Ms. Erin Mackler
Audit and Attest Standards
American Institute of Certified Public Accountants
1211 Avenue of the Americas
New York, NY 10036-8775

September 14, 2015

RE: Proposed Revision of *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy*

Dear Ms. Mackler:

We appreciate the opportunity to comment on the proposed Revision of *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy*.

We are supportive of the Proposed Revision that restructures and creates a new set of privacy criteria, adds illustrative risks and controls related to privacy, clarifies CC3.1 and CC3.3, and adds new criteria for confidentiality. We believe these changes enhance the usefulness of the privacy trust services principle and will lead to greater understanding and adoption in the marketplace.

We have included certain recommendations and comments relating to:

a) Additional guidance to practitioners on when the privacy trust services principle has been met, particularly when the nature of the entity's business model is such that certain of the eight categories related specifically to privacy are not applicable.
b) Additional clarity around the intent of changes that suggest application of the trust services principles to entities that are not service organizations.

We offer the following suggestions for consideration in finalizing the proposed Revision.

Comments for consideration

We believe additional guidance is required to practitioners on treatment when the nature of the entity's business model is such that certain of the eight categories related specifically to privacy (from paragraph .13e) are not applicable. The applicability of the individual categories depends on the relationship the entity has with the data subjects, and in many business models a number of the categories would not apply. Practitioners would benefit from guidance on the need to include all privacy criteria in an engagement vs. the ability to include only relevant criteria based on the entity's business model, as well as related considerations on the ability to meet the privacy trust services principle in cases where not all criteria are applicable.

We note the additions to paragraph .04 on the types of subject matter a practitioner may examine and report on using the trust services principles, specifically the third bullet after strikethroughs are removed, significantly expands the potential applicability of the trust services principles beyond service organizations and raise questions regarding the intent of this expansion. Additional clarity is needed on the overall objectives and the intended users of such a report. Further questions include how the concept of 'external users' would be applied within the criteria in the absence of a service organization, and how 'commitments' would be defined. In addition, clarity is needed on

the rationale for excluding the fairness of presentation of the description from the subject matter in cases where the entity is not a service organization.

With regard to the specific questions in the Guide for Respondents:

Q1: Are the criteria written at an appropriate level?

A1: Generally, yes, but we are interested in the rationale for removing more detailed sub-criteria from selected criteria. Also see comments on the wording of specific criteria in the Appendix.

Q2: Are the criteria complete?

A2: Yes

Q3: Are the criteria measurable?

A3: Yes

Q4: Does the revised structure of the privacy principle accurately reflect how a practitioner looks at privacy of the information processed by the system?

A4: Generally, yes, subject to the concern noted above when aspects of privacy (i.e., certain of the categories defined in paragraph .13e) are not relevant to the business model of the entity. We offer the suggestions above for consideration in finalizing the proposed revision.

The Appendix to this letter includes additional editorial comments on the proposed Revision.

* * * * * * *

We appreciate the opportunity to express our views and would be pleased to discuss our comments or answer any questions you may have. Please contact Mary Grace Davenport (646-471-8753) regarding our submission.

Sincerely,

PricewaterhouseCoopers LLP

APPENDIX

This Appendix provides our editorial comments on the Proposed Revisions.

- Title – first word should be 'TSP' instead of 'TPS'
- Paragraph .01 – in changing 'and' to 'or', a third instance should also be changed within the first sentence, in 'confidentiality and privacy'. This will mirror the similar wording in paragraph .02
- Paragraph .04 – suggest adding the publish date of the AICPA Guide to avoid potential confusion. Also, at end of first lengthy sentence of the first bullet, the 'operating effectiveness of those controls throughout a specified period' would not be included in a type 1 engagement.
- Paragraph .06 – final sentence, final clause, AT 101 may also be an option in addition to AT 601
- Paragraph .12 – commitments may also be made to parties other than customers
- Paragraph .13e – each of the other principles has a single defining sentence, but privacy does not. It is defined more by what it addresses instead of a single declarative statement.
- Paragraph .13e – because it references criteria, the lead in to the eight categories should note that these categories of privacy criteria are in addition to the common criteria.
- Paragraph .13e, category i – when using the word 'including', are there others that are not listed?
- Paragraph .13e, categories iii – vi – the ending phrasing differs by category even though it seems it should be consistent. Category iii ends with 'consistent with its privacy commitments in accordance with system requirements', category iv with 'in accordance with privacy commitments and system requirements', category v with 'in accordance with its privacy commitments and system requirements', category vi with 'in accordance with the entity's commitments and system requirements'. Also, in category vi, 'regulator' should be 'regulators'.
- Paragraph .14 – the second sentence needs grammatical correction and (a) and (b) appear redundant to points (1) and (2). Also, in bullet f on Systems operations, need to delete 'of" in the final clause.
- CC1.2 (in paragraph .15) – should 'placed in operation' be 'implemented'?
- CC2.3 – not clear on definition of 'respective parties'
- CC2.4 – should 'approving' be added to the actions in order to better mirror CC1.2?
- CC2.6 – users should be users'
- CC3.1 – need for more clarity/practitioner guidance on the application of the newly inserted verbiage on threats from user of vendors/third parties and customer personnel. Suggestion to include examples of organizations that could be relevant to the engagement (e.g., if this just subservice organizations or would this extend to other parties as well)?
- CC3.3 – should 'deployment of control activities' be 'implementation'?
- CC5.2 – Similar to edit to first sentence, final sentence on removal of access may also be amended to indicate applicability when 'access is administered by the entity'.
- CC7.1 – is 'approval/authorization' needed here to mirror CC1.2?
- A1.2 – is 'approval' needed here?
- PI1.1 – should 'to meet the entity's processing integrity commitments…' be changed to 'in accordance with the entity's processing integrity commitments…' to be consistent with phrasing in PI1.2-PI1.5?
- C1.7 – Is 'retains' specific enough? Should it be 'retains confidential information for a specified time in accordance…'?
- P1.2 – Is the word 'related' needed? It is not used before other instances of 'system requirements'
- P6.5 – insert 'system' before requirements
- P6.6 – Aren't the 'established incident response procedures' part of the 'system requirements'?
- Appendix B (paragraph .18) Illustrative Risks and Controls – general comment that many of the illustrative controls read more as policy statements than controls, with an example being C1.8.