IBM Response to Notice Of Inquiry (NOI) Regarding Governance for the National Strategy for Trusted Identities in Cyberspace (NSTIC)

1 Introduction

This document provides IBM's response to the Notice of Inquiry (NOI) from NIST regarding a governance structure for a steering committee for the Identity Ecosystem Framework. The framework is described by the NSTIC strategy is "the overarching set of interoperability standards, risk models, privacy and liability policies, requirements, and accountability mechanisms that structure the Identity Ecosystem".

IBM is pleased to be active in numerous industry-led, collaborative, open and transparent, standard-setting processes where governments can and do participate. Our response addresses several key, high-level issues that can help NIST, especially models and lessons learned for effective industry-government collaboration in the governance of technical standards and issues.

Specifically, IBM works with industry partners, academics, individual entrepreneurs and governments to develop open standards and conduct interoperability testing. For decades, we have participated in hundreds of industry-led standards bodies and working groups that interface with government, from the Automotive Industry Action Group (AIAG) and Association for Cooperative Operations and Research and Development (ACORD) to the Organization for the Advancement of Structured Information Standards (OASIS), the Open Group (TOG) and the World Wide Web Consortium (W3C). IBM has also helped to establish the Open SOA community, GridWise Alliance and the Health Level 7 (HL7) standard setting organization. In addition, IBM is a founding member of the Open Group Trusted Technology Forum (OTTF) which provides an open environment for vendor and government members to provide best practices to identify trusted providers and products in a global supply chain.

These organizations – and other formal, and less-formal, collaborations – produce open standards for software interoperability[1] that represent the best thinking of many creative minds and that are truly global in scope.

2 Recommendations

As technology is being increasingly infused into the systems and processes that make the world work, the "identity ecosystem" has become quite vast and diffuse. No single government agency or non-government enterprise is completely responsible for any single significant part of this ecosystem – rather, there are "systems of systems." Accordingly, standards as well as policies and guidance on privacy, liability, accountability and risk become paramount to ensure interoperability within and among existing and future ecosystems of ecosystems – especially as a way to guide decisions made today by governments that can affect the long-term global competitiveness of nations and industry, as well as the delivery of critical goods and services.

IBM urges the US government to learn from recent experiences in standard-setting activities and engage in truly open, consultative, transparent public-private collaborations with industry in this effort. Further, any action that the government takes should consider in advance how it will be viewed outside its borders, and have appropriate plans in place to ensure proper articulation of such actions.

Specifically, we recommend that the government:

2.1 Initiate public-private coordination and arbitration efforts to address particular industry gaps and government needs

To be successful, any standards-coordinating activity must have governance procedures that are clearly written, fair and fully-transparent. Voting, governance, membership, intellectual property (IP) rights, legal protection and development processes are all serious issues that need to be clearly stated from the onset and managed so that concerns are resolved in an appropriate, timely, and transparent way.

For example, in the smart grid space, NIST's establishment of the public-private consortium Smart Grid Interoperability Panel (SGIP) effectively addressed coordination

[1] IBM defines open standards as specifications that are well-documented through publication and have been accepted by either formal standards bodies or, increasingly, through a collaborative process involving interested players. Once published, these specifications are available for implementation without restriction. Moreover, interested parties can license or otherwise obtain authorization under a patent of standards body members that is needed to implement the standard or, at least, are made aware of such necessary patents. The acid test for an open standard is whether or not it actually permits substitutability and choice among independent, multi-vendor implementations on different technology platforms with acceptable levels of functionality. Diversity of competing applications that support the standard also indicates its openness and ensures choice for procurers and longevity for users. For example, open standards for software, like HTTP, HTML, TCP/IP, XML, ODF, SQL and UNIX, are evolved collaboratively in a well defined, open and transparent process under the auspices of standard bodies, generally not-for-profit organizations such as W3C, OASIS, TOG and IETF.

issues between standard-setting organizations in the area of smart grid interoperability standards. One of the key successful characteristics of the SGIP is its transparent private-sector governance via a cross-sector governing board and member representation, which helps to assure participation and acceptance ("buy-in") by companies. This type of public-private partnership enables NIST to participate in the process, providing input regarding national goals and requirements and assuring its mission of coordination can be fulfilled, while not being prescriptive.

Two other examples are worth considering when constructing the steering committee:

- The Year 2000 President's Council, which pulled government and industry together in guiding the nation with a significant technology challenge.
- The President's National Security Telecommunications Advisory Committee (NSTAC), to see how to is organized and how it interacts with all Federal agencies and commercial parties to achieve National goals.

2.2 Work within existing standard-setting communities whenever possible

As mentioned in the Smart Grid example above, establishing a government coordinator (such as George Arnold, as National Coordinator for Smart Grid Interoperability), is a key step by government to foster involvement in the standards process -- not by developing the details, but by identifying direction and usable standards/architectures where cross-sector standards solutions are required and acceleration is important. The government should not, on the other hand, create ad-hoc standards groups, which tend to halt activity before standards can be inculcated into organizations.

Most importantly, standards should be vetted through existing structures as much as possible. IBM sees no need in this space for additional standards structures.

2.3 Serve as equal and vendor-neutral participants and ensure consensus decision- making

The government has facilitated valuable technical collaboration and expertise where needed without the encumbrances that come with garnering vendor supplied talent. Government participation can bring technical expertise that is not attached to any particular vendor, platform, approach or technology. For example, in Integrating the Healthcare Enterprise (IHE), NIST involvement has helped to avoid and resolve conflict and improve the standard. However, in some security-related standards activities, the government's role has been less collaborative and less neutral. Government participation should count as one vote among contributors -- an environment of equals will promote acceptance of true standardization.

2.4 Consider how size and structure of the committee impact success

The steering Committee should consist of less than 25 members and preferably less than a dozen. Larger groups tend to have challenges with real dialogue and decision-making. There should be subcommittees groups for each of the major private sectors, plus one for civil government and one for the defense and intelligence community. The subcommittee

ensures timeliness of work and that relevant expertise is brought to the steering committee. The steering committee should include the chair of each of the subordinate subcommittees (two government optional; cultural/political decision), plus a few significant authorities from the industry, security, and privacy domains.

Part of the challenge of the NSTIC will be to get a critical mass of representatives from each of the major stakeholder groups. Identity providers, relying parties, technology providers, and public sector entities will all need representation.

2.5 Ensure governance models that are open, transparent and fair

It is critical to have written governance and processes and to take voting, governance, membership and process seriously, so that questions are resolved in an appropriate, timely and transparent way. Models for good governance can be found within existing standards and open source communities, including numerous efforts in which NIST participates. Furthermore, participation within federally-funded standards selecting entities should be open and transparent.

Specifically, the government will have to define a legal scope and authority of the steering committee. IBM suggests that the role be advisory, with government establishing guidelines and mitigating risks. The steering committee should have a written scope of work that includes broad national policy recommendations, a general implementation strategy, support, and implementation monitoring.

Sector-specific policy, strategy, implementation and monitoring that supports the broad national direction should be the sector subcommittee responsibility, and explained as so in appropriate documentation.

Most importantly, having a disinterested party maintain and enforce the governance structure of the steering and other committees ensures that the stakeholders are all represented fairly. As an example, the Open Group[2] has a long track record of successful development and maintenance of open standards. They maintain standards that have had representation from the public sector, vendors, and many industries.

3 Industry Examples

IBM has shared below some examples of similar standards initiatives.

3.1 Telecom

One group of standards to consider is the cellular communications standards. Every modern country has an infrastructure for wireless communications. This includes the local infrastructure as well as the ability to connect to other countries. There are legal, privacy, technical, and regulatory constraints that must kept in mind. As the technology is evolving at a very fast pace, the relevant standards must be kept up-to-date.

---

[2] The Open Group publishes their process on their web site http://www.opengroup.org/standardsprocess/main.html and their standards development process can be found here: http://www.opengroup.org/standardsprocess/standards-dev.html.

3.2 Smart Grid

In fulfilling its mission to coordinate the development of smart grid interoperability standards, NIST has helped establish the Smart Grid Interoperability Panel (SGIP), a significant public-private partnership that currently has over 600 member organizations and almost 2000 participating individuals. NIST defined 22 stakeholder categories within the structure of the SGIP, and established a governing board with representatives for each of those stakeholder categories. In addition, to assure that an organization of this complexity could ramp up and become effective in short order, NIST contracted an administrator to provide logistical and administrative oversight.

There are several key characteristics that NIST has addressed in forming the SGIP, which represents a model that should be repeatable for other domains of public-private partnership standards collaboration:

- The involvement of a broad community of stake-holders in the governance of the activity to assure participation in the process and acceptance of the results.
- The need for a transparent and inclusive process.
- The need for a living process that continues to improve.

One of the primary benefits of the SGIP is that it is not affiliated with any single organization or stakeholder community – it provides a venue that can be used to address technical and non-technical collaboration and harmonization issues across multiple Standard Setting Organization (SSOs). It can also quickly define requirements and even create initial draft documents that can help speed initiation and development of new standards where needed. Finally, by creating certain permanent committees and working groups within the SGIP (e.g., the Architecture Committee and the Cyber-Security Working Group to name two), and by defining a process life-cycle that includes these permanent groups, there is a level of formal review and feedback in the internal SGIP processes that helps assure technical consistency and quality.

Much of what has been created in the SGIP's process life-cycles, and in its general structure, is easily applied to other areas of standardization. For example, the Priority Action Plan process has been effective in several instances in rapidly addressing tactical issues of harmonization or coordination across multiple SSOs. Also, the concept of a Catalog of Standards, which is still under development, is likely to be another effective mechanism that can be carried to other domains.

The SGIP is still rapidly evolving and maturing. However, it has already had a positive impact in the smart grid interoperability standards space. The investment by NIST in creating and supporting the SGIP has been valuable. It is important to identify a sustainable model to ensure the SGIP continues to be effective, a lesson that applies to NSTIC as well. Over time this may need to evolve into a shared public-private investment, but it will probably always benefit from having some level of investment from the government through NIST.

3.3 Healthcare

As a federally sponsored organization, Healthcare Information Technology Standards (HITSP) was very effective at getting communities of interest together to look at the challenges of healthcare use cases and build implementation guides to enable the use case of interest. This community building capability of HITSP was enabled by an open, transparent, well documented process. We support the HITSP model of governance as an effective method for building communities of interest and enabling standards selection for use cases of interest.

Where HITSP became less effective was in two aspects: a) excessive, overly complicated documentation b) too much breadth in too short a time. Unfortunately, these problems resulted in a lot of documentation, only a small portion of which was truly useful. We encourage the creation of focused groups that allow enough time to understand the use case at significant depth and creation of a standards based solution with a full understanding of the tradeoffs and values.

3.4 Technology Supply Chain

IBM was instrumental in creating the Trusted Technology Forum (TTF) under the aegis of the Open Group. Below is a quotation from the original press release[3]:

The TTF is a proactive response to the changing cybersecurity threat landscape and will address the mitigation of risks potentially introduced by vulnerable supply and development processes. Founding members are Boeing, Carnegie Mellon SEI, CA Technologies, Cisco, HP, IBM, Kingdee, Microsoft, MITRE, NASA, Oracle, and U.S. Department of Defense (OUSD(AT&L)/DDR&E); the forum will operate under the stewardship of The Open Group, an international vendor- and technology-neutral standards consortium.

Initially, the TTF will release a framework that for the first time unifies in a systematic way the industry best practices that contribute to the secure and trusted development, manufacture, delivery and ongoing operation of commercial software and hardware products. The TTF's long-term objective is to develop a globally-recognized program based on open, international standards. Such a program will identify trusted technology providers and products throughout the global supply chain, enabling suppliers to innovate and build technology products with integrity and customers to buy with confidence.

4 Contact

IBM would be glad to work with the government other stakeholders in creating the governance structure for the Identity Ecosystem. IBM will send representation to the upcoming NSTIC working groups.

[3] http://www.opengroup.org/ottf/OTTF_press_release_final.pdf

For any questions regarding this document, please use the contact information below:

Patrick M. Ryan
pmryan@us.ibm.com
301-803-2092
Technical Manager and Executive Architect
IBM Federal Software Group