ELECTRONIC FRONTIER FOUNDATION
Protecting Rights and Promoting Freedom on the Electronic Frontier

July 22, 2011

Annie Sokol
National Institute of
Standards and Technology
100 Bureau Drive, Mailstop 8930,
Gaithersburg, MD 20899

Re: Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace

Dear Ms. Sokol:

The Electronic Frontier Foundation (EFF) is pleased to share our thoughts on the NSTIC steering group and governance structure.

EFF has previously expressed concerns about the potential privacy costs of NSTIC as well as the many technical barriers to a stable voluntary federated ID management system. In this brief submission, we do not repeat those concerns, and focus mainly on how, from the perspective of an independent public-interest organization, the NSTIC governance structure may be crafted to enhance privacy.

EFF has several major concerns about any NSTIC governance structure.

1. Will the process and outcome be seen as publicly legitimate? The envisioned identity ecosystem will affect many people in many ways, but the "steering" process will have questionable legitimacy unless it is open and genuinely representative of users' interests. More generally, we question whether any putatively representative stakeholder process can be perceived as publicly legitimate in the absence of open public debate at every step of the process.

2. The Guiding Principles are merely general principles, and there will be considerable trade-off analysis in developing rules for the identity ecosystem. We see at least three major issues here:

a. Evaluating trade-offs objectively and accurately requires both information and metrics. It is unclear how members of the steering group, or the constituencies they represent, will obtain the necessary information. Even if they do, it is an open question whether we have sufficiently objective metrics for privacy and security to engage in sound trade-off analysis.

b. There appears to be an implicit but unstated practical assumption that viable business models exist for each of the many components of the envisioned identity

454 Shotwell Street • San Francisco, CA 94110 USA
+1 415 436 9333 +1 415 436 9993 www.eff.org information@eff.org

ecosystem. If it is assumed that the identity ecosystem must exist, it seems to follow that the private business components of the identity ecosystem must also exist and be sustainable. But the commercial incentives of these private components will be to exploit the vast amounts of personal data in the hands of these private components, at the cost of personal privacy. As Landau and Moore put it: "Any identity management system generates rich evidence of transactions as a natural byproduct." (Landau and Moore at 18) We believe that the pressure to commercialize personal data will be enormous; at present, the price of even low-level authentication appears to be significant transfers of personal data, including social graphs, from identity providers like Facebook to other websites.

c. Identity providers and relying parties, concerned about liability, will be particularly prepared to trade off privacy in order to use this "rich evidence of transactions" not only for their own independent commercial purposes but also for dispute resolution and investigating fraud, much as transactional data is used in existing systems. Although the prevention and investigation of fraud can be seen as an important form of consumer protection, it is one in tension with privacy when it involves the creation, analysis, and retention of massive transactional data sets. Nonetheless, the steering group process may tend to dismiss privacy advocates' concerns about this accumulation of data as insufficiently grounded in operational and business experience.

3. Reliance on a multi-stakeholder negotiation process aimed at consensus is problematic if privacy and security enhancement is a firm criterion. Consumer and privacy groups tend to be financially, technically and politically weak compared to the business entities interested in the identity ecosystem. We expect that business entities with commercial interests will more easily be able to participate in the process and marshal the resources to stay on top of the myriad legal, technical and policy issues. Indeed, business entities may be unwilling to disclose relevant information about their present activities and future plans to advocacy groups, thus weakening their ability to evaluate the privacy and security costs and benefits of proposals. (U.S. law does not give data subjects a general right of access to data third parties hold about them and there is much we don't know about the uses to which data is already being put.) Thus, as a practical matter, the mere fact that consumer and privacy groups are represented does not mean that they will be able to adequately represent their constituencies. Without significant representation-reinforcing safeguards, consumer and privacy interests are likely to be under-represented. Finally, privacy groups may have mixed incentives to engage in the governance process. EFF, for instance, is skeptical that NSTIC will yield privacy and security benefits to ordinary Internet users, and our involvement stems largely from concerns that user privacy and security interests will not be adequately represented as NSTIC proceeds.

4. The role of government poses another set of problems. EFF is pleased that the government is aiming for private, voluntary solutions that lessen the general privacy and civil liberties risks associated with a national ID system, which we and others have previously raised. On the other hand, EFF is dubious that the government can act completely as an "honest broker" in the governance process, for four main reasons.

a. Even if the federal government is not directly represented in the steering group itself, we expect it to have enormous influence in the overall governance process simply by virtue of NSTIC's being a federal government initiative. We are concerned that the federal government will be prepared to accept an outcome that is not meaningfully voluntary and does not enhance privacy and security because failure is not a viable political option.

b. The federal government has mixed incentives in the area of privacy and security; law enforcement and national or homeland security agencies often pursue policies inimical to individual's self-determination in these areas. The current debates over mandatory telecommunications data retention and expansion of the Communications Assistance to Law Enforcement Act are obvious examples. Moreover, because law enforcement and national or homeland security interests are often invoked under conditions of secrecy, with little or no publicly available evidence, it will be difficult in an open process to handle these issues if they surface.

c. NSTIC's Guiding Principles appear to be accompanied by a principle of not stifling innovation. In the policy area of online behavioral tracking, however, we often hear concerns that undue emphasis on privacy will be harmful to innovation (such as innovation around new applications of personal data).

d. The government may have a particularly strong role in crafting liability "rules of the road" for the identity ecosystem. This is not necessarily bad. Experience in other arenas, such as with credit cards, suggests that a purely private standard crafted without consumer input is likely to short-change consumer privacy concerns. But government engagement on liability issues is not guaranteed to resolve them in a more privacy-protective way.

Accordingly, EFF believes that there are two fundamental requirements for the overall governance process. First, the outcome must actually be voluntary and actually enhance privacy and security. Correspondingly, the NSTIC process must be willing to fail if the outcome is not voluntary and unlikely to enhance privacy and security. In our view, if the process is goes forward with the expectation that a system must be created—especially on a quick or fixed timeline—it is highly likely that privacy, security, or both will be sacrificed.

Second, the NSTIC governance process must be open and broadly representative. We are somewhat troubled by the NOI's suggestion that the steering group may be too large to be effective. We are concerned that pressure to make progress will sacrifice representation in the name of expediency. On the contrary, the process must be open and highly representative, even if it is slower as a result.

The government could proactively assist the effective participation of privacy advocates in various ways. One possibility is providing financial assistance or locating grants to help public interest privacy advocacy organizations afford to travel to in-person meetings; an alternative is trying to increase the proportion of deliberations that take

place on-line. Still another approach is to provide staff from government entities specifically devoted to helping make steering group activities more transparent and accessible (while remaining neutral on the substantive issues debated by the steering group). The steering group should also ensure that privacy advocates are represented in any subcommittees and working groups that it may establish.

Many of the issues about identity and on-line identity management are technical, complex, and far-reaching in their implications for specific constituencies and groups of prospective users and participants. We believe that it's important to look for participants from a correspondingly broad field of advocates: not simply the largest and best-known national privacy and consumer organizations, but also smaller and more specialized public-interest organizations, such as those focused on specific kinds of privacy threats and particularly vulnerable constituencies. For example, we would suggest outreach to organizations such as Patient Privacy Rights, Privacy Rights Clearinghouse, the World Privacy Forum, the National Network to End Domestic Violence, Muslim Advocates, CAIR, the National Immigration Law Center, the National Center for Transgender Equality, or the Asian Law Caucus. It would also be valuable to include technically experienced computer security practitioners who are not representing specific firms or industries.

Disagreement within the steering group must be expected. In many cases, disagreement will be based on empirical skepticism about assertions about justifications, technical feasibility, costs, etc. There must be a clear process by which steering group members can express and deliberate about their disagreements.

At all times, the steering group must be broadly representative and accountable. Moreover, it must not treat privacy and voluntariness as mere obstacles or items to be readily traded away. Each of the guiding principles is important, of course, but EFF could not support a system that is secure and resilient, interoperable, and cost-effective and easy to use if it is not also privacy-enhancing and voluntary. The first of the guiding principles must be *primus inter pares*, first among equals.

Sincerely,

Lee Tien, Senior Staff Attorney
<tien@eff.org>

Seth Schoen, Senior Staff Technologist
<schoen@eff.org>

454 Shotwell Street
San Francisco, CA 94110
+1 415 436 9333 (tel)
+1 415 436 9993 (fax)