goals of the CCRA are to be met effectively then the U.S. should participate according to its promise and ideally lead the other nations in also maintaining the agreement.

The CCEVS should support participation from any nation who is willing to provide assurance that they will meet the CCRA objectives; they should actively participate in shadowing schemes and other mechanisms to ensure adequate performance and maintain quality standards promised under the CCRA. Ideally the U.S. should contribute in effectively evolving the arrangement and the standards (as pointed out above) to meet the needs for security assurance, in the fast evolving technology and cyberspace on a global scale.

Failure to do this will mean that other schemes will develop and effectively undermine the initial reasons for the CCRA in supporting vendors with products that have a global impact. (Smartcards, operating systems, virtualization software, databases, network devices etc.)

It is known that nations like China and Russia use the Common Criteria standard within their national schemes without currently being a signatory of the CCRA. This policy allows them to use their national schemes as a barrier for foreign vendors to enter their IT markets unless those vendors undergo a separate evaluation of their products under their national schemes. Undergoing an evaluation is not only a factor of time and cost, but also requires vendors to disclose some of their IP implemented in the product to those schemes and the (usually government controlled) laboratories that perform the evaluation. This clearly is a disadvantage for U.S. vendors that want to do business in those countries. Having those national schemes being part of the CCRA would resolve those issues, but would of course also imply that evaluations performed in those countries being accepted by all other signatories of the CCRA. With proper supervision in place this seems to be the better solution, keeping in mind that the acceptance of evaluations does not apply when national security issues are involved. For a summary of the application of the Common Criteria, see the presentation given by the Chinese certification body in 2008 [4].

Study of developing assurance schemes in nations currently outside the CCRA is garnering some interest. For example in “The Common Criteria for Information Technology Security Evaluation Implications for China’s Policy on Information Security Standards” [2] the authors contrast China’s Multi Level Protection Scheme with the Common Criteria schemes. It cites some influential developers who underlines that having to meet sometimes substantially varying requirements of different national schemes requires significant resources from vendors. This paper also points out that increased government involvement and control brings potentially two negative consequences

- Suppression of the collaborative role of domestic vendors in the Infosec evaluation process
- Disruption of global innovation networks, making it more difficult to collaborate with foreign companies and therefore hurting the ability to recognize the value of new information, assimilate it, and apply it to commercial ends

These points considered in context with the need for collective defense discussed in “From Chaos to Collective Defense” [1] would indicate that some direct benefits to the global cybersecurity problem may be drawn from encouraging entry to internationally co-operative schemes such as the CCRA by nations that have not yet done so.

Items often discussed in earlier years, such as the need to allow access to source code to nations that may not otherwise have an opportunity to review such assets can be addressed, since through mutual recognition of certificates the need to share detailed evaluation evidence outside the scheme in which the evaluation occurs is reduced. It is outside terms of the CCRA that the need to expose source code and other high-value assets to foreign schemes becomes apparent.

Can useful U.S. Government or international product assurance guidelines be crafted for the current real-world software development environment?

The relationship between product assurance standards and the software development environment is one of mutual dependence. Reasonable assurance of the integrity of product security functionality cannot be made without consideration of the development methods used and the environment in which they are developed. I.e. it is necessary for product assurance standards to assess/evaluate the software development methods and the development environment according to established criteria.

There are already several standards and guidelines covering the topic of the development environment and processes including several well-know international standards.

It would be appropriate to support U.S. product assurance expertise to software development and environment standards so that these are continuing to be supportive of product assurance process and recognize that current real-world software development environments can vary immensely.

The protection of source code assets and design details has important commercial and national security considerations. Consideration of not just standards, but also measured assurance based on the evaluation of development processes and environments should be seriously considered as a matter of importance and allow for evaluations where the protection of critical assets of a developer can be upheld.

To what extent can a security oriented software assurance ‘‘tool’’ be useful in software validation?

As general as the question is stated, the correct answer is probably “forty two.” [3]

Tools can play an important role in development to ensure that security and assurance principles are followed. Tools can also play an important role in analyzing existing products for potential security problems. On the other hand, all tools will have their specific area of applicability and their limitations. Without proper knowledge of those the use of a tool may be harmful, providing a false level of assurance.

For the assurance assessment, tools can be very useful for the assessors allowing them to collect evidence, build evidence chains, and produce checklists to be included in reports. As with tools used by the developer, they can also be easily misused, produce misleading and poor results, and even downright dangerous if they are not wielded by experienced professionals.

Tools often are specific for the type of product developed, the development methodology, or the implementation language used. Tools can be very helpful to validate compliance with functionality defined in a specific standard. When it comes to detecting critical vulnerabilities, tools can be helpful to analyze the code or the behavior of a product for specific aspects. This can provide significant help to an experienced assessor to check for

some kinds of vulnerabilities. In the hand of an inexperienced assessor those tools will in most cases not be useful.

Examples are tools that analyze the control flow in software allowing an assessor to follow the flow and check where functions are called and variables are used. While those tools help an assessor tremendously when looking for vulnerabilities like incomplete parameter validation or race conditions, nobody should hope that tools will find those types of vulnerabilities automatically. They will help to identify the areas the assessor needs to focus on, thereby significantly reducing the time and cost of the assessment. Using similar tools during the development process to avoid such problems will even further reduce the effort for the assessment. As stated before: Preparing for the assurance assessment during the development and integrating the assessment into the development process are the key factors for reducing the time and cost of the assessment and maximizing the assurance gained. Using the right combination of tools for both development and assessment can help tremendously in the overall process.

Development and use of such tools should therefore be promoted, although there will never be a single family of tools applicable for all product types, development procedures or implementation languages.

What elements would be necessary to develop an effective industry-government dialogue to clarify the product assurance goals and challenges, and identify workable solutions?

A common forum for all U.S. government product assurance schemes including the several U.S. Government product assurance schemes using several standards and operating from various agencies. These include (but are not limited to)

- NSA's NIAP for Common Criteria (The Common Criteria Evaluation and Validation Scheme – CCEVS);
- NIST's Cryptographic Module and Validation Program (CMVP), Cryptographic Module validation Program (CAVP), the NIST Personnel Identity Verification Program (NPIVP) and the program for assurance of the Security Content Automation Program as well as involvement with voting systems and several others;
- The General Service Administration (GSA)'s FIPS 201 Evaluation Program;
- FBI Fingerprint testing
- Voting Machines
- Health Industry IT
- Postal Systems
- And others

The goal of the forum should be to

1. Establish an effective dialogue with all stakeholders (Across all U.S. product assurance programs)
    a. Those able to set a national strategy and provide appropriate resourcing
    b. Vendors
    c. Schemes/Programs (NIST, NSA, GSA)

   d. Laboratories
   e. Consumers
   f. Standards developers

2. Consider a ***unified strategy*** for U.S. product and systems assurance.
3. Act on agreed results

NOTE: No input is provided from atsec on the following topics in the NOI:

- Raising Awareness
- Web Site and Component Security
- Authentication/Identity(ID) Management
- Research & Development
- An Incentive Framework for Evolving Cyber-Risk Options and Cybersecurity Best Practices

References

[1] James Bret Michael, Eneken Tikk, Peter Wahlgren, Thomas C. Wingfield, "From Chaos to Collective Defense," Computer, pp. 91-94, August, 2010

[2] Dieter Ernst, Sheri Martin "The Common Criteria for Information Technology Security Evaluation _ Implications for China's Policy on Information Security Standards" East West Center Working papers, Economics Series No. 108, January 2010. Avaliable from http://www.eastwestcenter.org/fileadmin/stored/pdfs/econwp108.pdf. Accessed 2010-08-27

[3] Douglas Adams "The Hitch Hiker's Guide to the Galaxy", 1978-2005 Multi Media: Paperback Pan Books ISBN 0-330-25864-8

[4] Zhuohui Liu, Xiaohua Chen "CC in China" Common Criteria Portal, Sept 23, 2008. Available from http://www.commoncriteriaportal.org/iccc/9iccc/pdf/A2311.pdf Accessed 2010-08-31

[5] IEEE-2600-2008 MFP Security Standard, June 30, 2008, Available from http://ieeexplore.ieee.org/servlet/opac?punumber=4556650 (Available to subscribers and IEEE members)

[6] U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices in Basic Robustness Environments (IEEE Std. 2600.1-2009) Version 1.0 available from http://www.niap-ccevs.org/pp/pp_hcd_br_v1.0/ Accessed 2010-09-01