OASIS RESPONSE TO NSTC REQUEST FOR FEEDBACK ON STANDARDS PRACTICES

OASIS (Organization for the Advancement of Structured Information Standards) is pleased to respond to the request from the National Science and Technology Council's Sub-Committee on Standards published at 75 FR 76397 (2010), and extended by 76 FR 3877 (2011), for feedback and observations regarding the effectiveness of Federal agencies' participation in the development and implementation of standards and conformity assessment activities and programs.

We have advised our own members about the Federal Register inquiry, in case they wish to respond. 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.

I. RESPONDENT'S BACKGROUND

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 600 member organizations and individual members in over 80 countries. We host widely-used standards in multiple fields including

- cybersecurity & access control (such as WS-Security, SAML, XACML, KMIP, DSS & XSPA) [/1],
- office documents and smart semantic documents (such as OpenDocument, DITA, DocBook & CMIS) [/2], and
- electronic commerce (including SOA and web services, such as BPEL, ebXML, WS-ReliableMessaging & the WS-Transaction standards) [/3]

among other areas. Various specific vertical industries also fulfill their open standards requirements by initiating OASIS projects, resulting in mission-specific standards such as

- UBL and Business Document Exchange (for e-procurement) [/4],
- CAP and EDML (for emergency first-responder notifications) [/5], and
- LegalXML (for electronic court filing data)[/6].

Several OASIS activities also specifically address e-government framework needs. [/7]

Each technical project at OASIS is encapsulated in a specific Technical Committee (TC). As of this writing, we currently host over 70 active technical committee projects. Our TCs collectively have produced hundreds of final specifications, of which about 90 have been nominated and selected by our membership as OASIS Standards. Around 50% of our members are technology providers, 35% are users and influencers, and 15% government and academic institutions. Government agencies from US federal government agencies, and others, frequently initiate and participate as members in OASIS TCs. NIST itself has supplied some of our key TC experts and chairpersons, for various relevant strategic projects, throughout our 18-year history. NIST and US federal agency involvement in OASIS TCs is discussed further below.

OASIS maintains a professional staff to facilitate and guide our members' standards contributions, supervised by a Board of Directors, elected globally from our members, who ultimately govern OASIS as a US (Pennsylvania) not-for-profit corporation. OASIS charges a membership fee to sustain its operations on a cost-recovery basis, but makes every effort to keep participation accessible for individuals and smaller organizations, including entry-level low-cost associate memberships often used by SMEs and members in developing countries.

OASIS puts strong emphasis on global accessibility to its work process and its output. About one-half of our participating experts self-identify as being located in North America, with the majority of the reminder being in Europe and Asia. The consortium has enjoyed broad international participation and adoption. We work closely with, and work avidly on cross-fertilization among, both *de jure* standards authorities such as ITU, ISO, IEC, JTC1, ANSI, INCITS, ETSI, CEN, etc., and a wide range of other industry consortia. It's our general practice to encourage cooperation and share widely, and many of our standards are submitted to and adopted by other bodies.

Our process and intellectual property rules widely are considered the best of class in our field, and provide strong support for a fair, transparent playing field in which market participants, academics and public administrators collaborate on shared beneficial open data structures. Further details on our process and IPR practices, and government agency activity in OASIS, are noted where relevant in our response below.

II. OASIS ACTIVITIES RELEVANT TO INQUIRY

The Federal Register inquiry notes several specific areas of interest: SmartGrid, Health Information Technology, Cyber Security, Emergency Communications Interoperability & Radioactivity Detectors and Radiation Monitors, and Other technologies involving significant Federal agency participation. This section notes relevant OASIS and e-government activities, for purposes of context.

(a) OASIS in US government SmartGrid activities

In the US "SGIP" project, OASIS was one of the consortia asked originally by NIST to participate in the planning stages (in 2009), and provided a number of standards for populating the project's first draft roster of open data standards useful and relevant to a common SmartGrid data architecture. OASIS experts and staff have participated actively in five of the "PAP" topical panels supplying proposed standards, three of which are bring fulfilled by new specifications developed in purpose-built OASIS technical committees. [/8] One of those committees, addressing electricity demand/response exchanges, is co-chaired by a senior NIST technologist.

OASIS staff actively works with the NIST staff, and their SGIP contractors drawn mostly from the utilities industry, to help ensure a successful program. OASIS representatives attends the relevant SGIP proceedings, providing a neutral open-standards perspective in panels often largely composed of commercial stakeholders. At appropriate times, OASIS also has made experts available for consultations with FERC, the White House OSTP, state PUCs and other agencies, to assist or provide expert information on various issues involving licensing, program governance and architectural matters as well.

(b) OASIS in US government Health Information Technology activities

OASIS open data standards for identity, message security and access control have long been employed for various health IT implementations. Among other things, the 2003-04 implementation of mandatory electronic health records by the NHS, in the UK [/9], and the 2009-10 US Army & Veterans Administration implementations of web-services-based military personnel health records [/10], were based on OASIS standards, and government representatives drove the development or extension of these specification projects.

In 2005-09, US HHS through its office of the National Coordinator for Health Information Technology administered a multi-year program called the "Healthcare Information Technology Standards Panel" (HITSP), for which ANSI served as secretariat, to identify and if necessary extend open standards for implementation of HHS' various electronic-records regulatory initiatives beyond HIPAA. OASIS, along with several health-facing consortia including HL7 and IHE, assisted in the original design and requirements process for HITSP, and supplied many of its existing standards into the community pool of approved and recommended specifications. Quite a few of our security and access control standards were included in the HITSP recommendation lists amassed before the project's termination. However, for purposes of this study, it should be noted that those final lists did not appear to be supported by the government by inducements, assistance, significant mandates or even clear final guidance, and so industry benefit from the project's work was only intermittent when the program ended.

(c) OASIS in US government Cyber Security activities

OASIS data security standards are in wide use in a range of public and private sector implementations. Several OASIS Standards including DSS and KMIP provide specific extended functionality to asymmetric encrypted key technologies, which various implementers of modern PKI find useful. [/11] For the most part, these specifications tend to be elective components in a security architecture, not a mandated practice. However, in the access-control and identity domains, key OASIS Standards are central to current best practices. OASIS was consulted and provided expert comment to NIST staff in preparation for the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative, subsequently announced by the White House cybersecurity office and the Department of Commerce. NSTIC relies somewhat on outputs from several consortia and organizations (including the Open ID Foundation and the Kantara Alliance), which in turn base some of their core technologies on OASIS standards including SAML, XRI and XACML. [/12] Providing technical material, regular liaison and some degree of advice and stability to those organizations, which share overlapping experts and interests with OASIS, has been a key OASIS deliverable in support of the NSTIC initiative.

It may be useful to note that the key data specifications are more than serialization methods: often, their most important role is to reify and represent underlying data models, use cases, workflows and policies that already have been established by practice. Those codified processes often have value well beyond any specific instantiation of code or markup. Thus, as with earlier migrations of EDI practices into XML in our field, the underlying standards-implementing work of analysts and implementers to normalize data and business processes, in the encodings used today, likely also will underpin future encodings as well. This helps ensure the achievement of assurance and policy goals, as business process owners normalize their activities, even though tools evolve from format to format and programming method to programming method.

(d) OASIS in US government Emergency Communications Interoperability activities

OASIS work on widely-usable, simple alerting protocols began with the "Common Alerting Protocol" (CAP) project early last decade, an initiative started by US-based commercial vendors to first responders. OASIS' Emergency Management TC has enjoyed long-time active participation and implementation by multiple agencies including the Department of Homeland Security (through FEMA's Disaster Management eGov Initiative), the National Weather Service, USGS, and state emergency services and transportation agencies, resulting in a final first release in 2004. Subsequent work, also involving those agencies and commercial implementers, as well as global ITU workshops (and parallel approval by ITU), have produced several updates and extensions to CAP. Due to OASIS liaison work and the efforts of our experts, relevant data elements of CAP also were incorporated in the Department of Justice's "Global Justice XML Data Model" project, the precursor to the current US interagency "NIEM" data elements catalog, and so also interoperate with that vocabulary. NIEM and

GJDXM shared design elements and experts, early on, from our LegalXML projects as well. With continued support from DHS, the OASIS TC has developed additional related Emergency Data Exchange Language (EDXL) standards for responder resource tracking, hospital bed and patient provisioning and similar functions.

(e) Nascent cloud computing activities and other technologies

Recently, NIST and other agencies have focused closely on cloud computing architectures as alternative or additional solutions for many e-government operations. In some functional areas, cloud computing may present novel issues. In many others, the architectural and risk issues derive from other, known bodies of work, many of which already are addressed by existing technical guidance documents and open standards, from OASIS and other standards bodies. As with the SGIP SmartGrid program, the federal government's interest to spur development of cross-platform methods for "the cloud", and enjoy the network effects of standardization, likely will require some cat-herding and facilitated cooperation. OASIS standards projects will happily assist in those efforts. As a well-established organization with a broad, diverse technical membership, OASIS takes a conservative approach in new project announcements and claims; still, several OASIS cloud projects are in process, and one is approaching mature deliverables. [/13]

Of course, in addition to the foregoing vertical areas, a number of other foundational and architectural projects at OASIS provide basic methods that are widely embraced by e-government projects in the US and globally. OASIS-hosted foundational work, contributed from a variety of our member technical communities (see Section I above), underpins many current G2B and G2C installations.

III. STANDARDS PROCESSES, PARTICIPATIONS & BENEFITS

This request for comment notes correctly that the US policy framework for standardization, under the NTTAA (1995) and OMB Circular A-119, generally guides Federal agencies to rely on voluntary consensus standards, rather than government-created methods. In the Internet, electronic commerce and e-government sectors where OASIS is most active, it is notoriously the case that innovations, and tremendous resulting network effects, often have come from market-based development of voluntary data standards, with minimal or no legal mandating.

The US approach of facilitating organic growth, with various agencies soliciting industry development in their own sectors, seems to have worked quite well. The OASIS-hosted public policy projects noted above are strong evidence of that success in the US, and there are many similar instances in other countries. In contrast, nations which appear, instead, to centralize their data standards management risk being less open to agile technical development, and may have experienced less innovation and technical advance as a result.

As our sector of the standards industry matures, it is important that we respect, and design for, shifts of creative power from toolmakers to data owners and end-users, whose business requirements and use cases must be our ultimate drivers. Data structures unavoidably embed rules and assumptions; those responsible for the real world events and assets that data controls necessarily should be in a position to see, control, and be responsible for, the effects that the data structures impose on those events and assets.

Government encouragement of market-driven open standards development takes several forms. Important junctures where public agencies can and should have an effect include: (a) "openness" as a criterion, (b) competition law enforcement, and (c) encouragement of conformance & interoperability.

(a) Openness, RfP criteria and mandates

Agencies often are called upon to assess whether an offered "standard" comes from a source and process with sufficient indicia of openness and fairness. This assessment, informed by the NTAAA and Circular A-119, may arise in the context of purchasing program criteria, a proposed legal mandate, or regulatory guidance to an industry to seek consensus. In such assessments, public officials may need to make evaluative judgments about a standards organization, its process, constituents or outputs.

The expected benefit of "open" process is a fair and broadly-considered outcome. It is hoped that those qualities support higher likelihood of a standard's stability, quality and vendor-neutrality. But these determinations are nontrivial, and sometimes difficult. Self-assertions of openness and transparency are rampant, but rarely sufficient. We note that, in several broad e-government projects in which we've worked, specifications and stakeholders sometimes are drawn into disputes over the merits of one method or another, or one organization over the other, where facial sparring over the relative "openness" of an artifact or source simply might be a veneer over subjective competitions among adverse stakeholder groups. In the government's facilitative work [/14], careful attention sometimes must be given to the breadth, process and transparency of projects offered up as standards, to ensure that they will be acceptable for reference by federal and state regulators as the safe and genuine output of “voluntary consensus standards bodies” under the NTTAA and OMB Circular A-119.

The fast pace of information technology, public policy considerations of access and fairness, and the novel ways in which stakeholders may cooperate formally or informally, all have *increased* the pressure on public agencies to assess standards landscapes. Agencies need clear and objective criteria to help identify genuinely open and transparent standards activities, and to provide reasonable degrees of vendor- and stakeholder- neutrality. In our industry today, the nomenclature of standards may be too quickly misused. It's common for some proprietary sources to simply name their artifact a "standard", without any assurance of its stability, ownership or openness. *Ad hoc* efforts have value. But it's also possible for a handful of aligned interests to quickly create a "dot.org", or a new re-purposing of an old unattended forum, to provide an appearance of vendor-neutrality, while remaining completely closed and tightly controlled.

Several specific elements seem to us to be obvious common indicia for examination.

- One is *transparency*: reasonable public access to working draft materials and contributions. This helps reduce single-source risks, if an "open" proposal remains too closely isomorphic to a single participant's product or service, by the sunlight method of exposing it to comment. However, standards groups differ in their degree of transparency, sometimes due to their business models.

- Another is *permeability and heterogeneity*: standards bodies are more likely to attract diverse, balanced views when their rule-set is readily understandable, their documentation and structure easy to find; and where mature, neutral staff or volunteer leadership genuinely work to maintain an intellectual social ecology that permits new points of view. The rulesets, and what vetoes or supermajority chokepoints are embedded in them, also may matter.

- *A proper leadership and ownership structure* also is essential to reliability. Standards that have stable, reputable hosts and appropriate IPR terms are somewhat less likely to be deprecated, withdrawn, versioned out of existence, or suddenly made unavailable for strategic advantage. This gives users a better assurance of longer-term return on their implementation investments.

Finally, while accreditation of standards bodies has been used as a solution in some cases, it has not fulfilled all public administration needs, and we believe that is likely to continue to be so. Even a group with a set of approved rules can be problematic, if those rules are never followed, or if a homogeneous viewpoint dominates with no checks and balances. Often the lead agency in a given sector, sometimes with expert coaching from NIST or elsewhere, is in the best position to assess a given community of cooperating competitors. European public administrations recently rejected the idea of having *de jure* bodies certify standards consortia, for that reason, and we believe that continues to be the correct answer in the US as well. [/15]

We believe that government agencies increasingly will be called upon to make difficult value judgments about when "standards" efforts can be accorded governmental preference. We note that the current criteria may be evolving, or at least have the opportunity to do so. [/16] The panel may wish to consider how NIST and other experts can improve the objective tools and guidance available to agencies when they must make these determinations. The government should encourage all innovation, but sometimes may need to be cautious about too quickly embracing an artifact before checking its catholicity.

(b) Competition law

We have no complaints about the engagement of US antitrust and fair trade regulators in the open standards arena. But it is important to note, for a complete picture of the use of standards in public administration, that *de jure* and consortia standards organizations both rely on the functions provided by those regulators. The latter provide assurances that simply may not occur in standardization organically.

If a group of stakeholders collaborate on the creation of open standards, in conformance with well-formed rules of a reputable neutral standards body, those rules should indeed provide some assurance about the openness, fairness and quality control of the outcome. If the group's IPR practices are well-formed, the resulting availability of user licenses should be improved.

But other issues relevant to a standard's equanimity are left to external regulation: whether a disclosure, voting block or royalty-seeking behavior is a deceptive practice, or whether a patent arrangement has competitive consequences (just to pick two examples), are matters usually simply not addressed by the rules of even the best organizations. Public administrators who rely on the openness of a standards host should remain aware of the limits to what a properly open and neutral process can assure.

(c) Conformance & interoperability

In our domains of e-commerce, structured data and cybersecurity, many standards developed in the last decade are just now reaching a critical mass of entrenched use. That body of widely-used standards is only recently at the advanced lifecycle stage where users may broadly feel a need for sustained maintenance and testing capabilities.

This is in part because of the different ways in which software serves as a user's interface into standardized open data. In a data exchange domain where all data is siphoned though a handful of dominant software applications, users may not quickly reach acute pain points over technical conformance. To oversimplify, for example, if the most popular web browsers in 2005 reliably could exchange web page data among themselves, many lay readers of static web content might have seen no problems, even if conformance with the web standards was missing.

However, in a many-to-many data exchange environment, technical conformance becomes a more acute issue. A new entrant who relies solely on conformance to a declared standard, in order to join an exchange, could be thwarted if the established players can "talk to" each other, but not to him. Consider, in the SmartGrid case, the anticipated conversion from a closed ecology of control signals from a finite number of utilities and their contractors, to one where a multiplicity of signals is expected to be transmitted and re-used -- by a host of additional disruptive new entrants, innovative services from heretofore-uninvolved parties, and various devices from a large number of new manufacturers. (Arguably, the same diversification has happened to the web, as well.)

Such broad, heterogeneous networks can only form with, and must rely on, standards that provide widely-available, objectively-testable criteria. (Laudably, the NIST SGIP project is structured to provide for this requirement, although at this writing the program's conformance execution successes remain in the future.) We believe that the kind of significant technical assistance, test-bench facilitation and advocacy of precision that NIST has helped foster, in the SGIP program, will become more widely sought and required elsewhere, as government continues to encourage and promote many open exchanges and marketplaces of shared data. We look forward to continuing to collaborate with NIST and various agencies to make that possible.

OASIS has worked closely and happily with NIST on many conformance-promoting activities, from the guidance authored by the first OASIS Conformance TC (chaired by a NIST expert) in 2002, through several extensions of that guidance [/17] and into various concrete projects like the SmartGrid work mentioned above. OASIS rules require that our final specifications obtain implementer statements of usage, and include specified forms of testable conformance clause. Additional interoperability test requirements apply to work that OASIS submits to other external organizations. OASIS continues to sharpen its requirements in support of conformance, and believes this is a necessary strategy for any peer seeking to supply reliable open standards. We expect that public agencies will need to give increasing attention to this element of an "open" standard, and that there may be more call for NIST to facilitate or encourage joint testing activities, as reliance on stable open standards continues to grow.

IV. ISSUES IN STANDARDS SETTING

The Federal Register inquiry asks for comments on coordination with foreign open standards and foreign regulations, and on intellectual property rights handling within standardization.

(a) Foreign coordination

OASIS generally shares the values expressed by the open government data movement and the World Trade Organization’s Technical Barriers to Trade Agreement, which assume that mobility of data via common standards is a public good, and that gratuitous variations or opacity in data structures should be viewed skeptically, as a possible competitive obstacle or trade barrier. (There are limited use cases where national boundaries appropriately apply to shared data structures, but for most e-transaction networks this probably is not the case.)

Accordingly, re-use of global standards usually is superior to re-invention of a method at a national level. Generally, we have pursued this view in the projects described above, advocating, for example, for contributions of the SGIP standards up to the IEC upon completion, and for extensions of US-derived healthcare data transaction standards to international use cases. Usually we enjoy receptive reactions from federal government agencies.

However, we do occasionally encounter geographic "not-invented-here" resistance from stakeholder groups or some standards organizations. A few sectors, even sometimes supported by government sponsorship, may see themselves as having an exclusively-US constituency or political ecology. Some may not yet have confronted the likelihood that some components of their data transactions will cross borders eventually, regardless. So, in government-facilitated or funded work where the use cases and security considerations are appropriate, we would like to see federal agencies promote the same general receptivity to global interoperability, in their contractors and supported standards projects, that the agencies themselves laudably demonstrate.

In our own experience, consortia standards from established bodies tend to naturally take global re-use into account, as they are market-driven, influenced by the natural flow of the relevant data across geographic boundaries. Many of the key projects with which we work are as thoroughly international as OASIS. Since 2002, we have been signatories to and participate in the MoU on global coordination of Electronic Business standards with ISO, ITU, IEC and UN/ECE, which helps identify points of cooperation or overlap [/18]; and we maintain multiple liaisons across the globe with standards activities in order to share or collaborate on work of mutual interest.

(b) Intellectual property rights and standardization

What kind of IPR policy a government ought to require, and whether royalties are tolerable in standards used in public administration functions, is one of the great debates of the current decade. This topic was recently and prominently debated in the development of the European Interoperability Framework (version 2) paper issued last month. [/19] The manner in which free and open source software licensing interfaces with commercial licensing goals also has been a topic of detailed discussion. [/20] Those debates seem fated to go on for some time. Still, we may be able to offer some specific observations about IPR licensing and standards generally.

First and of most importance, a careful, thorough and reliably administered IPR or patent & copyright licensing policy of *some* sort is essential to any standards project. When we are working with other organizations, a policy that is unclear or missing is much more problematic than one that varies from ours in substance. Unfortunately, we cannot overstate the number of times that otherwise-plausible organizations have proceeded with flawed or incomplete IPR rules, or shorted their importance, resulting in outputs with fatal provenance problems. Agencies must make a competent assessment of any standards partner's IPR practices, as a key facet of their evaluation and purchasing criteria.

The reliability of license commitments also matters. Our own practice since 2005 has been to secure written commitments at a project's outset from participants, to license in support of the final output of committees in which they have made contributions. [/21] Other peer standards organizations have copied our model. We heartily recommend that approach. It seems to have worked well for our community, and avoids some of the problems of errant, late or incomplete disclosure that have hampered some well-known standards projects.

Availability also sometimes is an issue. OASIS permits its standards to be read and used freely without imposing any copying charges. Some other consortia (like IETF and W3C) and some *de jure* standards bodies (like ITU) do the same. Others are dependent on their sales revenue model and do not permit copies to circulate other than by sale. While both models may be valid, the for-pay model creates some obvious obstacles to public review. In our own SmartGrid work, we occasionally have needed to enter into complex, burdensome arrangements to make sure that price-bearing, restricted-circulation draft copies of one cooperating group can be shared, for review and coordination purposes, under some kind of one-off license with the members of another (no-charge) standards group who normally posts their work in public. This may be no problem for small or single-industry ecologies, but can be a damper on collaboration as a community grows larger and more heterogeneous. Agencies should give thought in advance to their specific use case, and the needs and tendencies of necessary stakeholders and the relevant public, before carefully specifying in advance what accessibility to drafts and final outputs will be required from an endorsed standards host.

OASIS does trend towards royalty-free standards. Our members are allowed to publish claims, for standards where they have contributed, indicating that they seek a license, or if the TC reserves this option, a royalty. However, we note that the number of projects and members in our domains who seek any payment, or even a written license, appears to have decreased steadily and markedly over the past five years. To the extent that our committees represent our "market", the market is measurably moving towards free and unrestricted re-use.

The data exchange architecture of an anticipated user base also may matter. A many-to-many network (of the sort described earlier), which constantly acquires new self-designed nodes, might find it difficult to leverage data encoded in a standard that requires each new user to enter into a legal contract in order to decode it. On the other hand, users in an oligarchic technical data exchange market, where all users participate via a handful of portals or suppliers who cross-license, might not encounter this problem.

Finally, combinations of standards often multiply intellectual property use concerns. This is a nontrivial issue, sometimes unwisely glossed over. Consider a theoretical standard W from a facially-appropriate source which says "do X+Y+Z", where X is a native process described and licensed in the open standard, but Y and Z each are proprietary technology developed in some other non-open process, and incorporated only by reference. If a regulator instructs a market participant to use the nominally-open W, she may for all practical purposes also be requiring him to use Y and Z as well. Agencies should assess the licensing effects of proposals with that concatenation property taken into account.

V. HOW GOVERNMENT PARTICIPATES

The Federal Register inquiry asks for an evaluation of current US federal agency involvement in standards within our domain.

We are pleased to report that practically all of our interactions with US federal government agencies over the course of our history have been positive, collaborative and amiable. As noted above, we have particularly been grateful for our long and happy cooperative relationship with NIST, and active and significantly contributing members over the years from many federal offices including DoD (and its DISA and service branches), Homeland Security, HHS, the VA, DOE, NASA/JPL, NSF, the IRS and NOAA.

We do have one cautionary note. The HITSP project, described above, ended after about five years of dedicated contributions from multiple experts and standards organizations, and with some agreed taxonomic specifications, but arguably with much of the original scope truncated, and no clear mandate of implementation for many data structure issues. Later reports suggest that policymakers simply may have decided not to make use of much of the material. There could be sound reasons; it is mentioned here not to examine that specific outcome's merits, but only to give rise to a general caution.

Like any consultation process, a consensus standards project initiated by a public agency requires participants to invest substantial time. If the agency eventually walks away from it, that investment may appear in a negative light retroactively. So, when agencies are committed to a large and resource-intensive cooperative industry project, the results it produces should be assessed in a clear way, used where feasible, and not lightly derailed or routed-around by nontransparent considerations. To ensure this, a project's goals should be clear and objective enough both to assess success, and to permit clear communication regarding any failures. We certainly anticipate and hope to see concrete implementations and directions flow from the completion of the SGIP program, now in approximately its 18th month.

VI. RESOURCE ADEQUACY

We are pleased with and grateful for the membership and event support we receive from US federal agencies who elect to initiate or participate in our relevant projects, and grateful for NIST's role as a valuable center of expertise.

Building on our experience with the last few major e-government initiatives noted above, there are a few areas where we would like to direct the panel's attention for future investment and policy choices.

First, the basic model of the SGIP project seems to us to have leveraged a finite federal spend, successfully, to obtain a high volume of volunteered effort from market participants. This may be a good roadmap for future successes in other domains.

This is not to say that it's perfect. To some degree, any project with substantial economic impact bears a risk of skewed representation: stakeholders with less financial means or interests than the largest players might find it difficult to keep up with sustained demanded commitments of meetings and manhours. In a number of the e-government programs in which OASIS has been involved, in the US and elsewhere, we have ourselves felt that burden, as a nonprofit not seeking any commercial market advantage from the project's outcomes. We wonder if some other start-ups, SMEs, non-profits, end-user advocates, and the like may also find it daunting, or inaccessible. Agencies planning such programs in the future may wish to consider, depending on the topic and the relevant stakeholders, designing for policy accessibility. Perhaps (even if over-simplistically), $1 for SME subsidized access or relevant membership cost should be put aside, for every $20 or $40 spent on industry-facing contractors administrating a program. Another strategy is to permit and emphasize remote, asynchronous collaboration -- as we do in our own OASIS working committees, and as the SGIP has attempted to model -- so that travel budgets and employee count are not the dominant determinants of outcomes. Ombudsman models also may be worth considering in some cases.

Finally, we wish to reinforce our earlier point about the centrality of interoperability and conformance, by urging agencies to put their money where their mouth is on this function. NIST has long been a genial host for some concentrations of industries wishing to conduct interoperability workshops. However, in our field, some formerly well-ordered markets are diffusing into much larger networks (by number) of individually-smaller potential trading or data partners. Where we may have been summoning a GM, Ford and Chrysler into a room 40 years ago, to address a given supply chain methodology, now we are trying to facilitate open standardized marketplaces, perhaps across thousands of spontaneous remote nodes. We respectfully request NIST and sponsoring agencies to consider how different kinds of support might be offered, modeled and facilitated, via testbeds, asynchronous events, self-tests and other delivery methods, for this newer kind of constituency; and how the federal government can assist and promote conformance and interoperability in that updated, highly-distributed context.

Thank you again for the opportunity to provide our comments.

Respectfully submitted,

James Bryce Clark
Laurent Liscia

FOOTNOTES

[1] Cybersecurity and access control. *http://www.oasis-open.org/committees/tc_cat.php?cat=security ; http://www.oasis-open.org/committees/tc_cat.php?cat=privid*

[2] Office documents and smart documents. *http://www.oasis-open.org/committees/tc_cat.php?cat=contech ; http://www.oasis-open.org/committees/quomos*

[3] Electronic commerce including SOA and web services. *http://www.oasis-open.org/committees/tc_cat.php?cat=ws ; http://www.oasis-open.org/committees/tc_cat.php?cat=soa*

[4] E-procurement. *http://www.oasis-open.org/committees/ubl ; http://www.oasis-open.org/committees/bdx*

[5] CAP for emergency first-responder notifications. *http://www.oasis-open.org/committees/emergency*

[6] LegalXML for electronic court filing data. *http://www.oasis-open.org/committees/legalxml-courtfiling*

[7] E-government frameworks. *http://www.oasis-open.org/committees/tgf ; http://www.oasis-egov.org/*

[8] OASIS experts and staff in NIST SGIP PAPs. *http://www.oasis-open.org/committees/tc_cat.php?cat=smartgrid ; http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP03PriceProduct ; http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP04Schedules ; http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/PAP09DRDER*

[9] Standards (ebXML) in UK NHS health records. *http://www.ebxml.org/case_studies/NHS-ebMSG-casestudy-041206.pdf*

[10] Standards (XSPA) in US Army & VA health records. http://www.oasis-open.org/news/oasis-news-2010-03-02.php ; http://www.oasis-open.org/committees/xspa

[11] Standards (DSS, KMIP) with extended functionality for PKI. http://www.oasis-open.org/committees/dss-x ; http://www.oasis-open.org/committees/kmip

[12] Standards (e.g., SAML, XRI, XACML) used in NSTIC trust frameworks. http://www.oasis-open.org/committees/security ; http://www.oasis-open.org/committees/xri ; http://www.oasis-open.org/committees/xacml

[13] OASIS cloud computing standards activity. http://www.oasis-open.org/committees/id-cloud

[14] Examples, NTTAA assessment activity in SGIP. http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/PAP10EnergyUsagetoEMS/PAP10_report_to_SGIP_GB_15Jun2010.pdf ; http://www.nist.gov/smartgrid/upload/FERCtech_conference_013111-7.pdf

[15] European assessments of changing roles of consortia and *de jure* bodies. http://ec.europa.eu/isa/strategy/index_en.htm

[16] Openness criteria: comments on comparative definitions. http://www.talkstandards.com/european-codes-and-guidelines-for-standards-processes-in-a-bilateral-and-international-context/

[17] OASIS/NIST activities on standards about conformance. http://www.oasis-open.org/committees/ioc ; http://www.oasis-open.org/committees/tc_cat.php?cat=conform

[18] MoU on e-Business with ISO, ITU, IEC etc. http://www.itu.int/ITU-T/e-business/mou/index.html

[19] EIF v2, royalties in government standards use. http://ec.europa.eu/isa/strategy/index_en.htm

[20] Open source and licensing issues discussed. http://ec.europa.eu/enterprise/sectors/ict/standards/extended/ict-ipr-conference_en.htm ; http://www.pcworld.com/businesscenter/article/151519/european_public_sector_opensource_guidelines_spark_debate.html

[21] Written IPR commitments up front. http://www.oasis-open.org/who/intellectualproperty.php#types_obligations ; http://www.oasis-open.org/join/membership-agreement.pdf