atsec information security
Suite 260
9130 Jollyville Road,
Austin, Texas 78759

Mr. Alfred Lee

National Institute of Standards and Technology

100 Bureau Drive, Stop 8930

Gaithersburg, MD 20899

29th April, 2013

RE: Incentives To Adopt Improved Cybersecurity Practices

Dear Mr Lee,

atsec is pleased to be able to submit comments in response to the request and thanks NIST for the opportunity to do so.

The text below is a comment from atsec on the topic of incentives to adopt improved cybersecurity practices as solicited in the NIST RFI published in the Federal Register on March 23rd, 2013.

Are there disincentives or barriers that inhibit cybersecurity investments by firms?

and

For American businesses that are already subject to cybersecurity requirements, what is the cost of compliance and is it burdensome relative to other costs of doing business?

atsec is an accredited laboratory performing evaluations under the NIAP CCEVS Common Criteria scheme and also conformance testing for several of the NIST led testing programs for information security in regard to Commercial Off the Shelf Products. atsec has been involved with information assurance services in the US and abroad since 2000 and is regarded as an expert in this topic.

While the US government has:

- Mandated the use of Common Criteria as a procurement criterion for DoD, through DOD 8500.1 and 8500.2
- Expressed preference in acquisition of evaluated and validated products according to Common Criteria in CNSS NSTISSP No. 11.
- Recommends the use of ISO/IEC 15408 (The ISO published equivalent to Common Criteria) in NIST SP 800-53 (Rev 4)

The NIAP's current policy is that the NIAP will only accept products for evaluation claiming exact compliance with one or more published "NIAP approved PPs". Further, the NIAP policy is that the CCEVS will not accept evaluations that do not have valid U.S. Government customers as outlined in CCEVS Policy #12.

This situation forces US developers and vendors that do not target US Government customers to seek evaluation from a scheme outside the US relying on the Common Criteria Recognition Arrangement (CCRA) for acceptance in the US. However This strategy is becoming increasingly difficult since NIAP must be involved with evaluations to NIAP approved PPs performed outside the US, and because NIAP policies are specified so that acceptance under the CCRA is no longer possible.

The result of these NIAP policies is that suppliers of ICT products to those parts of the critical infrastructure, or in the US general infrastructure and that would desire to follow the US government policies and recommendations for evaluation are effectively precluded from doing so.

Further, NIAPs current policy of demanding low-assurance evaluations, through the specification of low-assurance PP's effective for the US does not meet the needs of developers of mature technologies that have already established high-assurance, these technologies are often critical to the assurance case for a larger system and include operating systems, virtualization, smart-cards and real-time embedded systems. All of which are key technologies in protecting the US critical infrastructure.

COTS developers are subject to assurance demands from around the world, not just the US. The current US policies add costs and time-delays to developers and it is unlikely that other nations will accept ICT products with only US specified low-assurance as suitable for their own needs.

atsec notes that the National Information Assurance Partnership (NIAP) makes the following claims:

The National Institute of Standards and Technology (NIST) and the National Security Agency (NSA) have established a program under the National Information Assurance Partnership (NIAP) to evaluate IT product conformance to international standards. The program, officially known as the NIAP Common Criteria Evaluation and Validation Scheme for IT Security (CCEVS) is a partnership between the public and private sectors. This program is being implemented to help consumers select commercial off-the-shelf information technology (IT) products that meet their security requirements and to help manufacturers of those products gain acceptance in the global marketplace.

1 Project Objectives

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

2 Goal of the Partnership

The long-term goal of NIAP is to help increase the level of trust consumers have in their information systems and networks through the use of cost-effective security testing, evaluation, and validation programs. In meeting this goal, NIAP seeks to:

- *Promote the development and use of evaluated IT products and systems;*
- *Champion the development and use of national and international standards for IT security;*
- *Foster research and development in IT security requirements definition, test methods,*

tools, techniques, and assurance metrics;

- *Support a framework for international recognition and acceptance of IT security testing and evaluation results; and*
- *Facilitate the development and growth of a commercial security testing industry within the U.S.*

atsec believes that the current situation represents a disincentive to US companies and developers that would otherwise invest in providing validated security assurance claims in regard to their COTS ICT products.

atsec recommends that the project for a Framework to improve critical infrastructure Cybersecurity consider this problem of providing effective evaluations in the US and recommend a solution for developers wishing to demonstrate through independent analysis the security assurance claims of their COTS products to critical infrastructure and commercial sector users.