July 22, 2011

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

By electronic mail to NSTICnoi@nist.gov

Ladies and Gentlemen:

OASIS (Organization for the Advancement of Structured Information Standards) is pleased to respond to NIST's Notice of Inquiry (docket no. 110524296-1289-02, the NOI) regarding Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace (NSTIC or the Strategy) released in April 2011. Based on our 18 years of hosting and facilitation of member-driven voluntary open data standards, we're happy to share our understanding of the common elements of successful standards cooperation programs.

Under the Strategy, the Department of Commerce plans to provide certain facilitative support for the voluntary development of policies, standards, liability and accountability mechanisms, by organizations and individuals (an Identity Ecosystem Framework), which will promote widely-interoperable and trusted digital identity systems. The NOI asks how stakeholders in those systems could best organize to develop and maintain that framework, and how the federal government ought to be involved.

OASIS is a voluntary standards organization, with many constituent members, who may have their own views and responses to the NOI. Of course, their opinions are their own, and this response does not represent the views of any members, but only the observations of OASIS professional staff.

Summary.

A permanent structure for ecosystem self-governance should be standards-based, self-governing, open in the sense of transparent, and open in the sense of accessible. The basic technical plan of NIST's SGIP program has worked well: (1) map existing standards, (2) devise a standards roadmap, permitting some optionality, (3) identify gaps, and (4) commission SDOs to fill gaps. Any "steering" structure should be lightweight, and facilitate community decision-making, but not itself hold veto power over substantive technical outputs, which deserve a more broadly democratic process. Some government agencies unavoidably will wear multiple 'hats', but this will not create unmanageable conflicts. The risk of overregulation can be mitigated by careful scoping and requirements-drafting.

Inclusive, successive stakeholder representation requires attention to (a) matters of economic access; (b) remote tool availability; (c) openness of participation and process; and (d) clear, proper IPR rules and terms. In the international area, interoperability with the relevant standards programs of global de jure SDOs may be an important goal.

Background to these comments.

OASIS is one of the largest and oldest global open data standards consortia, founded in 1993 as SGML Open. OASIS has over 5000 active participants representing about 500 member organizations and individual members in over 80 countries. We host widely-used standards in multiple fields including electronic identity and access control, as well as cybersecurity, office documents and smart documents, e-government content standards and electronic commerce (including SOA and web services).

US agencies currently involved as instigators and members in OASIS standards projects include units in DHS (in first responder data and e-health data access), DHHS and the VA (e-health data access and e-identity), NIST (semantic data, cybersecurity, conformance testing and smartgrid), DOE (smartgrid), DoD (supply chain, semantic data and e-health) and NSA (cybersecurity). OASIS also has robustly participated in the planning and execution stages of the US federal Smart Grid (SGIP) project; OASIS experts and staff have participated actively in five of the "PAP" topical panels supplying proposed standards, three of which commissioned new specifications developed in purpose-built OASIS technical committees.

More information regarding OASIS' involvement with e-government projects in the US and elsewhere is contained in OASIS' response to the US National Science and Technology Council's 2010 call for comments on Federal agency standards participation [/n1].

[n1] *http://standards.gov/standards_gov/sos_rfi_docs/95_OASIS.pdf*

Goals of a permanent structure for ecosystem self-governance.

The design of any persistent community to support an identity ecosystem should pay attention to several overarching principles:

- ***Standards-based.*** A large, re-useable identity ecosystem necessarily will rely on the availability of sets of open data standards for vendor-neutral, cross-platform interoperability. This is not to say that an identity ecosystem should or even could exclude nonstandardized innovation and nonstandardized legacy systems; nor that one exclusive set of standards should be preferred for a given function. However, consistent with OMB Circular A-119 [/n2] and industry best practices, the ecosystem should leverage what mature open standards we have (don't break things that already work), and should encourage their extension and improvement (be responsive to use cases).
- ***Self-governing.*** An ecosystem that holds continuing relevance and interest for commercial, citizen and government successful arrangement necessarily is one that's governed by those stakeholders and responsive to their evolving needs. See more under “Role of Government” below.
- ***Open in the sense of transparent.*** A process that asks enterprises to invest time by contributing, and asks for conformance ought to be clear and self-evidently fair enough

to deserve confidence. Processes should be documented and obvious, working drafts and inputs should be visible, and outputs should be well-archived. This transparency helps reduce single-source risks: if an "open" proposal remains too closely isomorphic to a single participant's product or service, sunlight helps, by exposing this weakness to comment, early and throughout the development process.

- ***Open in the sense of accessible.*** See more under “Stakeholder Involvement” below.

[n2] OMB Circular: *http://www.whitehouse.gov/omb/circulars_a119*

As a robust participant in the US federal smartgrid (SGIP) standards project, OASIS believes that NSTIC can learn much from the successes and evolution of that program:.

- The SGIP process and tools are well-designed for openness and inclusiveness.
- SGIP's basic technical methodology, mapped out by NIST at the very start of their project, seems to work well: collect and map existing stable standards, permit optionality, describe an aspirational roadmap of standards, identify gaps, and commission SDOs to create needed gap-fillers.
- Each of the functional areas defined (as 'Priority Action Plans') by the SGIP roadmaps has a stakeholders interest group, and assignments to multiple SDOs to host new work or evolve existing standards to meet the identified needs.

“Steering” with a light touch. Standards work generally, and attempts to govern its participants specifically, have to be conducted with some humility about how much a human process can do. Not all technically-successful standards are widely adopted; market participants and competitors often carry their competing interests into the standards arena. (See Shapiro & Varian [/n3] for a reality check on those matters.) Accordingly, NSTIC should approach the problem of a centralized steering group with some caution.

Separating facilitative decisions from substantive work would be helpful. Administrative matters may sometimes be committed happily to a smaller group; but broad technical decisions usually reside more safely in a large, diverse body. The SGIP bylaws [/n4], and OASIS' own rules for standards approval [/n5], both demonstrate that de-centralization bias:

- Technical products are developed in open expert groups, close to the sources of expertise
- The “governing boards” generally stay out of that work. Even where OASIS members form clusters of related work under a common name (“member sections” in our parlance), the steering committees for those groups defer most technical decisions to the expert technical committees.
- Final approvals are conferred by large member voting processes, not a star chamber.

This approach significantly increases rank-and-file stakeholder investment in outcomes, by reducing the participation-sapping fear that good technical work will be vetoed up the chain by a small control group.

[n3] Shapiro & Varian, Information Rules: A Strategic Guide to the Network Economy (Harvard Business Press, 1999). See also *www.inforules.com.*
[n4] SGIP Bylaws: *http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SGIPCharterAndBylaws*

[n5] OASIS TC Process: *http://www.oasis-open.org/policies-guidelines/tc-process* and OASIS Member Section Policy: *http://www.oasis-open.org/policies-guidelines/member-sections*

Work program coordination. One challenge for a large standards-based project, illustrated by the SGIP's experience, is the coordination of multiple, mostly-autonomous projects into a cohesive whole. The original 2009 draft "map" of about 16 functional areas for Smart Grid standardization spawned 16 workgroups (augmented by a few more later) [/n6] which were expected to re-use some of each others' functionality. Over the life of the project, discrete workgroups sometimes tend to solve their own silo-ed technical problems first, so interdependencies can get lost in the shuffle. SGIP management addressed this by adopting a strong set of dependency models and critical path monitoring, in its administrative "Program Management Office", about halfway through its lifecycle. [/n7] OASIS has experienced similar needs for "shuttle diplomacy" between projects in development, when an interoperable set of outputs is the stated goal. Often, in our experience, the availability of neutrals and "honest brokers" to work out diverging paths is essential; when that task is left to sectoral partisans, it seems to fail a greater percentage of the time. A key design issue for NSTIC should be providing for that role to be populated; this might sometimes by done by and within suitable SDOs, and at other times might require facilitative direct government input.

[n6] Priority Action Plans: *http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PriorityActionPlans*
[n7] SGIP PMO: *http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PMO*

The multiple roles of government and regulation. Multiple government agencies (state and local, as well as federal) unavoidably and necessarily will wear multiple hats in an NSTIC ecology. We see little difficulty with this. Within OASIS standardization examples, some of our government agency participants simply come to the table as one more user with a use case to fulfill (such as the XSPA project [/n8] and PLCS [/n9]); others act mostly as funders and requirements sources (CAP and EDXL [/n10]); some simply provide expertise (KMIP [/n11]).

NIST also long has provided expertise to various US industry efforts in its own areas of technical pre-eminence, which include two of the four NSTIC Guiding Principles: *"secure and resilient,"* relating to NIST's own significant body of cybersecurity guidance and experts, and *"interoperable"*, an area where NIST testbed technology and advice has assisted many industry standards projects. Those resources will assist NSTIC development as well.

One interesting instance of government's role was the 2003 EU-initiated OASIS project on Auto Repair Information, in which a voluntary standard was attempted first, but regulation eventually followed. [/n12]

Legal mandates pose a different set of issues. Governments have a mixed track record, when it comes to incorporating voluntary open standards into regulatory requirements. The lumpy adoption path for HIPAA security procedures after the original proposed rule was promulgated in 1998 [/n13] – with a long list of then-current standards – should give some pause to legislative pens. As can be seen from the many data and security standards referenced in the HIPAA rule appendices, there often is a long time lag between issuance of a data standard, and its eventual citation in a slower-moving body of regulatory requirements. Open standards generally reflect a moving path of technology and consensus; it can be

difficult and sometimes inadvisable to bake that into a static mandate. This is one reason why we admire the SGIP model of stimulating development of data standards, thereby establishing interoperability possibilities and incentives, but without necessarily converting them into positive sources of law.

In the electronic identity ecology, where different sectors come with differing degrees of regulation, there's some concern about accidental “pull-through” of heavier, more burdensome legal mandates into lighter-weight sectors. We suggest that careful, explicit scoping and requirements statements at the outset of projects may do much to reduce that risk. The “pull-through” concern reminds us of the experience our community had a decade ago with encryption trends: New technical capabilities sometimes inspired the escalation of requirements even when not necessary for the purpose. In other words, just because an e-signature *can* be encrypted at the AES 128-bit level (for example) does not mean that it always *ought to* be. In some contexts that's the minimum acceptable; but in others, it's more than is needed. If a standards development process begins with a clear scope statement, and an understanding of the use requirements and risks for a case, those can serve as agreed constraints that help check overspecification beyond what's needed in any given instance.

[n8] XSPA, a healthcare records access control project, championed by the US VA: *http://www.oasis-open.org/committees/xspa/*
[n9] PLCS, a supply-chain product life cycle data project, in which US DoD and contractors for the UK MoD played a key launch role: *http://www.oasis-open.org/committees/plcs/*
[n10] CAP and EDXL: emergency first-responder notice and response message standards, in which US DHS has been a key instigator: *http://www.oasis-open.org/committees/emergency/*
[n11] KMIP: an encryption key management protocol, primarily an industry initiative, but one to which NIST's cybersecurity experts have provided valuable insight. *http://www.oasis-open.org/committees/kmip/*
[n12] EU Auto Repair Info: *http://www.oasis-open.org/committees/autorepair/* A group of automobile manufacturers (OEMs) and auto repair industry representatives in the European marketplace, along with regulators from the EC Enterprise & Industry Directorate, convened an OASIS TC to define data exchange specifications for OEM data about certain vehicle repairs and parts, to make it broadly available to independent repair shops as well as the OEM's own repair facilities. (Among other things, this was thought important to maintain widely-effective auto exhaust emission controls and stimulate competition.) The committee defined and published a mutually acceptable data structure, but declined to approve it by final vote, due to a stated disagreement about how to bear the cost of provisioning that data. Eventually, seeing no voluntary resolution of the cost sharing issue, the European Parliament passed legislation mandating its use nevertheless, in a resolution amending its Directive 72/306/EEC. *http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2006-0561+0+DOC+XML+V0//EN*
[n13] HIPAA Security Rule: *http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html*

Initiation of the self-governance process.

The objective of NSTIC's initial phase should be to use government leverage to encourage a self-governance structure that weans itself off of the need for support.

Several strategies can help reduce the risk of the “Paris Peace Talks Table” problem, where effort spent on jockeying for position can detract from, or sometimes even exceeds, effort invested in the substantive goals of the project.

- As noted above, a steering group may be easier to manage if it is facilitative in nature, and is not chartered not to have its own veto power over the substantive work of technical panels.
- The SGIP program's two-step launch seemed to serve it well. SGIP first built out a draft roadmap and some draft operating rules for consultation in early 2009, using lightly-moderated group meetings to air drafts; and then commenced a second phase by ratifying its operating rules (the 'charter'), and establishing an official governing board under those rules.
- The fast timing sought from the White House for SGIP's launch led to a very compressed conversation about formal project structure. NSTIC does not necessarily need to build its entire permanent framework in a few months.

The two-step approach allows the participating community to react to a strawman charter, thus having more ownership interest in the result, while moving forward simultaneously on substantive mapping and gap-spotting issues. OASIS would be happy to participate in and help facilitate such a first phase. We suggest that NSTIC's program office give serious consideration to asking a collection of relevant cooperating SDOs to do so, as a jointly hosted project.

Stakeholder involvement.

A shared sense of accessibility to decision-making processes enhances participation and buy-in, in a voluntary project.

Economic access to project decision-making is one issue. NSTIC should avoid designs that scale influence with financial contribution. Still, some kinds of meetings fees or periodic fees may become necessary for a self-supporting project eventually.

Another form of resource barrier arises from work that is conducted too quickly or under poor rules for remote participation. A well-formed rule set assures ease of contribution from the outside, and should be permeable & accessible to all points of view -- particularly from stakeholders with a valid but limited degree of interest. Big-conference-room standards & policy work can be a war of attrition sometimes. Stakeholders who aren't inclined, or able, to attend months of meetings, field large teams, or wade through reams of RfPs, still need to be heard fairly.

There are process indicia that can make a difference. In our experience, these include:

- Rule matters such as published stable process rules; careful adherence to agendas; respect for minimum public comment period durations, and reliable, timely posting of meeting reports & results.
- Tool choices, such as official web-enabled workspaces (whether it is a email list, wiki or etc); and avoidance of proprietary and nonpervasive file formats.
- Attention to openness behaviors that may exceed the minimum requirements of OMB Circular A-119 at times. With apologies to Orwell, some open animals are more open than others. In our industry, sometimes the words “standards” and “openness” are too quickly applied. It's common for some proprietary artifacts to simply be named as "standards", without any assurance of their stability, ownership or openness. A handful of aligned interests may quickly create a "dot.org", or a new re-purposing of an old unattended forum, insert the word “open” in various places, but nevertheless mostly remain opaque to the outside. Draft works, or transient versions, may be offered up as if they are final products, though they have none of the assurances associated with the latter. Responsible neutrals and administrators should be cautious about such matters.

Finally, the roles of copyright and patent licensing and disclosure practices cannot be overstated. Constituent stakeholders in the ecology ought to discuss, at the outset of this project, what kinds of license, ownership, archival stability and royalty terms are desired for NSTIC elements or standards body outputs. In our experience, only a very clear set of rules reliably will deflect many risks of license conflict, for standards in development. Also, royalty-free use, and the right to distribute copies freely, may be very important in a widely-adopted architecture.

International considerations.

Most of our work in OASIS has focused primarily on globally-adoptable work, due to the highly-networked, cross-border nature of so many Internet-based transactions and information exchanges.

For this reason, we generally encourage our members to design their standards projects so that they potentially conform to, and are upwards compatible with, submission to global *de jure* standards bodies (e.g., ISO, IEC, ITU). OASIS and other peers worked, early in the SGIP project, to make eventual sharing of the US program's outputs with the relevant international IEC panels a program requirement.

Generally, in practice, we have seen little difficulty when national-oriented voluntary industry standards programs simply welcome those foreign participants who wish to participate. Seeking formal relationships beyond a simple exchange of liaisons may not always be necessary – or even advisable, in cases where asking for a formal designation would amount to asking for recognition.

Respectfully submitted,

James Bryce Clark
General Counsel, OASIS