The Identity Ecosystem Steering Group Privacy Coordination Standing Committee

1 Introduction

The National Strategy for Trusted Identities in Cyberspace[1] (NSTIC) is founded on four guiding principles. The first principle, that identity solutions will be privacy-enhancing and voluntary (Privacy Guiding Principle), is intended not only to protect individuals' privacy and civil liberties from potential adverse impacts - for example, unwarranted correlation of individuals' online transactions and over-identification of individuals - but also to enhance privacy from the current state by, for example, enabling attribute assertion without the transmission of personally identifiable information elements. Building effective privacy into the Identity Ecosystem in the early stages is an important way to facilitate trust between organizations and consumers and increase consumer willingness to participate. The NIST Recommendations for Establishing an Identity Ecosystem Governance Structure (NIST Recommendations) and the incorporated Recommended Charter for the Identity Ecosystem Steering Group[2] call for the formation of a Privacy Coordination Standing Committee (Privacy Committee) within the Identity Ecosystem Steering Group (Steering Group) as a means of implementing the Privacy Guiding Principle.

2 Purpose

In its role as a standing committee, the Privacy Committee will maintain long-term consistency and focus around the achievement of the Privacy Guiding Principle by coordinating all activities within the Steering Group related to privacy and facilitating the implementation of the Fair Information Practice Principles (FIPPs) into the Identity Ecosystem as called for by the NSTIC.

3 Membership Composition

The composition of the Privacy Committee should reflect its mission. It needs individuals that have "extensive experience in the privacy field" as stated in the NIST Recommendations.[3] These privacy experts should have, at minimum, employment as a privacy practitioner, a curriculum vitae demonstrating appropriate privacy experience, or a widely-recognized privacy certification. At the same time, the Privacy Committee could substantially benefit from the knowledge of interested parties that may represent different fields of expertise, but who can provide insight into making privacy implementable and usable in Identity Ecosystem solutions. Consequently, the Privacy Committee also should accept as members, interested parties who do not have privacy expertise. However, to enable the Privacy Committee to appropriately maintain its privacy-focused mission, the majority of the

[1] National Strategy for Trusted Identities in Cyberspace, The White House, April 2011. http://www.whitehouse.gov/sites/default/files/rss_viewer/NSTICstrategy_041511.pdf

[2] Recommendations for Establishing an Identity Ecosystem Governance Structure, Department of Commerce, National Institute of Standards and Technology, February 2012. http://www.nist.gov/nstic/2012-nstic-governance-recs.pdf

[3] Id at 15.

members should be privacy experts and the Privacy Committee officers and liaisons (see 4.1.1) should always be privacy experts. Maintaining a membership ratio weighted towards privacy expertise and selecting officers and liaisons with strong privacy backgrounds will allow the Privacy Committee to carry out its core privacy functions while benefitting from the knowledge of other communities.

As further called for in the NIST Recommendations, the Privacy Committee should represent a "balance of viewpoints across a spectrum of experience." Therefore, it should include privacy experts from all types of organizations including advocacy groups, industry, and government. The Privacy Committee chair should have responsibility for achieving this balance through a variety of means, including member recruitment, building consensus in discussions, and maintaining a respectful environment that allows all members to be heard.

4 Scope

Based on the NIST Recommendations, the Steering Group will include Working Groups and Standing Committees that will conduct the work required for adopting standards, policies, and procedures that comprise the Identity Ecosystem Framework. The Privacy Committee should provide privacy expertise and assistance to the Working Groups and Standing Committees from the earliest stages to ensure privacy is "built in" to their work products. The Privacy Committee also should provide a formal review of these work products for the mitigation of privacy risks prior to review and approval by the Plenary. In addition, the Privacy Committee should identify privacy gaps that may not be addressed by other Working Groups and Standing Committees and develop appropriate recommendations for mitigating risks to individual privacy and civil liberties arising from the activities of the Steering Group. Both of these work streams should implement the FIPPs in their processes, but the Privacy Committee could also consider applying other consistent privacy frameworks, such as the Consumer Privacy Bill of Rights outlined in Consumer Data Privacy in a Networked World,[4] to guide its work. Finally, the Privacy Committee should establish reporting processes that promote transparency and accountability.

4.1 The Gatekeeper Function

The NIST Recommendations called for a gatekeeper function as a mechanism to create adherence of Steering Group work products to the Privacy Guiding Principle by ensuring that "…no recommendations on policies, standards or other work products should be reviewed or approved by the Plenary unless first approved by the Privacy Coordination Committee."[5] As noted by one commenter, "[i]t is worth mentioning the significant and powerful tension between protecting personal privacy and the desires of the marketplace to monetize personal identity. Therefore, the market alone is unlikely to force commercial entities to adhere to the guiding principles."[6] The NIST Recommendations view the gatekeeper function as critical to accomplishing such goals. Nonetheless, it is important to clarify that the gatekeeper function is intended to support a process wherein Working Groups and Standing

[4] Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy, The White House, February 2012. http://www.nist.gov/nstic/2012-nstic-governance-recs.pdf
[5] Recommendations for Establishing an Identity Ecosystem Governance Structure at 15.
[6] Id at 15.

Committees coordinate with the Privacy Committee from the earliest stages to build privacy into their work products, in contrast to being a barrier to forward progress in the development of the Identity Ecosystem Framework. The Privacy Committee should participate in the development of work products and identify and address privacy risks while products are being developed. This will increase the likelihood that privacy impacts are addressed early in the product development process and avoid potential delays or difficulties arising from attempts to "retro-fit" privacy into finished work products. To achieve these objectives, the Privacy Committee should maintain liaisons with privacy expertise to work with each Working Group and Standing Committee to identify privacy concerns with work products and provide guidance on how to resolve them.

4.1.1 Privacy Liaisons

The primary purpose of privacy liaisons is to identify privacy risks in work products of their assigned Working Groups and Standing Committees and facilitate agreement on how to address privacy issues as the work products develop so that formal Privacy Committee review can proceed in a streamlined manner. The Privacy Committee should determine the best means of supporting liaisons to achieve good outcomes – one possibility is to establish a subcommittee. This subcommittee could bring together resources to assist liaisons and provide a central place for collaboration, reporting and feedback.

The charters of the Privacy Committee, Working Groups, and Standing Committees should include mutually reinforcing language to support the role of liaisons. The Working Groups and Standing Committees should have procedures in place to request a privacy liaison and the Privacy Committee should have an obligation to proactively provide the liaisons.

It should be a core tenet that privacy liaisons and the members of the Working Groups and Standing Committees make good faith efforts to reach agreement. However, in the event that the parties are unable to reach common ground, the issues should be elevated to the Privacy Committee chair and the Working Group or Standing Committee chair for resolution. The chairs may also look to the Secretariat to provide facilitation assistance. If the chairs cannot reach an agreement, the work product should move to the formal Privacy Committee review process.

4.1.2 Formal Review

Formal review is a necessary complement to the liaison advisory function. The formal review will allow the Privacy Committee, once a work product has been completed, to review it for privacy risks using a standard methodology (see 4.1.3) and adherence to the FIPPs before Plenary review and approval. If the liaison process has worked well, the review should be able to proceed in a streamlined manner. To the extent that the resolution process outlined above (see 4.1.1) does not result in agreement and the Privacy Committee formal review correspondingly does not result in an approval, the Privacy Committee should provide the Plenary with a report explaining its decision to not approve the work product so that the Plenary can consider it with its review and vote. If the Plenary still approves the work product, the Privacy Committee's report should go to the Management Council. The Management Council should have to consider this report in its ratification decision. This review and reporting process provides a

number of checkpoints at which privacy concerns can be widely considered and triggers a series of escalating resolution approaches. As a result, this process should increase the likelihood that the gatekeeper function appropriately fosters adherence to the Privacy Guiding Principle without creating a barrier to forward progress in the development of the Identity Ecosystem Framework.

4.1.3 Privacy Assessment Framework

The Privacy Committee should develop processes and tools using a standard set of criteria based on the FIPPs articulated in the NSTIC (and other consistent privacy frameworks) to evaluate work products, identify privacy risks, and provide recommendations for mitigating potential adverse privacy impacts. The Privacy Committee should publicize this assessment framework to enable other Working Groups and Standing Committees to understand the process by which the Privacy Committee will assess their work products. Privacy liaisons should operate under this framework to provide consistent analysis of work products. As one methodology example, the federal government analyzes systems early in their development for the presence of privacy risks, referred to by some agencies as a privacy threshold analysis (PTA). If it finds privacy issues, the federal government will use a privacy impact assessment (PIA) to analyze those issues in depth. If it does not find privacy issues, further privacy analysis may not be warranted. Similarly, the Smart Grid Interoperability Panel (SGIP) Privacy Group performed a high level PIA for an initial analysis of privacy issues within the Smart Grid environment that it has used to guide its approach to addressing privacy risks for ongoing SGIP activities. One of the first tasks of the Privacy Committee should be to determine the best methodology and develop appropriate tools for managing consistent analysis.

4.2 Identifying Privacy Gaps in the Identity Ecosystem Framework

A comprehensive approach to facilitating the implementation of the Privacy Guiding Principle in the Identity Ecosystem Framework by the Privacy Committee will include not only responsive measures such as providing privacy liaisons and reviews of Steering Group work products, but proactive measures as well. Thus, the Privacy Committee should identify privacy gaps that may exist in the Identity Ecosystem Framework and that do not seem to be addressed in the scope of work covered by Working Groups and Standing Committees. The Privacy Committee should make and publicize recommendations as to how to address those privacy gaps. These recommendations could include the need for new policy development or standards adoption. As appropriate, the Privacy Committee may form its own subcommittees to execute certain recommendations. Other recommendations may call for the establishment of new working groups or new deliverables in existing ones.

4.3 Reporting and Accountability

The Privacy Committee should periodically compile reports and make them available to the public. The Privacy Committee report should include statistics and supporting evidence that describe the work products it reviews and the actions of its liaisons, the results of formal reviews, the time required to complete formal reviews, privacy gaps identified with associated recommendations and actions taken, and the status of its membership. This reporting should keep the Privacy Committee accountable for its actions within the Steering Group and allow the Privacy Committee to monitor its own processes to

increase its effectiveness. Privacy liaisons and any subcommittees should support such reporting by maintaining accurate documentation of their activities. The Secretariat should have responsibility for providing administrative support for this reporting.

The reporting would also allow the Management Council and Plenary Chair to evaluate the Privacy Committee's actions and, if they find problems in the process, recommend changes. Additionally, the Privacy Committee Chair should report to the Management Council or Plenary Chair upon request.

Appendix: Draft Privacy Coordination Privacy Committee Charter

IDENTITY ECOSYSTEM STEERING GROUP

CHARTER OF

THE PRIVACY COORDINATION STANDING COMMITTEE

Privacy Committee's Official Title. Privacy Coordination Standing Committee (hereafter referred to as "the Privacy Committee").

Authority. Under the authority of the Identity Ecosystem Steering Group Charter and By-laws, this charter establishes the Privacy Committee.

Scope of Objectives.

- The Privacy Committee shall facilitate the implementation of the Privacy-enhancing and Voluntary Guiding Principle of the National Strategy for Trusted Identities in Cyberspace (NSTIC) in the Identity Ecosystem Framework.
- The Privacy Committee shall maintain liaisons with privacy expertise to work with each working group and standing committee in the Plenary to build privacy into their deliverables as appropriate.
- The Privacy Committee shall provide a formal review of working group and standing committee work products for the mitigation of privacy risks prior to review and approval by the Plenary.
- The Privacy Committee shall identify privacy gaps in the Identity Ecosystem Framework and make recommendations to remedy them.

Roles and Responsibilities.

- Responsibilities of the Chair
    - The Chair is the presiding officer of the Privacy Committee, and guides its efforts to the effective completion of its tasks.
    - The Chair shall adhere to the Charter and such other rules of order and operating procedures as the Privacy Committee may adopt.
    - The Chair shall maintain a respectful environment that allows all members to be heard and work to build consensus within the Privacy Committee.
    - The Chair shall assign liaisons to the working groups and standing committees to ensure privacy expertise is available during the development of work products and recommendations, and assist them as needed. This responsibility may be delegated.
    - The Chair shall be responsible for working with other working group and standing committee chairs, the Plenary Chair and the Secretariat as appropriate to resolve concerns about mitigating privacy risks in Steering Group work products.

    - The Chair shall be responsible for membership recruitment as necessary to support balanced viewpoints within the Privacy Committee.
    - The Chair shall report to the Identity Ecosystem Plenary Chair or the Management Council upon request.
    - The Chair shall be responsible for addressing any impediments to the effective functioning of the Privacy Committee and taking appropriate corrective actions.
- Responsibilities of the Vice Chair
    - The Vice Chair shall support the Chair in fulfilling his or her responsibilities.
    - The Vice Chair shall assume and perform the duties of the Chair in the event the Chair is absent or unavailable.
- Responsibilities of the Secretary
    - The Secretary shall write meeting minutes and present them to the Privacy Committee for approval.
    - The Secretary shall support the Chair in fulfilling his or her responsibilities.
    - The Secretary shall assume and perform the duties of the Chair in the event that both the Chair and Vice-Chair are absent or unavailable.
- Responsibilities of the Liaisons
    - The Liaisons shall attend relevant meetings of their assigned working groups or standing committees.
    - The Liaisons shall identify privacy risks in their assigned working groups or standing committees' work products and provide guidance on mitigating these risks.
    - The Liaisons shall report on their activities to the Privacy Committee and shall maintain appropriate documentation to support these reports.
- Responsibilities of the Privacy Committee Members
    - Privacy Committee members shall attend meetings of the Committee and work to support the objectives of the Privacy Committee.
    - Privacy Committee members shall adhere to the Charter and such other rules of order and operating procedures as the Privacy Committee may adopt.
    - Privacy Committee members shall strive for a respectful environment that allows all members to be heard and work to build consensus within the Privacy Committee.

Evaluation Methodology. It is the responsibility of the Privacy Committee to develop, maintain, and adhere to a consistent evaluation methodology for identifying privacy risks, providing mitigating recommendations, and reviewing work products. The Privacy Committee shall develop processes and tools using a standard set of criteria based on the Fair Information Practice Principles articulated in the NSTIC. The Privacy Committee also may look to related and consistent privacy frameworks or relevant best practices in privacy in developing this methodology. The Privacy Committee shall publish the methodology to the Steering Group.

Conduct of Meetings. The Privacy Committee shall convene as needed, but no less than once per month. During these meetings, the Privacy Committee shall make decisions by consensus or voting in the absence of consensus. The Chair, Vice Chair, and Secretary shall have voting rights. The Privacy

Committee shall conduct meetings according to the procedures laid out in the Identity Ecosystem Steering Group By-laws.

Membership and Designation. Privacy Committee members shall be comprised of two types of members: experienced individuals in the privacy field (Privacy Experts) and other interested parties (Interested Parties). Qualifications for Privacy Experts shall include employment as a privacy practitioner, a curriculum vitae demonstrating appropriate privacy experience or a widely-recognized privacy certification. Interested Parties will not need to have any previous privacy experience. The number of members who are Interested Parties shall always be less than the number of Privacy Experts. The Chair, Vice-Chair, Secretary, and Liaisons shall all be Privacy Experts. Privacy Experts shall comprise a balance of viewpoints from all types of organizations including advocacy groups, industry, and government.

Membership participation requirements, and rights and responsibilities shall conform to the Identity Ecosystem Steering Group By-laws.

Appointment of Officers. The Privacy Committee shall annually elect the Chair, Vice-Chair, and Secretary by simple majority vote.

Subcommittees. The Privacy Committee may create subcommittees. A subcommittee may not work independently of the Privacy Committee and has no authority to make decisions on behalf of the Privacy Committee. Subcommittees shall report only to the Privacy Committee and shall maintain appropriate documentation of its activities to support these reports.

Reporting and Accountability. The Privacy Committee shall periodically create reports about its activities and make these reports available to the public. At a minimum, these reports shall include statistics and supporting evidence that describe the work products it reviews and the actions of its liaisons, the results of formal reviews, the time required to complete formal reviews, privacy gaps identified with associated recommendations and actions taken, and the status of its membership. The Privacy Committee also shall provide a report of its privacy concerns to the Plenary for any work product it does not approve. It shall provide this report to the Management Council in the event of Plenary approval. The Privacy Committee shall report to the Management Council and Plenary Chair upon request. The Secretariat shall provide administrative assistance in the development of these reports.

Duration/Termination. The Privacy Committee shall continue for the duration of the Identity Ecosystem Steering Group or until it may be dissolved by amendment to the Identity Ecosystem Steering Group Charter, whichever may be the earlier.