Date: **July 22, 2011**

To: Office of the Secretary,
U.S. Department of Commerce and National Institute of Standards and Technology,
U.S. Department of Commerce.

Attn: Annie Sokol

From: Timothy M. Jurgensen

(e-mail) tjurgensen@austin.rr.com ; (office phone) 512-452-8090

Subject: Notice of Inquiry
Docket No. 110524296-1289-02

Disclaimer: These comments are based significantly on the personal opinions of the author. They infer no acceptance or support from any other person or organization. Factual errors should be reported to the author for correction.

In the referenced Notice of Inquiry, two sets of information are solicited:

> *The Department seeks to learn and understand approaches for: 1) the structure and functions of a persistent and sustainable private sector-led steering group and 2) the initial establishment of the steering group.*

In preparing comments in response to the requests for these two sets of information, it is necessary to first address the basic assumptions of the inquiry.

Identity is foundational to any social system, specifically including the Internet and the World Wide Web. This foundation forms the basis of trust necessary for interactions to be effectively pursued. Trust, a mathematical concept, is the probability of correctly anticipating the outcome of an interaction. Identity allows individuals to be distinguished (*differential-identity*) and for information to be attributed in a trustworthy fashion to each individual (*experiential-identity*). Within any interaction, identity allows rules to be applied, reputations to be assessed, ownership and responsibility to be assigned and ultimate consequences to be adjudicated. In this manner, the anticipated outcome of pending interactions can be assessed versus the actual, final outcomes. Hence, trust can be initially established and can evolve through the accumulation of experiences in the form of interaction consequences.

The Identity Ecosystem Framework is the central basis for a trusted interaction environment. All other capabilities within the environment are subordinate additions to the framework. In the assessment of trust, consequences must ensue if there is any abrogation of the mechanisms through which trust is established. Consequently, the Identity Ecosystem Framework must be grounded in law; certainly administrative law, tort law and most likely criminal law as well. This presents a challenge to some of the basic assumptions noted in the National Strategy for Trusted Identities in Cyberspace; specifically that all aspects of the framework are voluntary and that

they derive purely from non-governmental entities and actions. While participation in the infrastructure might be voluntary, all aspects of the infrastructure must be established and protected by a legal framework. This suggests that while the steering-group might be grounded in the "private-sector", the environment must derive from and be protected by government action.

The purpose of the Identity Ecosystem Framework is to establish a basis of trust for those who elect to authenticate their identities under its auspices; we might refer to this group as the *end-user community*. This is the primary focus of the framework. Consequently, the steering-group has a *fiduciary duty* to this group; individually and collectively. The term "fiduciary duty" is used under its more expansive definition which mandates that the steering-group and its members must act to benefit the interests of the end-user community above their own interests (i.e. those interests specific to the steering-group and its members). While the members of the steering-group may be drawn from the various communities of "stakeholders", it must be clear that the specific interests of the various stakeholder communities are subordinate to those of the end-user community as prescribed by appropriate law.

If this concept of fiduciary duty is appropriately applied, the resulting Identity Ecosystem Framework should present a level playing field for all members of the end-user community. Essentially all stakeholders will participate in the framework as members of this end-user community. Hence, emphasis on this community does not subordinate individual members of any specific stakeholder community; only the interests of those individual stakeholders which are in competition with the interests of the end-user community at large.

With this preface, we can now address the specific questions posed by the Notice of Inquiry.

1 - Structure of the Steering-group

1.1 *Given the Guiding Principles outlined in the Strategy, what should be the structure of the steering group? What structures can support the technical, policy, legal, and operational aspects of the Identity Ecosystem without stifling innovation?*

Comment: One might consider the answer to this using the "Goldilocks criteria" as applied to existing government structures. The administrative branch centered on one person, the President, is probably too few to provide a good model for the steering-group. The legislative branch with its 535 members of the House and Senate is probably too many. The judicial branch centered on the 9 members of the Supreme Court is perhaps "just right." It seems like a good match for the size of the steering-group suggested by its stated goals.

An odd number of members of the steering-group insures a finality of decisions, a characteristic often illustrated by the Supreme Court through its 5-4 decisions. Further, a 9-member body offers up the prospect of one member per each of the following stakeholder groups:

a. End-user community
b. Service providers [e.g. web browser, web servers, content providers]
c. Token providers [e.g. smart cards and other ID tokens and authentication mechanisms]
d. Identity brokers [e.g. providers of differential-identity registries and experiential-identity registries]
e. Connectivity providers [e.g. networking hardware and software along with middleware]
f. Platform providers [e.g. all forms of computer platforms]
g. Adjudication [law enforcement, legal counsel and judiciary]
h. Regulatory [standards, rule-making and certification]
i. Privacy [advocates, counselors and technical mechanism experts]

Obviously, a different collection of stakeholder groups could be recognized without unduly impacting the governability of the steering-group. But, it's probably a "given" that the correct size of the steering-group is closer to nine members than to ninety.

1.2 *Are there broad, multi-sector examples of governance structures that match the scale of the steering group? If so, what makes them successful or unsuccessful? What challenges do they face?*

Comment: As noted in the previous comment, we might consider the branches of government as examples of governance structures that span domains comparable to the space addressed by the steering-group. The success of any of the governance structures is grounded in a well defined policy for selection of the members of the specific structure. The policy should be equitable, repeatable and enduring. The existence of trusted processes for selection enhances the effective authority of the various structures and makes obvious the specific community of interest (polity) to which each

structure is relevant. Policy should also encompass feedback mechanisms that influence those "elected" to foster the interests of "those that elected them". One can argue that when the selection process is a well defined election mechanism, each election constitutes a decision on the part of the polity as to whether the governance structure has appropriately pursued its fiduciary duty to the polity. However, while this is not to say that selection must always be based on an election, it really should be based on a feedback mechanism that makes the selected participant answerable to the appropriate community.

1.3 *Are there functions of the steering group listed in this Notice that should not be part of the steering group's activities? Please explain why they are not essential components of Identity Ecosystem Governance.*

Comment: As indicated in various comments above, it seems that the central concern in this regard is the degree to which the steering-group's activities are ultimately grounded in law. The infrastructure can clearly not accomplish the goal of establishing trust in the interactions that occur in cyberspace without the ultimate arbitration and adjudication of a compelling legal framework. The need to develop the National Strategy for Trusted Identities in Cyberspace is a clear indication that the current connection between identification mechanisms and jurisprudence is lacking.

1.4 *Are there functions that the steering group must have that are not listed in this notice? How do your suggested governance structures allow for inclusion of these additional functions?*

Comment: While participation in the infrastructure may be voluntary, there must be legal ramifications for anyone that seeks to impact the infrastructure, particularly if they haven't "joined" it in the accepted fashion. Thus, it is clear that the steering-group must comprise a subordinate component in a larger social order that possesses some level of "police powers". This can only derive from government. Indeed, the liability constraints implicit to the steering-group may only be acceptable under the concept of sovereign immunity.

1.5 *To what extent does the steering group need to support different sectors differently?*

Comment: The infrastructure must enhance the trust on which the end-user community depends for its individual engagement of interactions. This requires that the policies put forward by the steering-group need to provide a level playing field among all the members of the end-user community. This essentially means that the personal privacy of individual participants must be arbitrated in order to achieve equality of opportunity. Achieving this environment for members of the end-user community may require subordination of the interests of the other stakeholder communities. Members of these various communities must then be free to determine whether, or to what extent, they participate in the infrastructure.

1.6 *How can the steering group effectively set its own policies for all Identity Ecosystem participants without risking conflict with rules set in regulated industries? To what extent can the government mitigate risks associated with this complexity?*

Comment: The policies advocated by the steering-group must ultimately be grounded in the same laws which underlie all regulated environments. Obviously, the current arbitration among the overlapping regulatory environments is complex. So, the steering-group probably does not add any additional complexity. Perhaps, by appropriately pursuing the concept of fiduciary duty to the end-user community, the steering-group can actually enhance the existing arbitration environment. This is obviously going to ultimately involve the "adjudication stakeholder group" suggested in an earlier comment.

1.7 *To what extent can each of the Guiding Principles of the Strategy–interoperability, security, privacy and ease of use—be supported without risking "pull through"[1] regulation from regulated participants in the Identity Ecosystem?*

Comment: THE guiding principle of the strategy must be "privacy". However, the concept of personal privacy of individual members of the end-user community is far more expansive than is suggested by the strategy. Privacy is a concept more concerned with "control" than with "secrecy". Secrecy can derive from privacy, but a lack of (or loss of) secrecy does not abrogate privacy. Indeed, privacy mandates always apply to the ongoing ownership of the consequences of an interaction by all the participants to that interaction. The interaction environment provided by the Identity Ecosystem Framework must provide for equality in the arbitration of personal privacy among members of the end-user community. To a large extent, the potential "pull through" of regulatory constraints might be considered a "feature" rather than a "risk". Moreover, it seems clear that in addition to "pull through", there will be "push back" from the Identity Ecosystem Framework into the existing regulatory environment mandated by a comprehensive and expansive concept of personal privacy of the members of the end-user community.

1.8 *What are the most important characteristics (e.g., standards and technical capabilities, rulemaking authority, representational structure, etc.) of the steering group?*

Comment: The stakeholder community suggested in an earlier comment recognizes a comprehensive environment that must be addressed by the steering-group. This environment is not limited to the technical (digital) domain of cyberspace. Rather, it encompasses the intersection or extension of the existing social interaction environment into the digital domain of cyberspace.

1.9 *How should the government be involved in the steering group at steady state? What are the advantages and disadvantages of different levels of government involvement?*

Comment: The government must provide the basis of trust in the Identity Ecosystem Infrastructure. Ultimately, the distinguishing of individuals (i.e. authenticating differential-identity) is a mandate of government. The mandate is well established by the Constitution of the United States.

Government may, of course, choose to adopt this mandate to varying degrees. If government divorces itself from the infrastructure, then the trustworthiness of the infrastructure will suffer as a result. The alternative, of course, is not suppressive government control, but rather is comprised of the effective arbitration of the intersection of personal privacy among members of the end-user community.

In some instances, it may be necessary for government to infringe the personal privacy of individuals. This will, of course, be subject (just as current law is subject) to the demonstration of a compelling state interest in the infringement. There is less of a mandate for government to store information “about” people; i.e. to record the results of their interactions. This storage of (i.e. memory of) information about people should be subject to the arbitration of personal privacy among those participating in an interaction. It is, or course, quite reasonable for government to enforce the relevant policy that derives from this arbitration. And, in the case of a demonstrable compelling state interest (e.g. criminal acts) it may well be the responsibility of government to act as a repository for this experiential-identity information. But, in general, while government should be directly involved in the mechanics of distinguishing people (differential-identity), it should only be peripherally involved in the mechanics of maintaining information about people (experiential-identity).

2 - Steering Group Initiation

The initial membership in the steering-group should be submitted by consortia or other formal bodies relevant to the stakeholder groups listed above. Using formal groups, as opposed to soliciting membership from specific companies, will mitigate the possibility of large, multi-national corporations seeking membership on behalf of various stakeholders. Some possible formal groups might be (Note: this list of organizations is merely representative; it is not exhaustive.):

a. End-user community
   This group is ultimately represented by government. It would seem most appropriate for a representative to be selected by the relevant governing body responsible for the steering-group. The individual chosen should assume a fiduciary duty to the end-user community alone; not to one of the other stakeholder groups.
b. Service providers
   There are many large corporations and consortia that operate in this domain: for example, (1) The Open Group, (2) The ETSI consortium, (3) The EMV consortium, (4) SC38, the U.S. TAG for distributed computing
c. Token providers
   There are several consortia that operate in this domain: for example, (1) The Smart Card Alliance, (2) The Java Card Forum, (3) The Global Platform Alliance, (4) B10, the U.S. TAG for card based tokens
d. Identity brokers
   There are several government agencies that operate in this domain: (1) the Department of Motor Vehicles for most state governments, (2) the AMVA consortium, (3) VeriSign
e. Connectivity providers
   This is the domain for
f. Platform providers
   It should be noted that trust in platforms of necessity derives from outside the platform; for example, from certification procedures. It is impossible to establish trust in a platform using mechanisms subsumed by the platform.
g. Adjudication (law enforcement and judiciary)
h. Regulatory (rule-making and certification)
i. Privacy

2.1 *How does the functioning of the steering group relate to the method by which it was initiated? Does the scope of authority depend on the method? What examples are there from each of the broad categories above or from other methods? What are the advantages or disadvantages of different methods?*

Comment: The scope of authority, which exactly corresponds to the scope of trust of the infrastructure, must ultimately meld with the police powers of the state. Only in this way can

consequences for attacks on the trust infrastructure be addressed. The need for an Identity Ecosystem Infrastructure is an explicit recognition of the lack of adequate police power based oversight of the current incarnation of cyberspace. While the term "police power" is rather pejorative in this context, it is particularly germane to the discussion. At the present time, attacks on the trust infrastructure (to the extent that it exists at all) of the Internet and the World Wide Web are extremely difficult to address through existing legal mechanisms. Consequently, the Identity Ecosystem Infrastructure must feature complementary aspects of technical and legal mechanisms through which enhanced trust can be derived. It should be recognized that such trust mechanisms are as much of a guard against misplaced government authority and actions as they are a guard against existing threat communities.

2.2 *While the steering group will ultimately be private sector-led regardless of how it is established, to what extent does government leadership of the group's initial phase increase or decrease the likelihood of the Strategy's success?*

Comment: While the private sector may ultimately lead the steering-group the rationale for this is not entirely obvious. The ultimate causal basis of trust within the infrastructure will likely have to derive from legal policy. Moreover, within the stakeholder groups identified earlier, only government is based on mechanisms that are fundamentally aimed at addressing the interests of the end-user community. For essentially all the other private sector stakeholders, the end-user community represents a potential marketplace for goods and services. In such instances, the private sector entities typically have a legal fiduciary duty to their owners and operators such that the interests that bear on this duty may be at odds with the best interests of the end-user community. This can sometimes be the case even under the mechanisms of governance, but such instances typically can only be addressed through government.

2.3 *How can the government be most effective in accelerating the development and ultimate success of the Identity Ecosystem?*

Comment: Government can accelerate the development and success of the Identity Ecosystem by recognizing and embracing its central role in the ecosystem. As noted above, distinguishing people from a legal perspective is a central domain of government. Whether enforcing legal contracts between private individuals, or enforcing laws that address instances where one individual unfairly infringes the privacy of another (think assault and murder), the adjudication of interaction consequences ultimately falls to government. If the authentication of differential-identity is to be based on tokens or biometrics (or both), government has to be the ultimate source of trust implicit in the issuance of the authentication mechanisms and in addressing the consequences of authentication operations.

2.4 *Do certain methods of establishing the steering group create greater risks to the Guiding Principles? What measures can best mitigate those risks? What role can the government play to help to ensure the Guiding Principles are upheld?*

Comment: Government can play its most effective role by directly impacting the principles of "privacy-enhancing", "security and resilience", and "interoperability". By establishing administrative rules, certification procedures and adjudication mechanisms, government can enhance the levels of trust derived from the infrastructure. Effective trust will encourage the voluntary aspects of end-users choosing to engage the infrastructure. This, in turn, will foster the marketplace through which cost-effectiveness and ease-of-use will ultimately derive.

2.5 *What types of arrangements would allow for both an initial government role and, if initially led by the government, a transition to private sector leadership in the steering group? If possible, please give examples of such arrangements and their positive and negative attributes.*

Comment: In order to achieve the necessary levels of trust in the operational environment over the long term, government must have a continuing role in the leadership of the steering-group. Identity is a basic function of government. Government must exhibit ongoing involvement to achieve a long-lived trust infrastructure.

3 - Representation of Stakeholders in the Steering Group

3.1 *What should the make-up of the steering group look like? What is the best way to engage organizations playing each role in the Identity Ecosystem, including individuals?*

Comment: As indicated in earlier comments, the steering-group should be made up primarily of representatives put forward by existing organizations (e.g. consortia) that address various stakeholder domains. The steering-group must be relatively small (suggested 9 members) in order to allow any semblance of effective operation. If every member of every stakeholder domain seeks a seat on the steering-group, it will be far too large to achieve any level of coherent guidance.

3.2 *How should interested entities that do not directly participate in the Identity Ecosystem receive representation in the steering group?*

Comment: Such entities should participate indirectly through existing organizations (e.g. consortia). This makes it imperative that the organizations selected to be "representation feeders" into the steering-group not have excessively onerous membership requirements. It must be possible for small organizations or even individuals, as well as large organizations, to have representative participation in the steering-group.

3.3 *What does balanced representation mean and how can it be achieved? What steps can be taken to guard against disproportionate influence over policy formulation?*

Comment: The purpose of the Identity Ecosystem Framework is to allow participants of interactions conducted in cyberspace to establish sufficient levels of trust to conduct those applications. The purpose is NOT to enhance the business opportunities in this domain, other than to recognize that enhanced trust will lead to tremendously expanded business opportunities. Thus, the primacy of the end-user community must not be subverted for the sake of other stakeholders. As noted earlier, all stakeholders will participate in the Identity Ecosystem Framework as end-users. The interests of the end-user community should be the central focus of the steering-group.

3.4 *Should there be a fee for representatives in the steering group? Are there appropriate tiered systems for fees that will prevent "pricing out" organizations, including individuals?*

Comment: No! And, as noted above, the membership requirements in organizations used to feed representation to the steering-group should not be particularly onerous!

3.5 *Other than fees, are there other means to maintain a governance body in the long term? If possible, please give examples of existing structures and their positive and negative attributes.*

Comment: In order to maintain independence from the various stakeholder groups, funding for the governance body should derive from government. This domain is an iconic illustration of a domain that should be supported through government funding! Of course, as is the case with other infrastructure needs (e.g. roads, waterways and aviation), funding should ultimately derive from some fee structure paid by the end-user community, but probably administered by government.

3.6 *Should all members have the same voting rights on all issues, or should voting rights be adjusted to favor those most impacted by a decision?*

Comment: As noted earlier, the steering-group should exhibit a fiduciary duty to the end-user community. If the steering-group is properly constituted, an equal vote among all its participants will likely result in the most reasonable prospect for complying with this fiduciary duty. Hopefully, if the various stakeholders are correctly identified, the net competing impact of their respective interests will ultimately prove neutral to the end-user community.

3.7 *How can appropriately broad representation within the steering group be ensured? To what extent and in what ways must the Federal government, as well as State, local, tribal, territorial, and foreign governments be involved at the outset?*

Comment: As indicated earlier, the best approach to achieve broad representation is to select feeder organizations that cut across the domains of interest. This might entail either periodically drawing steering-group representatives from different organizations, or to encourage efforts to achieve some level of coherence among organizations in different domains.

4 – International

4.1 *How should the structure of the steering group address international perspectives, standards, policies, best practices, etc?*

Comment: The steering-group should work within existing international standards, or with existing standards organizations, to address the technical details of the Identity Ecosystem Infrastructure. There is no shortage of standards and standards organization that are applicable to this domain. In the policy domain, the steering-group should work through existing international (inter-governmental) agreements. The real problem to be addressed by the infrastructure is the initial causal basis of trust for the entire (international) infrastructure. This is a social policy issue, not a technical issue.

4.2 *How should the steering group coordinate with other international entities (e.g., standards and policy development organizations, trade organizations, foreign governments)?*

Comment: In all likelihood, the members of the steering-group will be part of organizations that participate in various, relevant standards organizations. At most, the steering-group might seek to establish liaison associations with such standards organizations in order to make sure the needs and concerns of the Identify Ecosystem Infrastructure are properly conveyed to the standards groups that may seek to develop or evolve standards to address such concerns.

4.3 *On what international entities should the steering group focus its attention and activities?*

Comment: The most relevant groups are ETSI, ICAO, Global Platform and the SC38, SC37 and SC17 standing committees of the International Standards Organization.

4.4 *How should the steering group maximize the Identity Ecosystem's interoperability internationally?*

Comment: Achieving interoperability among diverse implementations within a complex infrastructure is a difficult task. In general, achieving interoperability involves at least three areas of concern:

a. Backward compatibility
b. Static interoperability
c. Dynamic interoperability

Backward compatibility refers to making new systems or new capabilities within systems continue to interoperate with existing systems in areas where there is overlap. For example, Common Access Cards (CAC cards) and PIV Cards (Personal Identity Verification cards) are existing identity tokens.

They are based on *de jure* and *de facto* standards. Consequently, when new systems are defined which overlap the domain of smart card based tokens, it is not unreasonable to expect those new systems to be able to use existing CAC and PIV cards.

Static interoperability refers to specifications that will allow independent implementations of a complete system, or major elements of a system, to be interchangeable. Static interoperability is achieved through detailed, standardized specifications that are of sufficient completeness to allow independent groups to implement equivalent versions of the specification. Achieving static interoperability also requires standardized conformance testing that can be used to confirm the equivalence of the independent implementations.

Dynamic interoperability involves the creation of forward looking, standardized specifications of mechanisms that will allow independent system implementations to evolve over time and still maintain a sufficient degree of interchangeability. This is usually achieved through discovery mechanisms. This approach also requires conformance testing to confirm that the implementations of such discovery mechanisms are sufficient to really track the evolution of systems.

In the area of interoperability of token based identification systems, the ISO/IEC 24727 Interoperability standard utilizes all three mechanisms to achieve interoperability among such identification systems. It is a standard that certainly should be considered within the domain of the Identity Ecosystem Framework.

4.5 *What is the Federal government's role in promoting international cooperation within the Identity Ecosystem?*

Comment: If the Identity Ecosystem Framework is to function in an international environment, the trust infrastructure on which it is based must be international in scope. This can only be achieved through inter-governmental agreements pursued by the Federal government.

Summary

The comments presented include a number of suggestions for government involvement in the Identity Ecosystem Infrastructure. Such involvement is, of course, a policy decision ultimately to be made by those who implement and deploy the infrastructure. In general, all of the relevant mechanisms incorporated in the infrastructure should be policy neutral. That is, policy should never be implemented directly within the mechanisms. It should certainly be possible to derive some level of causal trust from non-governmental sources.

Others may present more compelling arguments for deriving trust from non-governmental sources. In this case, it will obviously be up to the steering-group and its associated organizations to compare and contrast the arguments and to determine the most appropriate approach.