Asia-Pacific
Economic Cooperation

2013/SOM1/ECSG/DPS/I/003
Agenda Item: II

CBPR Intake Document for Data Collectors

Purpose: Information
Submitted by: United States

APEC
INDONESIA 2013

Data Privacy Sub-Group Informal Meeting
Jakarta, Indonesia
31 January 2013

APEC CROSS-BORDER PRIVACY RULES SYSTEM
INTAKE QUESTIONNAIRE

GENERAL

i. Name of the Organization that is seeking certification:
_____

ii. List of subsidiaries and/or affiliates governed by your privacy policy to be covered by this certification, their location, and the relationship of each to you:
_____

iii. Organization's Contact Point for Cross Border Privacy Rules ("CBPR")
Name: _____
Title: _____
Email: _____
Phone: _____

iv. For what type(s) of personal information are you applying for certification? Please check all that apply.

Customer/ Prospective Customer_____
Employee/Prospective Employee _____
Other (Please describe)_____

v. In which economies do you, your affiliates and/or subsidiaries collect or anticipate collecting personal information to be certified under this system? Please check all that apply.

☐ Australia	☐ New Zealand
☐ Brunei Darussalam	☐ Papua New Guinea
☐ Canada	☐ Peru
☐ Chile	☐ Philippines
☐ People's Republic of China	☐ Russia
☐ Hong Kong, China	☐ Singapore
☐ Indonesia	☐ Chinese Taipei
☐ Japan	☐ Thailand
☐ Republic of Korea	☐ United States
☐ Malaysia	☐ Viet Nam
☐ Mexico	

vi. To which economies do you, your affiliates and/or subsidiaries transfer or anticipate transferring personal information to be certified under this system? Please check all that apply.

□ Australia □ Brunei Darussalam □ Canada □ Chile □ People's Republic of China □ Hong Kong, China □ Indonesia □ Japan □ Republic of Korea □ Malaysia □ Mexico	□ New Zealand □ Papua New Guinea □ Peru □ Philippines □ Russia □ Singapore □ Chinese Taipei □ Thailand □ United States □ Viet Nam

NOTICE (QUESTIONS 1-4)

The questions in this section are directed towards:

(a) ensuring that individuals understand your policies regarding personal information that is collected about them, to whom it may be transferred and for what purpose it may to be used; AND

(b) ensuring that, subject to the qualifications listed in part II, individuals know when personal information is collected about them, to whom it may be transferred and for what purpose it may be used.

General

1. Do you provide clear and easily accessible statements about your practices and policies that govern the personal information described above (a privacy statement)? Where YES, provide a copy of all applicable privacy statements and/or hyperlinks to the same.

_____ Y _____ N

a) Does this privacy statement describe how your organization collects personal information?

_____ Y _____ N

b) Does this privacy statement describe the purpose(s) for which personal information is collected?

_____ Y _____ N

c) Does this privacy statement inform individuals as to whether and/for what purpose you make personal information available to third parties?

_____ Y _____ N

d) Does this privacy statement disclose the name of your company and location, including information on how to contact you about your practices and handling of personal information upon collection? Where YES describe below.

_____ Y _____ N

e) Does this privacy statement provide information regarding the use and disclosure of an individual's personal information?

_____ Y _____ N

f) Does this privacy statement provide information regarding whether and how an individual can access and correct their personal information?

_____ Y _____ N

2. Subject to the qualifications listed below, at the time of collection of personal information, (whether directly or through the use of third parties acting on your behalf) do you provide notice that such information is being collected?

_____ Y _____ N

3. Subject to the qualifications listed below, at the time of collection of personal information, (whether directly or through the use of third parties acting on your behalf), do you indicate the purpose(s) for which personal information is being collected?

_____ Y _____ N

4. Subject to the qualifications listed below, at the time of collection of personal information, do you notify individuals that their personal information may be shared with third parties?

_____ Y _____ N

Qualifications to the Provision of Notice

The following are situations in which the application at the time of collection of the APEC Notice Principle may not be necessary or practical.

i. **Obviousness:** Personal Information controllers do not need to provide notice of the collection, use or third-party sharing of personal information in those circumstances where consent by the individual can be inferred from the provision of the individual's information (e.g. if an individual gives his or her business card to another individual in the context of a business relationship, the individual would not expect that notice would be provided regarding the collection and normal use of that information).

ii. Collection of Publicly-Available Information: Personal information controllers do not need to provide notice regarding the collection and use of publicly available information.

iii. Technological Impracticability: Personal Information controllers do not need to provide notice at or before the time of collection in those cases where electronic technology automatically collects information when a prospective customer initiates contact (e.g. through the use of cookies). However, the notice should be provided to the individuals as soon after as is practicable.

iv. Disclosure to a government institution which has made a request for the information with lawful authority: Personal information controllers do not need to provide notice of disclosure to law enforcement agencies for investigation purposes where the provision of such notice to the individual will likely prejudice the investigation.

v. Disclosure to a third party pursuant to a lawful form of process: Personal information controllers do not need to provide notice of disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

vi. Third-Party Receipt: Where personal information is received from a third party, the recipient personal information controller does not need to provide notice to the individuals at or before the time of collection of the information.

vii. For legitimate investigation purposes: When providing notice would compromise the availability or accuracy of the information and the collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

viii. Action in the event of an emergency: Personal Information controllers do not need to provide notice in emergency situations that threaten the life, health or security of an individual.

COLLECTION LIMITATION (QUESTIONS 5-7)

The questions in this section are directed towards ensuring that collection of information is limited to the stated purposes for which it is collected. The collection of the information should be relevant to such purposes, and proportionality to the fulfillment of such purposes may be a factor in determining what is relevant. In all instances, collection methods must be lawful and fair.

5. How do you obtain personal information:

    a) Directly from the individual?

    _____ Y _____ N

    b) From third parties collecting on your behalf?

    _____ Y _____ N

    c) Other. If YES, describe.

    _____ Y _____ N

6. Do you limit your personal information collection (whether directly or through the use of third parties acting on your behalf) to information that is relevant to fulfill the purpose(s) for which it is collected or other compatible or related purposes?

    _____ Y _____ N

7. Do you collect personal information (whether directly or through the use of third parties acting on your behalf) by lawful and fair means, consistent with the requirements of the jurisdiction that governs the collection of such personal information? Where YES, describe.

    _____ Y _____ N

USES OF PERSONAL INFORMATION (QUESTIONS 8-13)

The questions in this section are directed toward ensuring that the use of personal information is limited to fulfilling the purposes of collection and other compatible or related purposes. This section covers use, transfer and disclosure of personal information. Application of this Principle requires consideration of the nature of the information, the context of collection and the intended use of the information. The fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended usage stems from or is in furtherance of such purposes. The use of personal information for "compatible or related purposes" could extend, for example, to matters such as the creation and use of a centralized database to manage personnel in an effective and efficient manner; the processing of employee payrolls by a third party; or, the use of information collected by an organization for the purpose of granting credit for the subsequent purpose of collecting debt owed to that organization.

8. Do you limit the use of the personal information you collect (whether directly or through the use of third parties acting on your behalf) as identified in your privacy statement and/or in the notice provided at the time of collection to those purposes for which the information was collected or for other compatible or related purposes? If necessary, provide a description in the space below.

_____ Y _____ N

9. If you answered NO, do you use the personal information you collect for unrelated purposes under one of the following circumstances? Describe below.

    a) Based on express consent of the individual?

    b) Compelled by applicable laws?

10. Do you disclose personal information you collect (whether directly or through the use of third parties acting on your behalf) to other personal information controllers? If YES, describe.

_____ Y _____ N

11. Do you transfer personal information to personal information processors? If YES, describe.

_____ Y _____ N

12. If you answered YES to question 10 and/or question 11, is the disclosure and/or transfer undertaken to fulfill the original purpose of collection or another compatible or related purpose? Describe below.

_____ Y _____ N

13. If you answered NO to question 12, or if otherwise appropriate, does the disclosure and/or transfer take place under one of the following circumstances?

a) Based on express consent of the individual?

b) Necessary to provide a service or product requested by the individual?

c) Compelled by applicable laws?

CHOICE (QUESTIONS 14-20)

The questions in this section are directed towards ensuring that individuals are provided with choice in relation to collection, use, and disclosure of their personal information. However, this Principle recognizes, through the introductory words "where appropriate" in the Framework itself, that there are certain situations where consent may be clearly implied or where it would not be necessary to provide a mechanism to exercise choice. These situations are detailed in "Qualifications to the Provision of Choice Mechanisms".

General

14. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the collection of their personal information? Where YES describe such mechanisms below.

_____ Y _____ N

15. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the use of their personal information? Where YES describe such mechanisms below.

_____ Y _____ N

16. Subject to the qualifications described below, do you provide a mechanism for individuals to exercise choice in relation to the disclosure of their personal information? Where YES describe such mechanisms below.

_____ Y _____ N

17. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they displayed or provided in a clear and conspicuous manner?

_____ Y _____ N

18. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are they clearly worded and easily understandable?

_____ _____
Y N

19. When choices are provided to the individual offering the ability to limit the collection (question 14), use (question 15) and/or disclosure (question 16) of their personal information, are these choices easily accessible and affordable? Where YES, describe.

_____ _____
Y N

20. What mechanisms are in place so that choices, where appropriate, can be honored in an effective and expeditious manner? Provide a description in the space below or in an attachment if necessary. Describe below.

Qualifications to the Provision of Choice Mechanisms

The following are situations in which the application of the APEC Choice Principle may not be necessary or practical.

i. **Obviousness:** Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in the collection, use or third-party sharing of personal information in those circumstances where consent by the individual can be inferred from the provision of the individual's information.

ii. **Collection of Publicly-Available Information**: Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the collection and use of publicly available information.

iii. **Technological Impracticability**: Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in relation to those cases where electronic technology automatically collects information when a prospective customer initiates contact [e.g. use of cookies]. However, a mechanism to exercise choice as to use and disclosure should be provided after collection of the information.

iv. **Third-Party Receipt**: Where personal information is received from a third party, the recipient personal information controller does not need to provide a mechanism for individuals to exercise choice in relation to the collection of the information. However, if the personal information controller engages a third party to collect personal information on its behalf, the personal information controller should instruct the collector to provide such choice when collecting the personal information.

v. **Disclosure to a government institution which has made a request for the information with lawful authority**: Personal Information controllers do not need to provide a

mechanism for individuals to exercise choice in relation to disclosure to law enforcement agencies for investigation purposes where the provision of such mechanism to the individual will likely prejudice the investigation.

vi. **Disclosure to a third party pursuant to a lawful form of process:** Personal information controllers do not need to provide a mechanism for individuals to exercise choice in relation to the disclosure to a third party when such disclosure was requested pursuant to a lawful form of process such as a discovery request made in the course of civil litigation.

vii. **For legitimate investigation purposes**: When providing a mechanism for individuals to exercise choice would compromise the availability or accuracy of the personal information and its collection, use and disclosure are reasonable for purposes relating to an internal or external investigation of a violation of a code of conduct, breach of contract or a contravention of domestic law.

viii. **Action in the event of an emergency**: Personal Information controllers do not need to provide a mechanism for individuals to exercise choice in emergency situations that threaten the life, health or security of an individual.

INTEGRITY OF PERSONAL INFORMATION (QUESTIONS 21-25)

The questions in this section are directed towards ensuring that the personal information controller maintains the accuracy and completeness of records and keeps them up to date. This Principle also recognizes that these obligations are only required to the extent necessary for the purposes of use.

21. Do you take steps to verify that the personal information held by you is up to date, accurate and complete, to the extent necessary for the purposes of use? If YES, describe.

_____ Y _____ N

22. Do you have a mechanism for correcting inaccurate, incomplete and out-dated personal information to the extent necessary for purposes of use? Provide a description in the space below or in an attachment if necessary.

_____ Y _____ N

23. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the transfer of the information, do you communicate the corrections to personal information processors, agents, or other service providers to whom the personal information was transferred? If YES, describe.

_____ Y _____ N

24. Where inaccurate, incomplete or out of date information will affect the purposes of use and corrections are made to the information subsequent to the disclosure of the information, do you communicate the corrections to other third parties to whom the personal information was disclosed? If YES, describe.

25. Do you require personal information processors, agents, or other service providers who act on your behalf to inform you when they become aware of information that is inaccurate, incomplete, or out-of-date?

_____ Y _____ N

SECURITY SAFEGUARDS (QUESTIONS 26-35)

The questions in this section are directed towards ensuring that when individuals entrust their information to an organization, their information will be protected with reasonable security safeguards to prevent loss or unauthorized access to personal information or unauthorized destruction, use, modification or disclosure of information or other misuses.

26. Have you implemented an information security policy?

_____ Y _____ N

27. Describe the physical, technical and administrative safeguards you have implemented to protect personal information against risks such as loss or unauthorized access, destruction, use, modification or disclosure of information or other misuses?

28. Describe how the safeguards you identified in response to question 27 are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held.

29. Describe how you make your employees aware of the importance of maintaining the security of personal information (e.g. through regular training and oversight).

30. Have you implemented safeguards that are proportional to the likelihood and severity of the harm threatened, the sensitivity of the information, and the context in which it is held through:

    a) Employee training and management or other organizational safeguards?

    _____ Y _____ N

    b) Information systems and management, including network and software design, as well as information processing, storage, transmission, and disposal?

    _____ Y _____ N

    c) Detecting, preventing, and responding to attacks, intrusions, or other security failures?

    _____ Y _____ N

d) Physical security?

_____ Y _____ N

31. Have you implemented a policy for secure disposal of personal information?

_____ Y _____ N

32. Have you implemented measures to detect, prevent, and respond to attacks, intrusions, or other security failures?

_____ Y _____ N

33. Do you have processes in place to test the effectiveness of the safeguards referred to above in question 32? Describe below.

_____ Y _____ N

34. Do you use third-party certifications or other risk assessments? Describe below.

_____ Y _____ N

35. Do you require personal information processors, agents, contractors, or other service providers to whom you transfer personal information to protect against loss, or unauthorized access, destruction, use, modification or disclosure or other misuses of the information by:

a) Implementing an information security program that is proportionate to the sensitivity of the information and services provided?

_____ Y _____ N

b) Notifying you promptly when they become aware of an occurrence of breach of the privacy or security of your organization's personal information?

_____ Y _____ N

c) Taking immediate steps to correct/address the security failure which caused the privacy or security breach?

_____ Y _____ N

ACCESS AND CORRECTION (QUESTIONS 36-38)

The questions in this section are directed towards ensuring that individuals are able to access and correct their information. This section includes specific conditions for what would be considered reasonable in the provision of access. Access will also be conditioned by security requirements that preclude the provision of direct access to information and will require sufficient proof of identity prior to provision of access. The details of the procedures by which the ability to access and correct information is provided may differ depending on the nature of the information and other interests. For this reason, in certain circumstances, it may be impossible, impracticable or unnecessary to change, suppress or delete records.

The ability to access and correct personal information, while generally regarded as a central aspect of privacy protection, is not an absolute right. While you should always make good faith efforts to provide access, in some situations, it may be necessary to deny claims for access and correction. "Qualifications to the Provision of Access and Correction" sets out those conditions that must be met in order for such denials to be considered acceptable. When you deny a request for access, for the reasons specified herein, you should provide the requesting individual with an explanation as to why you have made that determination and information on how to challenge that denial. You would not be expected to provide an explanation, however, in cases where such disclosure would violate a law or judicial order.

General

36. Upon request, do you provide confirmation of whether or not you hold personal information about the requesting individual? Describe below.

_____ Y _____ N

37. Upon request, do you provide individuals access to the personal information that you hold about them? Where YES, answer questions 37(a) – (e) and describe your organization's policies/procedures for receiving and handling access requests below. Where NO, proceed to question 38

_____ Y _____ N

a) Do you take steps to confirm the identity of the individual requesting access? If YES, please describe.

_____ Y _____ N

b) Do you provide access within a reasonable timeframe following an individual's request for access? If YES, please describe.

_____ _____
Y N

c) Is information communicated in a reasonable manner that is generally understandable (in a legible format)? Please describe.

_____ _____
Y N

d) Is information provided in a way that is compatible with the regular form of interaction with the individual (e.g. email, same language, etc)?

_____ _____
Y N

e) Do you charge a fee for providing access? If YES, describe below on what the fee is based and how you ensure that the fee is not excessive.

_____ _____
Y N

38. Do you permit individuals to challenge the accuracy of their information, and to have it rectified, completed, amended and/or deleted? Describe your organization's policies/procedures in this regard below and answer questions 38 (a), (b), (c), (d) and (e).

_____ _____
Y N

a) Are your access and correction mechanisms presented in a clear and conspicuous manner? Provide a description in the space below or in an attachment if necessary.

_____ _____
Y N

b) If an individual demonstrates that personal information about them is incomplete or incorrect, do you make the requested correction, addition, or where appropriate, deletion?

_____ Y _____ N

c) Do you make such corrections or deletions within a reasonable timeframe following an individual's request for correction or deletion?

_____ Y _____ N

d) Do you provide a copy of the corrected personal information or provide confirmation that the data has been corrected or deleted to the individual?

_____ Y _____ N

e) If access or correction is refused, do you provide the individual with an explanation of why access or correction will not be provided, together with contact information for further inquiries about the denial of access or correction?

_____ Y N _____

Qualifications to the Provision of Access and Correction Mechanisms

Although organizations should always make good faith efforts to provide access, there are some situations, described below, in which it may be necessary for organizations to deny access requests. Please identify which, if any, of these situations apply, and specify their application to you, with reference to your responses provided to the previous questions, in the space provided.

i. **Disproportionate Burden:** Personal information controllers do not need to provide access and correction where the burden or expense of doing so would be unreasonable or disproportionate to the risks to the individual's privacy in the case in question, as for example when claims for access are repetitious or vexatious by nature.

ii. **Protection of Confidential Information:** Personal information controllers do not need to provide access and correction where the information cannot be disclosed due to legal or security reasons or to protect confidential commercial information (i.e. information that you have taken steps to protect from disclosure, where such disclosure would facilitate a competitor in the market to use or exploit the information against your business interest causing significant financial loss). Where confidential commercial information can be readily separated from other information subject to an access request, the personal information controller should redact the confidential commercial information and make available the non-confidential commercial information to the extent that such information constitutes personal information of the individual concerned.

Other situations would include those where disclosure of information would benefit a competitor in the market place, such as a particular computer or modeling program. Furthermore, a denial of access may also be considered acceptable in situations where, for example providing the information would constitute a violation of laws or would compromise security.

iii. **Third Party Risk:** Personal information controllers do not need to provide access and correction where the information privacy of persons other than the individual would be violated. In those instances where a third party's personal information can be severed from the information requested for access or correction, the personal information controller must release the information after redaction of the third party's personal information.

ACCOUNTABILITY (QUESTIONS 39-50)

The questions in this section are directed towards ensuring that you are accountable for complying with measures that give effect to the Principles stated above. Additionally, when transferring information, you should be accountable for ensuring that the recipient will protect the information consistently with these Principles when not obtaining consent. Thus, you should take reasonable steps to ensure the information is protected, in accordance with these Principles, after it is transferred. However, there are certain situations where such due diligence may be impractical or impossible, for example, when there is no on-going relationship between you and the third party to whom the information is disclosed. In these types of circumstances, you may choose to use other means, such as obtaining consent, to assure that the information is being protected consistently with these Principles. However, in cases where disclosures are required by domestic law, you would be relieved of any due diligence or consent obligations.

General

39. What measures does your organization take to ensure compliance with the APEC Information Privacy Principles? Please check all that apply and describe below.

    - Internal guidelines or policies (if applicable, describe how implemented) _____
    - Contracts _____
    - Compliance with applicable industry or sector laws and regulations ____
    - Compliance with self-regulatory organization code and/or rules ____
    - Other (describe) ____

40. Has your organization appointed an individual(s) to be responsible for your organization's overall compliance with the Privacy Principles?

    _____ Y _____ N

41. Does your organization have procedures in place to receive, investigate and respond to privacy-related complaints? Please describe.

    _____ Y _____ N

42. Does your organization have procedures in place to ensure individuals receive a timely response to their complaints?

    _____ Y _____ N

43. If YES, does this response include an explanation of remedial action relating to their complaint? Describe.

_____ Y _____ N

44. Do you have procedures in place for training employees with respect to your privacy policies and procedures, including how to respond to privacy-related complaints? If YES, describe.

_____ Y _____ N

45. Do you have procedures in place for responding to judicial or other government subpoenas, warrants or orders, including those that require the disclosure of personal information?

_____ Y _____ N

Maintaining Accountability When Personal Information is Transferred

46. Do you have mechanisms in place with personal information processors, agents, contractors, or other service providers pertaining to personal information they process on your behalf, to ensure that your obligations to the individual will be met (check all that apply)?
    - *Internal guidelines or policies* _____
    - *Contracts* _____
    - *Compliance with applicable industry or sector laws and regulations* _____
    - *Compliance with self-regulatory organization code and/or rules* _____
    - *Other (describe)* _____

47. Do these mechanisms generally require that personal information processors, agents, contractors or other service providers:

    - Abide by your APEC-compliant privacy policies and practices as stated in your Privacy Statement? _____
    - Implement privacy practices that are substantially similar to your policies or privacy practices as stated in your Privacy Statement? _____
    - Follow-instructions provided by you relating to the manner in which your personal information must be handled? _____
    - Impose restrictions on subcontracting unless with your consent? _____
    - Have their CBPRs certified by an APEC accountability agent in their jurisdiction? _____

- Other (describe) _____

48. Do you require your personal information processors, agents, contractors or other service providers to provide you with self-assessments to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.

_____ Y _____ N

49. Do you carry out regular spot checking or monitoring of your personal information processors, agents, contractors or other service providers to ensure compliance with your instructions and/or agreements/contracts? If YES, describe below.

_____ Y _____ N

50. Do you disclose personal information to other personal information controllers in situations where due diligence and mechanisms to ensure compliance with your APEC CBPRs by the recipient as described above is impractical or impossible?

_____ Y _____ N