September 13, 2010

TO: Diane Honeycutt, Department of Commerce

FROM: Randy Vanderhoof, Executive Director, Smart Card Alliance

SUBJECT: Smart Card Alliance Response to Department of Commerce Notice of Inquiry, "CyberSecurity, Innovation and the Internet Economy" (Docket No.: 100721305-0305-01)

The Smart Card Alliance Identity Council reviewed the Department of Commerce (DOC) Notice of Inquiry (NOI) titled "CyberSecurity, Innovation and the Internet Economy," published in the Federal Register, Vol, 75, No. 144, Wed., July 28, 2010, (Docket No.: 100721305-0305-01).

We offer the attached responses to several of the questions posed in Section 4, Authentication/Identity (ID) Management, and Section 6, Product Assurance of the NOI.

The Smart Card Alliance Identity Council appreciates the opportunity to provide input to the Department of Commerce on cybersecurity. We would be happy to work with the Department of Commerce on further defining and specifying the framework, policies, best practices and technologies for identity management and authentication in cyberspace.

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.

If you have questions on these responses, please contact our Identity Council Chair, Neville Pattinson, Gemalto (neville.pattinson@gemalto.com) or me (rvanderhoof@smartcardalliance.org, 1-800-556-6828).

Sincerely,

Randy Vanderhoof

Executive Director

Smart Card Alliance

Smart Card Alliance Response to Department of Commerce Notice of Inquiry, "CyberSecurity, Innovation and the Internet Economy" (Docket No.: 100721305-0305-01)

The Smart Card Alliance Identity Council reviewed the Department of Commerce (DOC) Notice of Inquiry (NOI) titled "CyberSecurity, Innovation and the Internet Economy," published in the Federal Register, Vol, 75, No. 144, Wed., July 28, 2010, (Docket No.: 100721305-0305-01).

We offer the responses below to several of the questions posed in Section 4, Authentication/Identity (ID) Management, and Section 6, Product Assurance of the NOI.

Responses

Section 4. Authentication/Identity (ID) Management.

Comment on the effectiveness of current identity management systems in addressing cybersecurity risks.

a. Beyond the measures recommended in the National Strategy for Trusted Identities in Cyberspace, what, if any, federal government support is needed to improve authentication/identity management, controls, mechanisms, and supporting infrastructures?

Response: The federal government, through NIST, must establish the levels of functionality that are necessary or even required to protect the cyber infrastructure and personal privacy. These functionality levels will enable many different sectors to understand clearly and concisely what is need to equally protect networks and personal information. The OMB M-04-04 document, "E-Authentication Guidance for Federal Agencies," describes four levels of assurance. We recommend that NIST review these levels and determine if there is a better model for addressing all of the assurance levels required in authentication and identity management.

b. Do the authentication and/or identity management controls employed by commercial organizations or business sectors, in general, provide adequate assurance? If not, what improvements are needed?

Response: Many different implementations are in use today for authentication and identity management. There is no consistent implementation apart from the Federal Bridge certification. In general, commercial organizations are moving towards identity badges that combine physical access and logical access for employees. The logical access portion includes PKI technology for secure authentication, VPN use, email digital signatures and encryption. Each commercial entity either roots to their own root CA or to a commercial root CA.

c. What specific controls and mechanisms should be implemented?

Response: A clear national definition for the various levels of authentication is required, including standards for identity proofing and use of authentication technologies. This is necessary to establish a framework for interoperability in cyberspace for trusted transactions and communications. It is imperative to know to which authentication level the communicating parties are interacting and to provide a level of trust assurance.

d. What role should authentication and identity management controls play in a comprehensive set of cybersecurity measures available to commercial organizations?

Response: See answer to (c) above.

e. Are the basic infrastructures that underlie the recommended controls and mechanisms already in place?

Response: Infrastructure is available and being used around the world for various applications. For example, the payment card industry and different national healthcare programs have adopted standards-based authentication technologies to enable interoperability.

Currently within the Federal government, standards established to protect the federal infrastructure could also be used or adapted to consumer-based programs, offering the same level of security, privacy and trust. The Federal Information Processing Standard (FIPS) 201, Personal Identity Verification (PIV) of Federal Employees and Contractors, provides a framework of policy, process and technology that establishes a strong and comprehensive program. This is already being leveraged by state and local governments and other organizations for PIV-interoperable credentialing programs.

f. What, if any, new tools or technologies for authentication or identity management are available or are being developed that may address these needs?

Response: Smart cards are a proven, cost-effective, secure and trusted mechanism for identity authentication for online use. FIPS 201 has defined the comprehensive Federal implementation using this technology. We recommend that smart cards, in conjunction with personal identification numbers (PINs) or match-on-card biometrics, be recognized for the highest levels of assurance in trusted communications and transactions.

For lesser authentication levels, out-of-band authentication methods, such as one-time-passwords delivered by a second channel (such as an SMS to a previously registered and authenticated cell phone), can deliver a level of assurance appropriate to less secure transactions or communications.

g. How can the expense associated with improved authentication/identity management controls and mechanisms be justified financially?

Response: First, the fraud numbers associated with online transactions appear to be increasing. Based on the U.K. experience with the transition to EMV credit and debit cards, there is evidence that fraud related to online transactions that have no way of being authenticated is steadily increasing.

Moving to smart card-based technologies for improved authentication can deliver a number of benefits and savings to organizations and individuals, including:

- Decreased fraud
- Protection from identity theft
- Simplified user password management (with lower support costs and increased user convenience)
- Reduced cost by combining multiple functions on a single smart credential or by using a single smart credential to access multiple services
- Better ability to comply with legislative and regulatory mandates (e.g., Sarbanes-Oxley, HIPAA, PCI DSS)
- Improved user productivity and reduced operating costs (for example, through easier access to networked resources and improvements to business processes (e.g., document signing))
- Reduced risk of security breaches and their resulting costs

h. How can the U.S. Government best support improvement of authentication/identity management controls, mechanisms, and supporting infrastructures?

Response: We recommend that the U.S. government form a public/private (industry/government) working group to drive adoption by publishing and using of standards. It is also critical for the U.S. government to promote the use of identity management and authentication technologies in any communication and transaction within and with the U.S. government.

i. **Is there a continuing need for limited revelation identity systems, or even anonymous identity processes and credentials?**

Response: There are many transactions and communications performed over the Internet. According to the perceived risk of an interaction and the need for identification or not, there should be mechanisms to allow for the full spectrum of identity authentication -- from anonymity to full disclosure of identity. Third parties could be employed as identity providers or credential authenticators to provide assurance levels against various personas employed by individuals.

j. **If so, what would be the potential benefits of wide-scale adoption of limited revelation identity systems or anonymous credentialing from a cybersecurity perspective**?

Response: People should have control of their privacy and identity. Accordingly it is important to allow for individuals to use various personas with varying levels of assurance according to the need of an interaction. Once a framework is established for the use of personas for different levels of authentication and identification, interactions can be defined to require a particular level of assurance.

k. **What would be the drawbacks?**

Response: There will be potential difficulties in establishing the true identity of an individual when lower levels of assurance are used for personas. If there is a criminal or terrorist issue arising, appropriate laws and controls should be established to allow for the disclosure of the root identity to authorities.

l. **How might government procurement activities best promote development of a market for more effective authentication tools for use by government agencies and commercial entities?**

Response: Procurements should incorporate authentication and identity management requirements against established levels of use to encourage the adoption of better practices and standards.

m. **Could a private marketplace for "identity brokers" (i.e., organizations that can be trusted to establish identity databases and issue identity credentials adequate for authorizing financial transactions and accessing private sector components of critical infrastructures) fulfill this need effectively?**

Response: Yes. Identity brokers or providers are an important part of an identity infrastructure. Individuals will need to establish persona identities according to their wishes. Third parties will need to assess the risks of providing this service and understand any liabilities that may be part of providing this service. In the event of criminal or terrorist issues, normal laws should be used to prosecute the parties/individuals concerned, not the identity brokers.

n. **What would be some of the issues or potential impacts of establishing standards and best practices for private sector identity brokers?**

Response: There is a strong need for solid consistency of implementation against standards for the operations of identity brokers. Regular audit and certification to these standards are necessary for identity brokers to operate and provide consistency. Any identity broker persona must be clearly identified as to what level of assurance it is applicable.

o. **Should the government establish a program to support the development of technical standards, metrology, test beds, and conformance criteria to take into account user concerns such as how to: (1) improve interoperability; (2) strengthen authentication methods; (3) improve privacy protection through authentication and security protocols; and (4) improve the usability of identity management systems?**

Response: Absolutely. There is some interest in the private sector to use authentication tools to protect IP and networks. However, that view will not become a standard practice until clear standards are established and accepted. Concerns about the healthcare environment and the transition to electronic health records fall into this category.

p. What are the privacy issues raised by identity management systems and how should those issues be addressed?

Response: The following elements are critical to addressing privacy:

- Ensure individuals are in control of their identities and personas.
- Allow individuals to have multiple personas according to role, risk and assurance level.
- Ideally, root all personas to a trusted authenticated identity and use technology, such as smart cards, to authenticate their usage.
- Only provide the necessary personal identification information necessary for the interaction being undertaken.
- Allow for redress scenarios where an individual can prove either non-repudiation of use or compromise of credential use.

q. Are there particular privacy and civil liberties questions raised by government involvement in identity management system design and/or operations?

Response: Yes. Care must be taken to assure that individuals cannot be tracked across government systems when using their personas. Individual, system-specific identifiers should be used to identify each user and these should differ across each system being utilized. Identity theft is an increasing issue that is undermining trust and confidence in cyberspace. It is recommended that individuals be given the choice to adopt appropriate authentication technology to protect their identity from being stolen. Any use of an identity should only be accepted once the user has presented and authenticated their identity according to their personally determined level of presentation. As a consequence of this requirement, a registry of identities and authentication pre-requisites should be maintained, either centrally or in a federated environment/cloud to allow relying parties to ensure the correct authentication level required for a specific identity.

6. Product Assurance

The following responses were developed by Smart Card Alliance member, atsec, and are included with the Smart Card Alliance response.

a. Do current U.S. Government product assurance requirements inhibit production of timely security IT products and systems?

Response: 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 accredited 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 and also developed Common Criteria Protection Profiles based on this standard. 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 (e.g., 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 stakeholders 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 was canvassed for input. However atsec was 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 U.S.

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 U.S. 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 U.S. product assurance scheme around the globe as the U.S. seeks to take advantage of the CCRA recognition without contributing effectively.

Currently NIAP fails 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 Evaluation Program

The service run by the GSA for establishing conformance to the FIPS 201 standards is operated in a bureaucratic 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 accredited 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.

b. Do current assurance processes inhibit innovation?

Response: 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 U.S. 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 U.S. 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 U.S. 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.

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

Response: 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. cybersecurity 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 and 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 with regard to the Common Criteria evaluation paradigm - product assurance scheme:

- Allow for appropriate higher assurance especially for core infrastructure components such as smart cards, network devices, operating systems, and core software such as databases

- Improve 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
- Improve 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.

d. 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)?

Response: 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 has 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 atsec supports 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”published in IEEE Computer magazine, 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 EAL4 (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, atsec suggests 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. Atsec supports that the U.S. should promote 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.

e. 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?

Response: 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 wholeheartedly, as described above. In particular through very restrictive entry policies, failure to properly maintain and validate protection profiles, and imposition of restrictions on evaluation assurance levels, this undermines 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 (e.g., smart cards, operating systems, virtualization software, databases, network devices).

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.

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”the authors contrast China’s Multi Level Protection Scheme with the Common Criteria schemes. It cites some influential developers who underline 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” 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.

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

Response: 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 -- 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-known 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.

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

Response: 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.

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

Response: 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

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

About the Smart Card Alliance Identity Council

The Smart Card Alliance Identity Council is focused on promoting the need for technologies and usage solutions regarding human identity information to address the challenges of securing identity information and reducing identity fraud and to help organizations realize the benefits that secure identity information delivers. The Council engages a broad set of participants and takes an industry perspective, bringing careful thought, joint planning, and multiple organization resources to bear on addressing the challenges of securing identity information for proper use.