NSTIC Notice of Inquiry - Microsoft Response (July 2011)

At its core, this response to the NSTIC NOI by Microsoft Corporation strives to strike the right balance in the recommended relationship between government and private-sector players in establishing and operating a steering group for the "Identity Ecosystem." We generally call for minimal government involvement. At the same time, we recognize that government is a key actor as it wears multiple hats – including its roles as identity provider, relying party, referee, standards setter, procurer, guardian of the public interest, actor on the international stage, etc.

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?

The steering group should be a private-sector led, self-regulatory organization with limited government involvement. The structure must include a means by which the various stakeholders in the Identity Ecosystem have a voice in its governance. A crucial consideration here is the importance of individuals, who are often left out of industry and policymaker discussions and who in recent years have borne an increasing share of risk.

NSTIC recognizes that citizens are at the center of the Identity Ecosystem. President Obama's cover letter refers to problems of online security and explains, "Giving consumers choices for solving these kinds of problems is at the heart of this new strategy." NSTIC frames the issue in a similar way: "By addressing threats in this environment, we will help individuals protect themselves in cyberspace and enable both the private sector and government to offer more services online." In this same spirit and with high hopes for the long term success of a private-sector led initiative, Microsoft believes it is critically important that the highest level of governance by the steering group belong to the general public. The Identity Ecosystem will be a public good shared by society. Its health depends on public acceptance of and confidence in its basic workings. Consistent with American values, we should aim for "governance of the people, by the people, and for the people" in the Identity Ecosystem.

This objective should inform the separate, ensuing questions of how representatives should be selected and how decisions should be made within the assembly of these representatives once they are chosen. These questions are rightly being studied through the NSTIC NOI process.

As an information technology company, we recognize that industry players are the participants that put together the components of the Identity Ecosystem and make it run. We believe that industry perspectives will necessarily need effective representation, particularly on technical matters where industry is often most knowledgeable. Average citizens may lack the expertise to make good governance decisions. At the same time, we have a direct interest in the success of the Identity Ecosystem, and we believe such success is most likely where the society in which industry players operate is informed and engaged. Public confidence in the Identity

Ecosystem is a prerequisite for businesses to sell their products and services. This confidence depends on public understanding and involvement.

For these reasons, we suggest a two-tiered structure for the steering group, with an upper chamber "Public Assembly" having responsibilities of a general nature, and a lower chamber "Trust Framework Provider (TFP) Council" of industry participants being tasked with specialized matters.

One way in which the Public Assembly represents the public interest should be to hold TFPs to the commitments of the "Principles of Openness" (see the attached Annex) in the trust frameworks they operate. These Principles of Openness call for lawfulness, open reporting and publication, ombudsmen, anti-circumvention and open disclosure, non-discrimination, interoperability, open versioning, participant involvement, data protection, accountability, auditability, and redress. The Public Assembly could also invite external experts to advise and make recommendations to them. The TFP Council, meanwhile, could represent other Identity Ecosystem players (e.g., identity providers, identity proofers, technology providers, and relying parties). This lower chamber would deal with more specific legal, technical, and operational matters of trust frameworks. Possibly in their activities outside the steering group, TFPs could create and oversee their own trustmarks to meet the needs of their various trust framework communities, but they would all be accountable to the Public Assembly in the sense that they would need to follow the Principles of Openness.

With the protections of the Principles of Openness as a foundation, the Identity Ecosystem should be market driven in other respects. In fact, the profit motive would be important to give businesses a reason to participate in the Identity Ecosystem. Looking at it from another angle, one of the greatest threats to NSTIC would be for it to turn out to be an interesting intellectual exercise but with no real attractiveness to business. To avoid irrelevance, NSTIC needs the private-sector led steering group to find and promulgate the Identity Ecosystem's value proposition.

In this vein, we recommend that the TFP Council concentrate on fostering viable business models. Primary scenarios include C2B, C2C, and C2G transactions as suggested in the NSTIC document. Other scenarios, such as B2B, B2G, and G2G transactions, can also drive compelling economic benefit and would likely garner attention from the Council. TFPs serve in the middle of trust frameworks to bridge the demands of policymakers, identity providers, attribute providers, relying parties, and other participants in the Identity Ecosystem. As such, they are envisioned as the orchestrators in the TFP Council. At the same time, it could make sense to have sub-committees dealing with interests of parties in the various other roles. (Organizations playing multiple roles could participate in all the relevant sub-committees.) As a whole, the TFP Council could work to ensure that neither the regulatory environment nor the technical architecture created too heavy a drag on the value proposition for business participants in the Identity Ecosystem.

In terms of regular government interactions with the steering group, in the upper chamber, the government has a role to play that it should not relinquish: that is, protecting the interests of people who otherwise would not be properly represented. Here the government could appoint someone to serve in an ombudsman capacity. In the lower chamber, government has an important role to play as a market maker, choosing to steer dynamics in the right direction through its own consumption and procurement rather than through regulation. Meanwhile, TFP

Council representatives could engage in government outreach to encourage legislation that would cap liability so long as certain requirements were followed. Such predictability would go far in fostering an Identity Ecosystem.

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?

By way of example of a self-regulatory organization, the UK government handed off regulation of their identity ecosystem to a non-profit membership organization as a result of feedback from the private sector particularly banks. This feedback was provided in private rather than made public. The UK body was formed as a private organization and runs a voluntary accreditation scheme that performs the functions of rulemaking, assessment, and award/revocation of approval marks.

The UK body was chartered by legislation that included a five-year milestone for review. The quinquennial review found the organization was working successfully so the government powers to regulate the identity ecosystem were allowed to lapse (i.e. the government handed off its regulatory powers to this body). Hence, there is no government involvement in the identity ecosystem at present. In practice, some fundamental issues have held back the viability of an identity ecosystem and as a result the participation in the UK body has declined. On the demand side very few commercial service providers emerged that wanted to consume identities, and even government agencies proved reluctant to accept the financial, commercial and political risks of depending on new types of contracts with private sector identity providers. On the supply side the burden and costs on would-be identity providers of proving compliance to win and sustain a trustmark was a significant obstacle. More recently the UK government has adopted a very similar strategy to NSTIC in seeking to enable and use private sector Identity providers and to provide support for user control and privacy. This time a lead department has the mandate to reform the process for how citizens claim welfare benefits and to shift to a digital delivery model so there is both the will and the funding from government to sustain an identity ecosystem, and also a more compelling reason for citizens to obtain a digital identity.

More recently the UK government has adopted a very similar strategy to NSTIC in seeking to enable and use private sector Identity providers and to provide support for user control and privacy. This time a lead department has the mandate to reform the process for how citizens claim welfare benefits, and in doing so to shift to a digital model. Thus, there is the will and funding from government to sustain an identity ecosystem and a more compelling reason for citizens to obtain a digital identity.

The UK accreditation body adopted existing certification schemes like ISO 27000, which it then adapted with new rules called Approval profiles. The UK body is/was governed by a steering group with members paying an annual membership fee of about $20k, and the 3 main functions are managed by committees drawn from the membership. The assessments of Identity providers are performed by external assessors like KPMG and these assessors must be accredited bodies. The UK has a body called UKAS that can accredit any consulting or quality assurance agency as being capable of conducting assessments.

The Approval profiles act as best practice guidelines and when used in an assessment they assure that the service provider is properly established and resourced and that the user receives the service expected. The idea is that users and relying parties themselves can then make

informed decisions as to whether the service is fit-for-purpose. It is possible that Approval profiles could be defined and applied to relying parties where a service provider wants to offer data protection assurances to individuals as proposed in the "Levels of Protection" paper that Microsoft submitted to the 2010 Privacy Standards Conference of the International Organization for Standardization (ISO).[1]

The Approval profiles do not test that the service is fit for any particular purpose, or for interoperability. It is impractical to mix interoperability goals with service provider assurance goals in one body, as these functions should be separated out. A service provider will likely want to be free to determine the interoperability standards that work for them and their users and relying parties (e.g. maybe some will like OAuth and others will like SAML).

In practice, the UK body did not have a smooth experience as there was much unease over leadership of the body, membership fees, and approaches to best to stimulate the market. In addition, it was difficult for technology providers to justify being part of a body comprised of service providers in the business of identity.

With respect to the U.S. case, however, it should be noted that (a) the political climate is different in that people generally do not hope for government intervention, and (b) the UK government's involvement did not solve the fundamental need for a business model.

* * *

Another example is the Multi-stakeholder Advisory Group (MAG) to the Internet Governance Forum under the United Nations, which operates at a similarly large scale (and arguably goes beyond it given the wider scope and geographical coverage). Fairly large in size (56 members), the MAG successfully factors in perspectives of different governments and industry sectors. The size of the group is not an obstacle to its functioning because it is consultative in nature and is not endowed with decision-making authority. Still, the size requires additional administrative efforts by a smaller number of people, and therefore a secretariat helps with organization. Challenges include:

- Legitimacy as the group was selected in a process that involved consultations by an appointed leader but no real accountability to the public;
- Freshness and heterogeneity as the same faces appear year to year and have much overlap with other bodies (which makes sense for feeding in inputs and promoting coherence, but which can at the same time result in a sort of incestuous-ness);
- Insularity as most publics around the world have no knowledge of the activities of the group and the implications of their recommendations and, as such, are not feeding their opinions into the discussion.

1.3. Are there functions of the steering group listed in this Notice [see pp. 4 and 5] that should not be part of the steering group's activities? Please explain why they are not essential components of Identity Ecosystem Governance.

The steering group should not delve into standards setting or recommend or prefer a particular standard. (This includes NIST, meaning that NIST should not be charged with doing NSTIC

[1] Mary Rundle and Sue Glueck, "Levels of Protection" *proposal submitted to the ISO Privacy Standards Conference* (October 8 and 9, 2010) (summary and link to free download at: http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/lop.aspx).

standards.) If the steering group finds that there is a need for additional standards, it could highlight that need to the appropriate standards-setting organizations (e.g., IETF, IEEE, ITU, ISO, and OASIS) and rely on them develop the standards. The steering group should also take cognizance of existing standards work and help promulgate the adoption of these standards, but in doing so it must be completely standard agnostic.

Assuming this Identity Ecosystem stands a good chance of taking off, it would be imprudent to treat it as a narrow realm since in fact most future economic and online activity will have a tie to this underlying structure. Given the substratum quality of the Identity Ecosystem, its governance must be understood as relating very closely to governance of the information society itself. For the sake of representation and jurisdictional clarity, it will be important that at least two issues are addressed: 1) the scope of the steering group's governance authority, relative to national jurisdiction of the United States; 2) establishing parameters around steering group governance authority to ensure both that the steering group decisions respect democratic values and goals, and the constitutionality of any decisions by government or a private-sector entity acting in a governmental capacity. Digital identities will be a fundamental prerequisite for anyone wishing to participate in the information society – not just as a consumer, but also, and more deeply, as a citizen. These types of issues are not simple matters of authentication and authorization; rather, they concern the very relationship between the individual and the state, and for Americans they must be determined with reference to the U.S. Constitution. Such questions should not be left to a steering group to decide absent some parameters that ensure decisions respect democratic values and law.

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?

[The Notice of Inquiry (Notice) indicates that the Strategy itself "calls for a 'steering group' to ***administer the process for policy and standards development for the Identity Ecosystem Framework*** *in accordance with the Strategy's Guiding Principles (p. 4). In addition, the Notice says this "persistent and sustainable private sector-led group will* ***maintain the rules of participating*** *in the Identity Ecosystem,* ***develop and establish accountability measures*** *to promote broad adherence to these rules, and* ***foster the evolution of the Identity Ecosystem to match the evolution of cyberspace itself****" (p.4).The Notice also says "the steering group will* ***administer the process for the adoption of policy and technical standards****,* ***set milestones and measure progress*** *against them, and* ***ensure that accreditation authorities validate participants' adherence*** *to the requirements of the Identity Ecosystem Framework" (p. 5). (Emphasis added.)]*

NSTIC suggests that the steering group might oversee a trustmark that signals the package of rights and responsibilities among participants in trust frameworks bearing that mark. It is not feasible to advocate the creation and use of a trustmark until the proposed criteria are well understood. Still, lessons may be drawn from existing approaches – in particular regarding the degree of specificity desired if designed for general usage. While groups like TSCP and InCommon may each use trustmarks, what their respective trustmarks represent differs considerably – after all, they have the luxury of tailoring the trustmarks to the particular constituents whom they serve. The take-away is that if there is to be a trustmark meant for broad usage, it will need to entail terms that are general purpose to meet the needs of the many different groups that the Identity Ecosystem is meant to serve.

Criteria such as those found in the "Principles of Openness" could serve as common requirements on which a trustmark for general usage is based. As noted, these Principles of Openness call for lawfulness, open reporting and publication, ombudsmen, anti-circumvention and open disclosure, non-discrimination, interoperability, open versioning, participant involvement, data protection, accountability, auditability, and redress. (The Principles of Openness were developed in consultation with a wide range of stakeholders. Please see the Annex.)

In any case it will be important that any system of trustmarks not create a false sense of trustworthiness.

The Public Assembly should be required – and equipped – to keep the public informed in a meaningful way.

The TFP Council may wish to set up a separate entity to handle incubation and sales/marketing.

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

The steering group must factor in the interests of all stakeholders, not just one set such as relying parties. To prevent capture and ensure that one group is not over or under represented, the two-tiered structure noted above is proposed so that interests of individuals as well as other participants in trust frameworks will be given due attention.

There are significant differences between regulated versus unregulated sectors. Fortunately, TFPs will be in a position to hear the needs of these stakeholders as TFPs implement trust frameworks that bring together diverse identity providers, attribute providers, and relying parties, while leveraging the insights of assessors and auditors with specialized expertise.

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?

TFPs will play a key role in fulfilling this responsibility. Because they will be responsible for ensuring compliance with law in the conduct of their trust frameworks, and because they deal with sectors that are subject to regulation, these TFPs are well positioned to understand this complexity and identify potential conflicts. By working with individual representatives and service providers, TFPs can call for government help to mitigate the risks when necessary.

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" regulation from regulated participants in the Identity Ecosystem? (Footnote off "pull through": NSTIC solutions will ideally be used across all industries, including both regulated and unregulated industries. "Pull through" refers to the concept that when implementing an NSTIC solution that touches some regulated industries, individuals or firms implementing those solutions would then find that they are subject to the specific regulations for those industries. This could create a confusing policy and legal landscape for a company looking to serve as an identity provider to all sectors.)

There are many historical examples of "pull through" regulation causing unintended and negative outcomes. This is even true across subsectors of government. For instance, in the state of Washington a green card held by a permanent resident is inadmissible as evidence of identity to buy a beer in a bar. This is despite permanent residents' being subject to strong enrolment

processes and the green cards' providing a strong credential using the latest biometric techniques. The root problem to address is instigating a policy for mutual recognition of equivalent identities and a mandatory governance policy that enables the relevant stakeholders to introduce changes.

As a general matter, each of the Guiding Principles is sufficiently generic so that collectively they serve as an overlay over sector-specific regulatory requirements that may apply in a given vertical sector – neither conflicting with such requirements nor attempting to substitute for them.

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

The most important characteristics for steering group members should be constitutional awareness, a commitment to fairness and justice, a commitment to transparency, innovativeness, insightfulness, pragmatism (in particular, the ability to recognize the realities of business and value propositions), multidisciplinary expertise, the ability to catalyze business models, the ability to drive toward goals and deliverables (which should be clearly defined), and an international perspective.

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?

Apart from providing the parameters of the steering group and directing its creation, there should be minimal government involvement. To the extent that government involvement is necessary, a pre-existing body such as the Federal Trade Commission (FTC) could exercise some degree of oversight by participating in the self-regulatory organization.

As noted previously, the FTC could also play an ombudsman role.

Once the steering group is self-sustaining, the government could still participate in the various stakeholder roles of government (e.g., as relying party, identity proofer, etc.), bearing in mind the presumably limited number of seats and the need to act through TFPs in the lower body.

2. Steering Group Initiation

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?

While a FACA body can provide certain benefits, it typically requires a considerable amount of time to stand them up and there is also a fairly regimented process governing how they operate. Standing up a non-profit entity with appropriate legal protections results in a more flexible structure that can make and execute decisions in a more efficient manner.

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?

Government involvement in the initiation of the steering group should be geared toward achieving appropriate representation of the public interest by setting parameters for the creation and structure of the steering group. To clarify its role, the government should emphasize that its involvement in day-to-day steering group operations will be as minimal as possible while still reflecting the government's interests as a stakeholder (given the various hats that government wears, e.g., as an identity proofer, relying party, etc.).

The private sector should coordinate to put a non-governmental entity in place to help with the initial meeting. The government might usefully suggest the contours and timetables based on findings of the NSTIC workshops and NOI.

The government should not be involved in selecting representatives in this effort, however, or in managing the work of the steering group. The steering group should be formed in a "bottoms-up" manner that naturally attracts and aggregates parties with different interests.

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

The most effective way to get the ecosystem going would be to find a proper business model.

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?

Special attention to a competitive market structure, civil liberties, and industry standards will help shore up the Guiding Principles of interoperability, security, privacy and ease of use.

The Guiding Principle most at risk in steering group establishment would seem to be voluntariness. If there is a scramble to get a seat at the table, the scramble will be due to a fear of missing out. While NSTIC crafters might be tempted to rejoice in the initiative's popularity, people's fears of being left out would cut against the sense that there were no repercussions for not participating. This pressure to participate might negate messaging around the voluntariness.

Government agencies whose mandates most closely relate to the Guiding Principles could add value to the steering group by participating in the self-regulatory organization. For example, to ensure privacy and the voluntary nature of participation in the Identity Ecosystem, the Federal Trade Commission (FTC) could oversee aspects, or, for interoperability, the National Institute for Standards and Technology (NIST) could be involved.

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.

Government involvement in the initiation of the steering group should be focused on ensuring fair representation and convening/moderating the initial meetings.

Please see the UK example in the response to question 1.2 for a case of government deciding to reduce involvement.

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?

The steering group's composition should reflect the range of interested stakeholders. To effectively implement a private-sector led effort, it will be important for the public to have confidence that their interests are sufficiently advocated and that the Identity Ecosystem is accountable to the public. As noted in the response to Question 1.1, we recommend a two-tiered structure with an upper Public Assembly that oversees TFP observance of the Principles of Openness, plus a lower TFP Council to ensure that the Identity Ecosystem offers compelling business value.

The best way to engage TFPs will be to let them recognize their interest in the creation of a self-regulatory organization. TFPs can then engage identity providers, relying parties, and other participants.

The more challenging issue is how to engage individuals, as it will be important for Public Assembly representatives to be seen by the public as representing the public interest. By no means should representation in the Public Assembly be based on pre-existing participation levels in trust frameworks since such an arrangement would bias the system in favor of early adopters – something that may be fine as a business incentive, but poor for the sake of representing the public. Letting leadership go to the most active individuals on the basis of their awareness of the initiation process would presumably be weak in terms of legitimacy.

Although not expedient, elections for seats based on population and geography may be perceived as most legitimate since the Identity Ecosystem is something that will affect everyone. While rotating representation by geography may seem archaic for the digital world, such a basis could be helpful in transitioning people into this new setting. To prepare for the longer term, one of the tasks of a subcommittee within the steering group or the FTC could be to classify the (digital) user community by demographics to ensure fair representation of the user base and public generally.

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

Both the upper and lower chambers of the steering group (i.e. the Public Assembly and the TFP Council) should have communication mechanisms for receiving input from interested entities. An ombudsman in the Public Assembly would have the specific job of looking after the interests of under-represented people. (The government would still have this responsibility generally in its activities.)

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?

To guard against disproportionate influence, special attention must be given to ensure separation of functions and a competitive market structure – with focus in particular on the degree of concentration, the extent of product differentiation, and conditions of entry. For competitive market structure, the FTC could be asked to adapt traditional anti-price-fixing safeguards to areas in which industry players might try to collude. To guard against the thwarting of civil liberties, it will be important to involve experts who have combined

knowledge of both technology and constitutional law. Employing a transparent process is also critical to help ensure accountability in achieving a balanced representation.

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?

The fee structure and other such matters should be determined by the parties forming the self-regulatory organization. One caveat for parties participating in its formation is to prevent the fee structure from allowing the bigger players to force out the smaller players with large fees. While fees will be required to run the steering group, it is important to represent the public's interest, regardless of the ability to contribute financially. We suggest that for every paying member there be a community member, and also that there be an executive committee that is voted into office.

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.

Transactions taking place within the Identity Ecosystem could have a nominal fee associated with them. (To determine citizenship for the purpose of this "tax" collection while at the same time following the privacy principle, systems could apply privacy enhancing technologies). The proceeds of these micropayments could fund governance.

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?

The upper Public Assembly (comprised of representatives of the class of individual users) as proposed here would have authority to oversee observance of the Principles of Openness. The TFP Council would act in a self-regulatory manner with respect to other issues relating to the specific legal, technical, and operational workings of trust frameworks.

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?

In the two-tiered arrangement, it is the Public Assembly that must entail broad representation. The Federal government should reach out to State, local, tribal, territorial, and foreign governments at the outset to ensure proper public representation in this upper chamber. TFPs can organize themselves and pull in other Identity Ecosystem participants for the lower chamber.

4. International

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

The steering group should involve experts with multidisciplinary backgrounds. Many TFP members will likely have this expertise. For example, many of them are abreast of standards relating to the Identity Ecosystem Framework and have gained an international perspective through their various experiences.

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

These questions should be left to the self-regulatory organization to address. The steering group may choose to coordinate with foreign self-regulatory organizations on the basis of liaison agreements. Nevertheless, the steering group should not have direct contacts with foreign governments and inter-governmental organizations as this foreign relations function more appropriately belongs to the Federal government.

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

These questions should be left to the self-regulatory organization with its two chambers to address.

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

These questions should be left to the self-regulatory organization with its two chambers to address. Still, standards setting activity for interoperability should be left to standards bodies.

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

The government should be involved only where required, for example, when governments are the members with voices in international organizations and the support of these organizations is needed, or when the Identity Ecosystem needs government participation to prevent the steering group from disrupting the Westphalian (nation-state) sovereignty of the international system.

ANNEX: Principles of Openness

SOURCE: "The Open Identity Trust Framework (OITF) Model" by Mary Rundle (managing editor and co-author), Eve Maler, Anthony Nadalin, Drummond Reed, and Don Thibeau.

All participants in an Open Identity Trust Framework must commit to abide by the Principles of Openness and to incorporate them into their agreements relating to the trust framework. These Principles are:

Lawfulness. OITF Providers are responsible for ensuring that the technical, operational, and legal requirements of the OITF are consistent with the laws of the jurisdiction(s) where parties use it to conduct exchanges involving identity information.

Open reporting and publication. OITF Providers must produce periodic reports on the operation and governance of the trust framework. They must ensure that a web site devoted to the OITF provides easy and timely access to (a) the periodic reports, (b) all agreements that constitute the legal structure of the trust framework, (c) all policies and procedures by which the OITF operates (including criteria and processes for certification), (d) a plain-language explanation of the trust framework's trust characteristics (for example, data protection strengths and weaknesses), and (e) records of dispute resolution activities and their results. However, publication is not required for assessment reports. OITF Providers must ensure that all parties to agreements under the OITF have visibility into who is participating in it and in what capacity.

Ombudsmen. OITF Providers must ask governments where they do business to designate independent ombudsmen whose role is to look after the interests of individual users under their respective jurisdictions, and they must ensure that the OITF is designed to allow these ombudsmen to do their job. If law requires the sharing of identity information (including biometric data, behavioral data, and social graphs) without the informed consent of the person in question, parties to the OITF who are ordered to share this information must involve the ombudsmen.

Anti-circumvention and open disclosure. OITF participants must not be party to any side agreements that compromise the integrity of commitments under the trust framework. If a participant is party to any agreements that might otherwise conflict with obligations under the trust framework, that party must disclose the existence and nature of these agreements to the affected party or parties at the earliest opportunity. OITF Providers and assessors must disclose all their agreements and the terms of those agreements.

Non-discrimination. Participants in the OITF must avoid discrimination. Participants must not engage in exclusive dealing arrangements relating to the trust framework.

Interoperability. Software and hardware specified in the technical requirements of an OITF must conform to defined standards that promote interoperability.

Open versioning. OITF Providers must spell out how new versions of the OITF will be decided, when they will be published, how participants will be transitioned to these new versions, and how the interests of participants in the OITF will be protected.

Participant involvement. OITF Providers must enable participants to share contact details so that they may convene virtually to discuss matters related to the trust framework.

Data Protection. Participants in OITFs will adhere to data protection practices at least as strong as those of the OECD's Privacy Guidelines (Part Two in its entirety, concerning collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability).

Accountability. OITF Providers must state on a publicly accessible web site how the OITF provides accountability to all participants, including the users whose identity information will be exchanged under it.

Auditability. OITF Providers must ensure that all parties to agreements under the trust framework, including themselves, agree to be subject to audit for conformance with these Principles of Openness.

Redress. OITF Providers must ensure that all agreements under the OITF afford the parties an effective right and mechanism to seek redress.