September 20, 2010

Secure ID Coalition

Comments to the Department of Commerce: Office of the Secretary; National Institute of Standards and Technology; International Trade Administration and National Telecommunications and Information Administration
Re: Cybersecurity, Innovation and the Internet Economy
Notice of Inquiry
Docket No.: 100721305–0305–01

Introduction

The Secure ID Coalition is pleased to offer the following comments to the Department of Commerce and the agency's offices with regard to cybersecurity, innovation and the Internet economy. Cybersecurity is critical to not only our national security and defense but also to our digital economic infrastructure owned and managed mostly by the private sector.

As the focus of the Secure ID Coalition has primarily been in the area of identity management, our efforts recently have been on the need for the development of strategic outlines like the National Strategy for Trusted Identities in Cyberspace (NSTIC). The Department of Commerce must be engaged in the cybersecurity effort to help create an e-commerce environment that is safe for all consumers, as well as offer businesses surety. Further, the efforts of the National Institute of Standards and Technology (NIST) to assist with the development of a standards based approach to identity management are essential for the success of cyber security and safety through identity management.

The focus of Secure ID Coalition response to the Notice of Inquiry (NOI) is on the area outlined in Section Four of the document: Authentication / Identity (ID) Management.

Federal Support

Beyond the measures recommended in the National Strategy for Trusted Identities in Cyberspace, the federal government, through NIST, must establish levels of functionality that are necessary, or even required, to protect cyber infrastructure and personal privacy. These functionality levels will enable many different sectors to understand clearly and concisely what is needed to equally protect networks and personal information. The Office of Management and Budget Memorandum 04-04 describes four levels of assurance. The Secure ID Coalition recommends NIST review these levels and determine if there is a better model for addressing all the assurance levels required in authentication and identity management.

Today many different implementations of identity management tools are in use for authentication and identity management, but the most consistent implementation in the federal government is the Federal Bridge certification. In general, commercial organizations are moving toward physical access combined with and logical access identity badges for employees. The logical portion includes PKI technology for secure authentication, VPN use, email digital signatures and encryption. Each commercial entity either roots to its own root Certificate Authority (CA) or to a commercial root CA.

Secure ID Coalition
919 18th Street, NW #925 | Washington, DC 20006 | www.secureidcoalition.org

The Secure ID Coalition respectfully suggests that the Department of Commerce consider outlining clear national definitions for various levels of authentication, including standards for identity proofing and use of authentication technologies. These definitions are necessary to establish a framework for interoperability in cyberspace for trusted transactions and communications. It is imperative to know with which level the communicating parties are interacting and to provide a level of trust assurance.

Leveraging Existing Infrastructure

Infrastructure around the world is already widely deployed for various identity management applications. Currently, within the federal government, standards established to protect federal infrastructure could also be used or adapted to consumer based programs, offering the same level of security, privacy and trust. Further standards could include an online identity authentication function to enable secure Internet transactions.

As part of this existing infrastructure, Smart Card-based solutions offer answers to many cybersecurity questions. The technology is a proven, cost effective, secure and trusted mechanism for identity authentication for online use. As Federal Information Processing Standards 201 (FIPS 201) has defined the comprehensive federal implementation using this technology, it has many advantages as a trusted solution online. The Secure ID Coalition recommends that the federal government consider implementing standards defined by FIPS 201 for the highest levels of assurance in trusted communications, commerce, and transactions.

One-Time-Passwords delivered by a second channel (such as an SMS to a previously registered and authenticated cell phone) perform a level of assurance appropriate for lesser authentication transaction requirements.

Authentication / Identity (ID) Management Is Cost Effective

The fraud numbers associated with online transactions are increasing in both financial transactions and shared online health data. In the financial sector, it is clear that numbers attributed to fraud in online transactions are steadily increasing. Similarly, data breaches in the healthcare sector have resulted in both identity theft and the manipulation of healthcare records, causing not only significant cost to the original record holder but also serious harm if the record includes information not attributed to that patient. In both cases the expense of improved authentication is offset and justified by the aggregate savings to both the retail merchant or healthcare provider and the consumer or patient. Today the cost of fraud and the cost associated with cleaning up the aftermath are often ultimately born by the consumer, which makes it difficult to quantify by just the bank or healthcare provider.

The federal government can best support improvement of authentication/identity management controls, mechanisms, and supporting infrastructures by forming a public/private (Industry/Government) working group to drive the adoption by the publication and use of standards. The federal government can also promote the use of identity management and authentication technologies in any communication and transaction between the government, its contractors, and citizens.

Information Revelation

The question of revelation identity systems comes down to the needs of the end users and their privacy protection. 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 a full

spectrum of information revelation available to end users, from anonymity to full disclosure of identity. Third parties could be employed as identity brokers to provide assurance levels against various personas employed by individuals.

People should have control of their privacy and identity. Accordingly it is important to allow for various personas to be utilized by individuals 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.

However, there will be potential difficulties in establishing the true identity of an individual when lower levels of assurance are used for personas. As such, if a criminal or terrorist issue arises there should be appropriate laws and controls established to allow for the disclosure of the root identity to authorities.

Identity Practices & Brokers

The Secure ID Coalition respectfully recommends that government procurements activities should be required to adopt best authentication and identity management practices. In doing so, these practices will provide a foundation for commercial entities. As government is the largest procurer of goods and services, establishing a government baseline of trust will create a culture of the trusted identities and in turn, make the entire Internet more secure.

An "identity broker" private marketplace could develop if encouraged in the correct way. This option is an important part of an identity infrastructure. Individuals will need and want to project persona identities according to their personal preferences. 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 order for such a market place to exist, however, there must be a defined limited liability for those vendors. All laws must be closely adhered to and in the event of criminal or terrorist activity all bad actors must be held accountable and prosecuted.

Standards and best practices are critical to the success of an identity broker marketplace. There is a strong need for solid consistency of implementation of standards for the operations of identity brokers; someone vetted with one broker must meet the same assurance level as another individual vetted through another broker. Regular audit and certification to these standards is necessary for identity brokers to operate and provide consistency. Any identity broker issued persona must clearly identify what level of assurance that persona is meets and with what applications it can be used.

The Secure ID Coalition emphatically recommends that the government establish a program to support the development of technical standards, methodology, test beds and conformance criteria. While there is some interest in the private sector to use authentication tools to protect intellectual property and networks, it 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, as improving privacy protections through authentication can lead to secure interoperability and exchange of healthcare data.

<u>Privacy Protections</u>

The best way to address privacy concerns raised by identity management is to ensure that the individual is in control of their identity and personas. A privacy framework should be part of the design of any management system. Such a framework should include allowing individuals to have multiple personas

according to role, risk and assurance level; rooting all personas to a trusted authenticated identity and use technology, such as smart cards to authenticate their usage; providing only provide the personal identification information necessary for the interaction or transaction; and allowing for redress scenarios where an individual can prove either non-repudiation of use or compromise of credential use.

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

The Secure ID Coalition is pleased to offer input to the Department of Commerce on this important Notice of Inquiry addressing cybersecurity, innovation and the Internet economy. We stand ready to assist the Department as identity management questions arise through this process or the National Strategy for Trusted Identities in Cyberspace.

Respectfully Submitted,

Kelli A. Emerick
Executive Director
Secure ID Coalition

About the Secure ID Coalition

The Secure ID Coalition is an affiliation of companies providing digital security solutions for identification documents, including contactless smart cards. Our mission is to promote the understanding and appropriate use of smart card technology that achieves enhanced security for ID management systems while maintaining user privacy.

Coalition members support specific citizen privacy rights as follows:

- **Privacy** of personal information as defined by all relevant regulations and laws, principally the body of laws know as Fair Information Practices.

- **Confidence** that ID documents have been appropriately secured against threats of fraudulent access to personal information.

- **Knowledge** of what data is contained in electronic ID documents; how that data will be collected, secured and transmitted; the presence of radio frequency (RF) technology in ID documents; and when, where and why RF devices are being read.

For more information, please visit our website at www.secureidcoalition.org

Secure ID Coalition
919 18th Street, NW #925 | Washington, DC 20006 | www.secureidcoalition.org