Transglobal Secure Collaboration Program (TSCP) response to the National Strategy for Trusted Identities in Cyberspace (NSTIC) Notice of Inquiry (NOI)

The Transglobal Secure Collaboration Program is pleased to submit comments in response to the Notice of Inquiry, 'Models for a Governance Structure for the National Strategy for Trusted Identities in Cyberspace (NSTIC), Docket No. 110524296-1289-02.

TSCP was founded in 2002 as concerns of data leakage, intellectual property protection, and export control compliance began to rise, TSCP established an industry approach to protecting sensitive information, based on interoperable trust mechanisms. TSCP members include major government departments and agencies as well as the largest defense and aerospace manufacturers and systems integrators around the world and Technology Vendors.

TSCP has four strategic goals:

1. Enable secure information sharing within and between industry and governments.
2. Enable collaboration compliant with export control and relevant policies and company Intellectual Property protection policies.
3. Define a set of interoperable specifications and solutions that enables re-use in a cost effective manner across multiple programs.
4. Make TSCP specifications and solutions a standard in the A&D community.

The first two goals require trusted identities.

At any given time there are hundreds of thousands of supplier companies working on government contracts, representing roughly 3 to 4 million individuals. The Aerospace and Defence (A&D) supply chain is able to leverage TSCP specifications, capabilities and business processes as they develop their solution roadmaps.

TSCP engages collectively with standards bodies and policy authorities ensuring continued alignment with TSCP specifications and policies.

TSCP achievements include:

- Framework for Secure Collaboration published in the public domain, providing members and partners with the technical architecture and business framework to operate secure electronic collaboration systems.
- Established a legal framework for the assertion of identities to facilitate the exchange of sensitive IP across organizations.

- Established the first Aerospace PKI Bridge, Certipath, cross-certified with the US Federal Bridge. Established a foundation for a multilateral trust network across the members and other stakeholders through the CertiPath PKI Bridge.
- Published the specification for PKI-enabled Secure E-mail (signed and encrypted email over the internet) including the How-To Guide to support for rapid adoption.
- Designed a digital certificate Lookup & Discovery system enabling automatic location and use of partner certificates for Secure E-mail and signature validation.

TSCP appreciates the opportunity to provide input on the NSTIC governance model and looks forward to future engagement.

Keith Ward

Keith Ward
TSCP Governance Board Vice Chair

TSCP Comments

Section 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?

TSCP believes that the Steering Group should be a formal governance body (adhering to the Strategy's four Guiding Principles); this is needed to drive industry adoption of higher identity assurance. The Steering Group should have a charter and terms of reference to ensure credibility and accountability.

The Steering Group / governance body should be supported by technical, policy, legal and operational committees / working groups. In addition there is a requirement for a communications outreach committee with responsibility for consensus building, stakeholder awareness and communicating decisions – eg endorsing standards to be adopted. This model is successfully implemented by TSCP.

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?

TSCP recommends that NSTIC looks at organizations such as the Internet Engineering Task Force (IETF), W3C and United Nations Centre for Trade Facilitation and Electronic Business, (UN/CEFACT), which facilitated the development of the United Nations / Electronic Data Interchange for Administration, Commerce and Transport (UN/EDIFACT) standards.

What makes them successful - UN/CEFACT - welcomes participation from United Nations Member States, intergovernmental agencies, sector and industry associations recognized by the United Nations Economic and Social Council (ECOSOC) as well as the private sector, from which much of UN/CEFACT's technical expertise comes.

Challenges - Trying to compete with other industry standards that are based on XML*.*

1.3. Are there functions of the Steering Group listed in this Notice that should not be part of the Steering Group's activities? Please explain why they are not essential components of Identity Ecosystem Governance.

NSTIC mentions '..develop and establish accountability measures'. This seems to suggest that the Federal Government is interested in holding private industry accountable for improving consumer security in the cyber world. It is unclear whether 'accountability' should be part of the Steering Group, when NSTIC are trying to foster adoption of an identity ecosystem that will mitigate cyber security risks.

The Steering Group rather than seeking to establish policies or interact directly with identity ecosystem providers should be responsible for defining an Identity Ecosystem

Framework / Principles within which policy authorities and service providers can operate.

The Steering Group should not focus on delivery of technical capabilities.

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 Steering Group should have functions that place emphasis on " fostering evolution of the Identity Ecosystem".

- In the financial industry, the US Federal Reserve has rules on 'minimum cash balance requirements' from each of the regulated financial institutions in order to manage the systemic risk of the overall financial system. Similarly, the Steering Group needs to define appropriate rules to manage systemic cyber security risks.
- Another way to foster adoption is leveraging the existing private industry governance mechanisms. An example might be defining how the private industry should implement 'security audit opinions' similar to 'financial audit opinion' in their annual company statements. This will enable existing governance regimes to address cyber security.

1.5. To what extent does the Steering Group need to support different sectors differently?

The Steering Group must communicate effectively to ensure public recognition of the differing needs of various industry verticals, ensuring that attention is not simply focused on one industry (e.g. financial services) at the expense of others which are equally important. For example, public calculations of cyber security risk are grounded in public experience – it may be easier for a citizen to understand the compromise of a bank account, rather than to understand the implications associated with the loss of privacy.

NSTIC should recognize the importance of addressing all identity assurance levels.

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?

The Steering Group should focus on 'Identity Ecosystem Framework / Principles rather than specific 'Policies'. The Steering Group should also identify the problems that are common across all industries and ensure it addresses those problems first.

Government is the potentially the biggest relying party for secure credentials. By accepting various equivalent regimes and not mandating a given technology, government can ensure that innovation is not stifled and create economies of scale.

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"1 regulation from regulated participants in the Identity Ecosystem?

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.

The Steering Group should not be seen as another regulator, nor should it interfere with existing regulations, rather it should enable private industry to take the lead in addressing the risks of the cyber world, where regulation is always struggling to adjust to rapidly changing conditions.

If NSTIC focuses on defining an Identity Ecosystem Framework / Principles rather than specific policies then there is no "pull through" effect. The regulated participants are enabled to express their requirements under the Identity Ecosystem Framework / Principles in the same manner as other participants in the Identity Ecosystem.

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

Of all the important areas of identity management in the cyber world, legal aspects are the least mature. This is the area where the Steering Group can help the most. By defining a clear legal framework for the Identity Ecosystem, the Steering Group can ensure that companies understand their responsibilities, liabilities and obligations. Lack of a common legal framework is driving each industry to define its own rules, which drives up the cost, and makes interoperability, in the broad sense, difficult or impossible to achieve. TSCP is working with the American Bar Association to define a legal framework.

The Steering Group should focus on identifying the Ecosystem Framework / Principles rather than defining or delivering technical capabilities.

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?

Government (Federal, State, Local and Tribal - combined) is the largest relying party. Use that effectively, but ensure innovation is not stifled due to overly complex rules or imprecisely stated standards. Without Government participation the credibility of an Identity Ecosystem Framework / Principles is lessened.

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?

'Start with the End in Mind' (S. Covey). If the end goal is that Private Industry should lead, make every effort to ensure this is planned for up front and that the end goal is considered when setting up the Steering Group.

In addition, adopt the quickest and easiest approach.

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?

Knowing that the biggest benefactor of this activity will be the Government (by virtue of the fact that they are the largest relying party), it is fair and equitable that the Steering Group should initially be funded by the Federal Government. This initial funding will increase its chances of success. The Steering Group can focus on the real issues to be solved if sustainability is guaranteed by the Federal Government.

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

'Lead by Example'. Government (all agencies) should be the first to adopt the Identity Ecosystem Framework / Principles in its role as the largest relying party. Adoption of the Identity Ecosystem Framework / Principles for Government contracts will ensure rapid take-up.

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?

TSCP believes that the following risks are inherent in starting any activity like this:

- Inequitable representation: For example, vendors will have clearer motivations and more experience in issues of identity management than consumers, and will consequently tend to exercise more influence.
- Conflicting priorities: Overemphasis on privacy requirements may undermine security requirements, or vice-versa.
- Private vs. Public sector differences: As an example, the private sector is profit driven, and the need to show relatively rapid returns on investment, while the public sector is not necessarily driven by the same pressures. These differences, if not acknowledged and accounted for, will undermine public-private collaboration.

- Risk Mitigation: Ensure that there is subcommittee of the Steering Group whose sole purpose is risk management.
- Role of Government: The Government should ensure that the Steering Group works to a charter which includes operating to the NSTIC guiding principles.

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.

An example of a working model is in the financial services industry (although the recent financial meltdown has led to some people questioning this model). FASB (private sector) and SEC (federal agency) demonstrate how the private sector and government can co-exist

- FASB promulgates accounting statements in accordance with US GAAP.
- SEC promulgates rulings on financial reporting based on FASB guidelines.

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 should include all interested parties in the Identity Ecosystem, including those who have invested in higher assurance credentials. Both Public and Private sectors should be represented. The Steering Group should be balanced to ensure that both privacy and security requirements are addressed.

A trade organization could be invited to nominate a member of the Steering Group.

The Steering Group should consist of members who are recognised in their industry / sector.

All members of the Steering Group should have a duty to represent the interests of the citizen as well as their industry / sector.

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

The Steering Group should operate transparently.

Uninvolved, but interested parties should be able to raise questions by contacting members of the Steering Group and / or sub committees / working groups.

If trade organizations have a member on the Steering Group this provides a contact point for their membership.

3.3. What does balanced representation mean and how can it be achieved? What steps can be taken guard against disproportionate influence over policy formulation?

Steering Group members should adopt a code of conduct. The code of conduct should include a declaration of interest to identify potential conflict of interest by members.

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?

TSCP believes that imposing a fee would not further the goal of fostering innovation.

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.

Federal Government should fund the Steering Group costs. Steering Group members' expenses should be covered by their employing sponsor / organization.

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?

Voting Rules should be simple and in principle all Steering Group members should have equal voting rights.

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?

Representation should evolve as NSTIC matures. As NSTIC engenders interest and draws a critical mass, the representation in the Steering Group may need to change. The Federal Government should be involved, as without the Federal Government this initiative will not take off.

4. International

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

The Steering Group should seek membership from entities who are addressing the international perspective within their industry sector. One such entity is TSCP. TSCP membership includes representatives from European and US Governments, Defence Primes based on both sides of the Atlantic and Technology Vendor members working together to develop a framework to allow sharing of information securely in cyberspace for the aerospace and defence sector. Therefore, for example, a Steering Group member from TSCP would be able to have a dual role - represent an industry sector and the international perspective.

The Steering Group should also seek representation from international organizations and standards.

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

The Steering Group should participate in and communicate with international entities and standardisation bodies involved in protecting digital identities.

The Steering Group may seek to establish a sub-committee or working group.

Within TSCP there is the Government Alignment Committee (GAC). The GAC provides a focal point for those members of TSCP that represent government entities to exchange information concerning issues related to harmonization of national activities as they impact the direction of TSCP. The specific purpose of the GAC is twofold:

- Evaluate policies that relate to TSCP's work and objectives to identify and address gaps between policy requirements and commercial solutions.
- Work with government members prior to issuance of national / local policies that will impact TSCP's work and objectives in order to assist in shaping policies that are consistent with commercial best practices.

Members of the GAC are expected to both participate in these activities and champion these activities within the government communities they represent.

4.3. On what international entities should the Steering Group focus its attention and activities?

These should include the European Telecommunications Standards Institute (ETSI) the European Network and Information Security Agency (ENISA), Secure idenTity acrOss bOrders LinKed (STORK). TSCP and other similar organizations.

4.4. How should the Steering Group maximize the Identity Ecosystem's interoperability internationally?

Interoperability will be achieved if the Steering Group base the Framework upon existing standards and seek to ensure that it is usable by any policy authority. The European Union works with standards based on best practices. The standards are objective oriented rather than rule based; the objective is to protect the digital form of the user's identity. ETSI prescribes the audit requirements for identity providers (ETSI TS 101 456). Both technology and procedures must be shown by identity providers.

For international interoperability there must be respect for the different approaches of protecting the digital identity.

The Steering Group should also look at other programmes / initiatives which have been successfully implemented:

- STORK (Secure idenTity across boRders linKed), an EU funded project.
- UN EDIFACT.
- Information Security Forum (ISF).

- TSCP

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

Use bodies such as TSCP who can represent NSTIC interests on the international arena.

The Federal Government should seek cross-representation on similar bodies within other nations and the European Union.