

Privacy Protection Cooperation Team  
The Korea Communications Commission,  
Personal Information Protection Cooperation Division  
The Ministry of the Interior and Safety

---

December 14, 2017

## Requesting a review of the APEC CBPRs Accountability Agent Recognition Application

1. In regards to APEC CROSS BORDER PRIVACY RULES SYSTEM (hereinafter referred to as 'CBPRs'), we, Korea Internet & Security Agency(hereinafter referred to as 'KISA'), are pleased to apply for the Accountability Agent.

2. KISA is a special corporation(a generic name for corporations established by national policy according to special laws for public interests) established in accordance with the 'Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.', and a public institution pursuant to the 'Act on the Management of Public Institutions'. Under these laws, KISA's all activities including those related to personal information protection or activities as an APEC CBPRs Accountability Agent or any other, should be managed and supervised by the competent authorities such as the Ministry of Science and ICT, the Korea Communications Commission and the Ministry of the Interior and Safety.

3. Also, KISA confirms that the documents necessary for the APEC CBPRs Accountability Agent application and additional documents are provided in the form of annexes or appendixes as follows.

- 1) documents that explain that KISA meets the certification authority approval criteria (Annex A)
- 2) KISA's detailed certification criteria that conforms to the program

requirements of the CBPR (Annex B)

3) The contact information and signature of KISA official in charge of this application (Annex C)

4) KISA's CBPRs operating system (draft version) (Appendix 1)

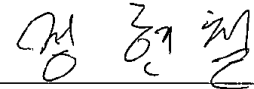
5) KISA's 'Complaints and processing rules for reports' (Appendix 2)

4. It will be appreciated if you review above documents and take a necessary step for APEC recognition on our application. For questions, please contact Jaesuk YUN, manager of the Personal Data Cooperation Team([jsyun@kisa.or.kr](mailto:jsyun@kisa.or.kr)).

*Jeong Hyun-Cheol*

*Vice President*

*Korea Internet & Security Agency*



---

## Accountability Agent Recognition Criteria Checklist

### 1 Conflict of Interest

1. Certification Applicant should describe how requirements 1(a) and (b) in Annex A have been met and submit all applicable written policies and documentation.

KISA is a special cooperation established by national policy according to special laws 'the 'Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.' for the public interest, and as a public agency under the 'Act on the Management of Public Institutions', KISA performs its duties fairly and objectively under the management and supervision of the Ministry of Science and ICT, the Korea Communications Commission as well as the Ministry of the Interior and Safety, etc. Also, revenues generated through certification activities will be deposited in the national account or used for public interests, but not for the interest of KISA.

※ 「**Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc.**」 **Article 52 (Korea Internet and Security Agency)** (1) The Government shall establish the Korea Internet and Security Agency (hereinafter referred to as the "Internet and Security Agency") to upgrade the information and communications network (excluding matters concerning establishment, improvement and management of information and telecommunications network), encourage the safe use thereof, and promote the international cooperation and advancement into the overseas market in relation to broadcasting and communications.

※ 「**Act on the Management of Public Institutions**」 **Article 4 (Public Institutions)** (1) The Minister of Strategy and Finance may designate any of the following institutions, which are a legal entity, organization, or institution (hereinafter referred to as "institution") other than the State or a local government, as a public institution:

1. An institution directly established pursuant to other Act with an investment by the Government;

2. Certification Applicant should submit an overview of the internal structural and procedural safeguards to address any of the potential or actual conflicts of interest identified in 2(b) of Annex A.

As a public agency providing public services, KISA is managed and supervised by the government, and establishes and enforces assessment rules and codes of conduct, and

regularly provides education on integrity in accordance with the 'Improper Solicitation and Graft Act' and government policies so that our employees will perform their duties in a fair manner.

◎ According to KISA's APEC CBPRs operating system (draft), it organizes and operates the certification committee that deliberates on and determines the review results for the sake of fair reviews, and makes sure that people with a conflict of interest cannot take part in any business related to certification.

※ **CBPRs operating system (draft) Article 6 (Composition of the certification committee)** ① The head of the Accountability Agent must install and operate the certification committee to deliberate and make decisions on the following:

1. Whether the results of certification assessment or re-certification assessment meet the certification criteria,
2. If the compliance review assessment found one of the reasons described in Paragraph 1 of Article 27 and whether the results are appropriate,
3. Matters concerning the cancellation of certification pursuant to Paragraph 1 of Article 27,
4. Matters concerning objections described in Article 28,
5. Other matters that the chairperson deems necessary in relation to CBPRs certification.

② The certification committee must consist of at least 10 committee members, and the committee members will be appointed by the head of the Accountability Agent from among people who have knowledge and experience in personal information protection, such as personal information protection experts, lawyers and professors, and the chairperson will be elected by the committee from among its members.

③ The chairperson will oversee the certification committee and represent the committee.

④ The head of the Accountability Agent may dismiss committee members if they violated any laws or these regulations.

**Article 8 (Organization and operation of the certification assessment team)** ③ A certification assessor who participated in the consulting for the CBPRs certification of the Applicant or the employee of the Applicant must be excluded from the certification assessment team.

**Article 9 (Exclusion, avoidance and evasion)** ① If certification committee members and assessors on the certification assessment team fall under any of the following in relation to the Certification Applicant, they cannot be involved in or participate in deliberation, voting and certification assessment:

1. In the event that committee members and assessors have a direct stake in the matters,
2. In the event that the matters are related to the present or former relatives of committee members and assessors,
3. In the event that committee members and assessors have a direct stake in the matters due to special legal relationships,
4. In the event that committee members and assessors were involved in assessment, investigation or examination of the matters before they were appointed.

② If committee members and assessors cannot guarantee the independence, objectivity, fairness and reliability of certification, e.g. deliberation, voting and certification assessment, the Accountability Agent may exclude, circumvent or ignore the committee members and assessors.

③ If committee members and assessors cannot be expected to be fair in deliberation, voting and certification assessment, the Certification Applicant may request circumvention, and the committee will vote on the matter.

④ If there are reasons for excluding or circumventing committee members and assessors, they may evade

deliberation, voting and certification assessment for themselves.

3. Certification Applicant should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

According to KISA's APEC CBPRS operating system (draft), the qualifications of certification auditors who acquired their qualifications by illegal means, or commit illegal acts related to certification, e.g. leaking information they acquired during certification assessment and getting illegal profits will be canceled.

※ **CBPRS operating system (draft) Article 14 (Cancellation of the qualifications of certification assessors)** If KISA finds any of the following reasons, it can cancel the qualifications of certification assessors:

1. In the event that the documents submitted during application for certification assessor qualifications were proven to be false,
2. In the event that the information acquired during certification assessment was leaked to others or used for purposes other than business without the consent of the Certification Applicant,
3. In the event that certification assessors received any money, valuables or profits in relation to certification assessment.

## 2 Program Requirements

4. Certification Applicant should indicate whether it intends to use the relevant template documentation developed by APEC or make use of Annex C to map its existing intake procedures program requirements.

KISA is mapping the detailed evaluation criteria based on our own Personal Information Management System (PIMS) to APEC's 50 CBPRS programs as shown in <Annex B> to satisfy APEC's criteria.

## 3 Certification Process

5. Applicant Accountability Agent should submit a description of how the requirements as identified in 5 (a) – (d) of Annex A have been met.

KISA's APEC CBPRS operating system (draft) includes the following certification process.



#### ④ On-going Monitoring and Compliance Review Processes

6. Certification Applicant should submit a description of the written procedures to ensure the integrity of the certification process and to monitor the participant's compliance with the program requirements described in 5 (a)-(d).

According to KISA's APEC CBPRS operating system (draft), we are regularly monitoring changes, e.g. changes in the participants' services during the term of validity of the certificate and changes in the targets such as when M&As occur, and if there is any such change, we conduct a compliance review. We can determine the review method, including online inspection and remote inspection of vulnerabilities, in consideration of changes by mutual agreement with the participants.

- ※ **CBPRs operating system (draft) Article 25 (compliance review assessment)** ① If the Accountability Agent finds it necessary to conduct regular assessment or to audit at any time during the term of validity of the issued certificate, the institutions which acquired certification must accept to receive the verification audit.
- ② If the targets of certification are changed or it is deemed difficult to maintain the certification due to changes in the certified services (reduction, expansion, etc.), or there is some sort of M&A of the services and the institutions which acquired the certification, the institution which acquired the certification must notify the matters to the Accountability Agent.
- ③ The institutions which acquired the certification and the Accountability Agent may carry out compliance review assessment by mutual agreement.
- ④ For compliance review assessment, the Accountability Agent can regularly check for any changes in the service environment, transfer of business and addition of new services as well as discontinuation of existing services within the certification scope of the institution which acquired certification, and carry out the website online monitoring and remote investigation on technical vulnerabilities by mutual agreement with the Certification Applicant.

7. Certification Applicant should describe the review process to be used in the event of a suspected breach of the program requirements described in 5(a)-(d) of Annex A.

According to KISA' APEC CBPRs operating system (draft), if the Certification Applicant does not cooperate with the assessment, is not prepared for the assessment or failed to take the supplementary measures demanded by the review result, we may stop the assessment. Also, if the certification was acquired illegally, or supplementary measures are not taken, certification may be canceled.

- ※ **CBPRs operating system (draft) Article 22 (Cessation of assessment)** ① The Accountability Agent may stop certification assessment in any of the following events:
1. in the event that the Certification Applicant intentionally delays or interferes with certification assessment, or it is deemed to be difficult to carry on certification assessment due to a reason attributable to the Certification Applicant
  2. in the event that the materials submitted by the Certification Applicant were reviewed, and it is difficult to say that it is ready for certification
  3. in the event that the corrective measures pursuant to Paragraph 4 of Article 21 are not taken within up to 90 days (including 60 days for the corrective measures) after certification assessment
  4. in the event that it is deemed to be impossible to carry on certification assessment due to natural disasters and changes in the business environment
- ② If the Accountability Agent stops certification assessment in accordance with Paragraph 1, it must notify the reason in writing to the Certification Applicant
- ③ If the reason for the cessation of certification assessment in Paragraph 1 is removed, or according to the result of the objection raised pursuant to Article 28, the Accountability Agent may resume or terminate certification assessment.

**Article 27 (Cancellation of certification)** ① In any of the following events, the Accountability Agent may cancel the certification after the deliberation and voting of the certification committee:

1. In the event that the certification was acquired by false or illegal means,

2. In the event that the certification criteria mentioned in Paragraph 1 of Article 20 are not met,
3. In the event that the institution which acquired certification failed to receive the compliance review assessment pursuant to Paragraph 1 of Article 25, or re-certification assessment pursuant to Paragraph 1 of Article 26, or take corrective measures pursuant to Paragraph 4 of Article 21,
4. In the event that the institution which acquired certification failed to take the necessary measures pursuant to Paragraph 4 of Article 29,
5. In the event that the institution which acquired certification refuses or interferes with the compliance review assessment or re-certification assessment pursuant to Article 25 and Article 26.

## 5 Re-Certification and Annual Attestation

8. Certification Applicant should describe their re-certification and review process as identified in 8 (a)-(d) of Annex A.

To maintain the participants' certificates according to KISA's APEC CBPRS operating system (draft), application for re-certification must be made at least three months prior to the expiration of the term of validity, and if the term of validity expires, certification will not be valid anymore. The re-certification process is the same as the certification process.

- ※ **CBPRs operating system (draft) Article 26 (Re-certification assessment)**
- ① The institution which acquired certification must apply for re-certification at least three months prior to the expiration of the term of validity of the certificate.
  - ② Re-certification assessment will be done in accordance with Chapters 5 and 6.
  - ③ If the institution which acquired certification fails to apply for re-certification pursuant to Paragraph 1, and the term of validity of the certification expired, the certification will become invalid.

## 6 Dispute Resolution Process

9. Certification Applicant should describe the mechanism to receive and investigate complaints and describe the mechanism for cooperation with other APEC recognized Accountability Agents that may be used when appropriate.
10. Certification Applicant should describe how the dispute resolution process meets the requirements identified in 10 (a) – (h) of Annex A, whether supplied directly by itself or by a third party under contract (and identify the third party supplier of such services if applicable and how it meets the conflict of interest requirements identified in sections 1-3 of Annex A) as well as its process to submit the required information in Annexes D and E.

According to KISA's APEC CBPRs operating system (draft), if there are complaints related to



the CBPRs, individuals can report them to Accountability Agent and those Accountability Agent may investigate the facts of the complaints and take corrective actions against the nonconformities, and if any of the participants to not comply with such request, the Accountability Agent can cancel the certification. Also, Accountability Agent must regularly publish a case note of CBPRs-related complaints and statistics every year.

Also, KISA discloses the number of personal infringement cases and counseling services it rendered, and statistics by type and annual statistics on a continuing basis which are available for review at all times on the national information disclosure website ([www.index.go.kr/](http://www.index.go.kr/) only in Korean), and discloses cases of key civil complaint handling on the personal information protection portal run by the government ([https://www.privacy.go.kr/eng/remedy\\_01.do](https://www.privacy.go.kr/eng/remedy_01.do)).

- ※ **CBPRs operating system (draft) Article 29 (Handling complaints related to personal information, etc.)** ① If APEC member economies or service users who acquired certification have any complaints related to personal information against the institutions which acquired certification, they may report the complaints to the Accountability Agent.
- ② When receiving complaints, the Accountability Agent will review whether they fall within the scope of CBPRs compliance of the institution which acquired certification, and if so, will notify the matter to the complainant in writing or electronic documents, and investigate the facts.
- ③ If the Accountability Agent needs to provide personal information to a third party as a part of the process of handling the complaints, it must obtain the prior consent of the user.
- ④ If the Accountability Agent confirms that the institution which acquired certification does not meet the CBPRs criteria, it may request corrective measures, and if the institution which acquired certification fails to take such measures, it may cancel certification in accordance with Paragraph 1 of Article 27.
- ⑤ The Accountability Agent will notify the results of the handling of the complaints to the complainant and the institution which acquired certification in writing or electronic documents.
- ⑥ The Accountability Agent will collect statistical data on the handling of the complaints related to personal information and issue the complaint cases report to APEC member economies and users on an annual basis.

KISA operates a Personal Information Infringement Report Center which handles complaints related to personal information, and handles complaints in accordance with the 'Complaints and Report Handling Rules'. These rules specifically stipulate the procedure for receiving and handling complaints, the related standards involved, the time period involved, the investigation method and the management of the results of the handling of the complaints.

Complaints handling procedure: Complainants may report complaints via phone, e-mail and/or postal mail, and the center will notify the receipt of the complaints to the complainees. The center may conduct interviews to check the facts about what was reported, collect evidence and investigate related sites, and recommend the complainees to take improvement measures or give a disciplinary warning to them depending on the results of the fact-finding. And if there is a serious violation of any law, the center will notify the relevant agencies, and also

notify the results of the handling of the complaints in writing to the complainants and the complainees.

※ **Rules on processing complaints Article 7 (Filing of complaints, etc.)** ① The complainant may file consultation complaints by phone, postal mail, e-mail or fax or via the KISA website.

② To file a civil petition for grievance, the complainant may submit the application by fax or via the KISA website as well. In an emergency or if there are special circumstances, however, the complainant may submit the application orally or on the phone.

**Article 12 (Notification of receipt)** ① If the person in charge of handling complaints receives a civil petition for a grievance, he/she must notify it to the complainee in writing or electronic documents.

② In any of the following events, he/she need not notify it to the complainant or the complainee:

1. In the event that the civil complaint is simply a report on the complainee's violation of a law,
2. In the event that it is possible to view the received civil complaint on the KISA website.

**Article 13 (Verifying facts)** ① The person in charge of handling complaints will verify the facts about the civil petition for grievance using any of the following methods:

1. Listening to the statement of the complainant or the complainee
2. Collecting evidential materials from the complainant or the complainee
3. Listening to the advice of an expert or the statement of a testifier
4. Photographing or other appropriate methods
5. Requesting the submission of materials according to related laws
6. On-site inspection pursuant to related laws

② If it is necessary to verify facts, the person in charge of handling complaints may request the complainee to submit materials, such as documents and articles related to the complaint.

③ To ensure appropriate on-site inspection pursuant to Subparagraph 6 of Paragraph 1, the head of the complaints handling department must prepare the specific requirements for on-site inspection, e.g. the criteria for selecting inspection targets and the inspection procedure and method.

**Article 15 (Measures taken with regard to the result of verifying facts)** ① After verifying the facts concerning the civil complaint, the team leader may recommend that the complainee make improvements so that the complainant's grievance can be resolved quickly.

② If the complainee's violation of law falls under any of the following, the team leader may recommend a warning to the complainee for prevention of recurrence.

1. In the event that the complainee's violation of law is minor, and the complainee took a corrective measure against the violation,
2. In the event that the complainee violated a law only once, and the notification of the violation of laws is useless as the complainee took measures to resolve the complainant's claim,
3. In the event that the complaints handling criteria, prepared in order to appropriately handle the civil petition for grievance, are applied.

③ If the complainee's violation of law is serious except for the cases stipulated in Paragraphs 1 and 2, the team leader will send the fact verification result report and related evidential materials to related departments.

④ If it was reported that the complainee, who was cautioned to prevent recurrence in accordance with Paragraph 2, was involved in the same kind of incident, and his/her violation of law was confirmed, Paragraph 3 will be applied.

**Article 17 (Notification of results, etc.)** ① The person in charge of handling complaints must notify the results of the handling of the complaints to the complainant and the complainee.

② He/she may notify the results by phone, telex or fax and via the KISA website.

② If it is possible to view the results of the handling of the complaints via the KISA website, he/she will notify it to the complainant or the complainee in advance, and may skip notification of the results of the handling of the complaints.

Protection of complainants : In order to protect complainants, the center should make an effort not to disclose complainants's personal information and person handling complaint needs to sign on the written pledge regarding this.

※ **Rules on processing complaints Article 23 (Protecting the information of the complainant, etc.)**

① The head of the complaints handling department must make efforts to ensure that the information and personal information acquired in relation to handling complaints is not leaked, or infringe on the rights of the complainant, etc.

② The department, which received complaints that especially require that the complainant, etc. be protected, may use false/substitute names for the complainant, etc. or render the complainant anonymous, etc. In this case, it must be clearly stated that the complainant, etc. was rendered anonymous or false/substitute names were used for them.

**Article 24 (Confidentiality, etc.)** ① The person in charge of handling complaints should not leak the progress or results of the handling of the complaints or any personal information or secrets acquired in the course of carrying out any duties without a valid reason, or use them for purposes other than the proper conduct of business. <Amended July 21, 2016>

② The person in charge of handling complaints must write a pledge in relation to Paragraph 1.

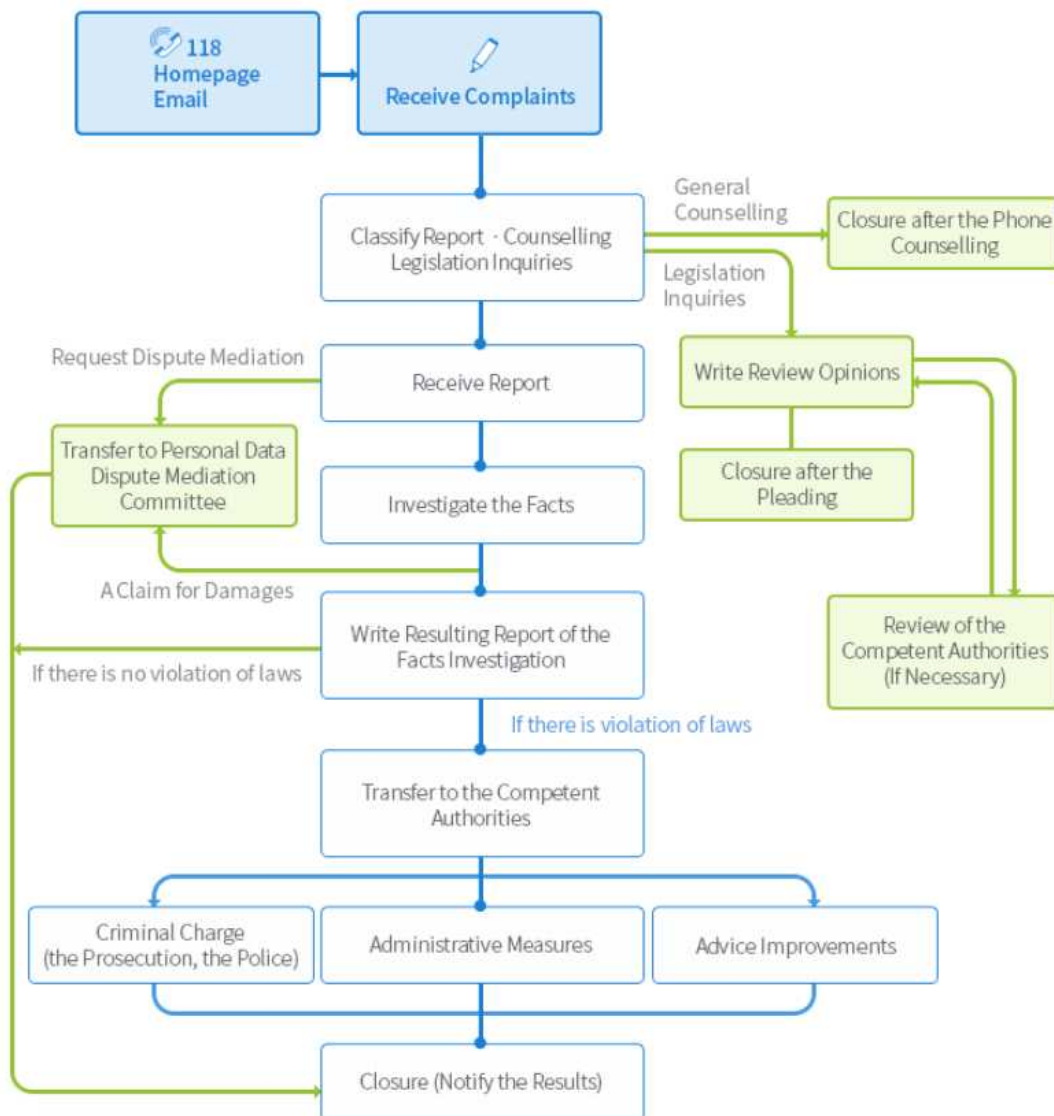
Complaint Statistics and Case notes : The person in charge of complaints should make report on complaint statistics and KISA may make public the result of complaint in order to prevent similar harm, to the extent that the complainants's personal information is not disclosed.

※ **Rules on processing complaints Article 5 (Designation of the person in charge of handling complaints)** ①

The head of the complaints handling department must designate the person in charge of handling complaints and manage the handling of complaints and related statistical data.

**Article 23 (Protecting the information of the complainant, etc.)** ③ To further prevent damages related to complaints, and help establish healthy use of information, KISA may summarize and disclose the results of the handling of the complaints to the extent that the identities and secrets of the persons involved are not disclosed.

## <Personal Data Infringement Procedure>



### 7 Mechanism for Enforcing Program Requirements

11. Certification Applicant should provide an explanation of its authority to enforce its program requirements against participants.

According to KISA's APEC CBPRs operating system (draft), if the certification was acquired illegally, or supplementary measures had not been taken, or no corrective actions taken with regard to the complaints, and compliance review is refused, certification may be canceled.

※ CBPRs operating system (draft) Article 27 (Cancellation of certification) ① In any of the following events, the

Accountability Agent may cancel the certification after the deliberation and voting of the certification committee:

1. In the event that the certification was acquired by false or illegal means,
2. In the event that the certification criteria mentioned in Paragraph 1 of Article 20 are not met,
3. In the event that the institution which acquired certification failed to receive the compliance review assessment pursuant to Paragraph 1 of Article 25, or re-certification assessment pursuant to Paragraph 1 of Article 26, or take corrective measures pursuant to Paragraph 4 of Article 21,
4. In the event that the institution which acquired certification failed to take the necessary measures pursuant to Paragraph 4 of Article 29,
5. In the event that the institution which acquired certification refuses or interferes with the compliance review assessment or re-certification assessment pursuant to Article 25 and Article 26.

12. Certification Applicant should describe the policies and procedures for notifying a participant of non-compliance with Applicant's program requirements and provide a description of the processes in place to ensure the participant remedy the non-compliance.
13. Certification Applicant should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e) of Annex A.

According to KISA's APEC CBPRs operating system (draft), if supplementary/corrective measures are not performed against non-compliance verified through compliance review, re-certification and reported complaints, certification may be canceled after the certification committee's review and decision, and if participants have an objection to it, they may raise an objection within the specified period of time.

- ※ **CBPRs operating system (draft) Article 28 (Objection)** ① If the Certification Applicant or the institution which acquired certification has any objection to the results of the certification assessment or the cancellation of certification, it must raise an objection to the Accountability Agent within 15 days after the results were notified.
- ② If the objection pursuant to Paragraph 1 is deemed to be reasonable, the Accountability Agent may request the certification committee to conduct assessment again.
- ③ The Accountability Agent must notify the results of the handling of the objections in writing to the Certification Applicant or the institution which acquired certification.

14. Certification Applicant should describe its policies and procedures for referring matters to the appropriate public authority or enforcement agency for review and possible law enforcement action. [NOTE: immediate notification of violations may be appropriate in some instances].

The Korea Communications Commission and the Ministry of the Interior and Safety regulate the 'Act on Promotion of Information and Communications Network Utilization and

Information Protection, Etc.’ and the ‘Personal Information Protection Act’, approved by the CBPRs, respectively, and KISA is the key public agency supporting the privacy policy studies and proliferation of technologies of the two ministries (see checklist No. 1). CBPRs non-compliance falls into the violation of the above two laws related to personal information protection. In such a case, KISA quickly notifies the offenders of the seriousness of their violation and consults with the two authorities mentioned above through constant collaboration with them.

See the Dispute Resolution Process in checklists No. 9 and 10 for information on the procedure for transferring complaints reported to KISA to relevant authorities.

※ **CBPRs operating system (draft) Article 30 (Certification criteria execution system)** ① If the institutions which acquired certification among the targets of certification cancellation pursuant to Article 27 or Paragraph 4 of Article 29 are believed to have seriously violated laws or intentionally violated laws, the Accountability Agent may notify them to the Korea Communications Commission or the Ministry of the Interior and Safety or other relevant authorities.

15. Certification Applicant should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.

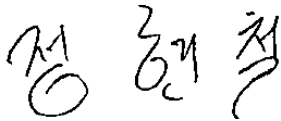
According to KISA’s APEC CBPRs operating system (draft), KISA will cooperate with overseas law-enforcement agencies or Accountability Agent to handle complaints or jointly enforce laws.

※ **CBPRs operating system (draft) Article 30 (Certification criteria execution system)** ② The Accountability Agent will cooperate with the law-enforcement agencies or Accountability Agent of foreign economies which joined the CBPRs in terms of handling complaints or enforcement of laws.

Annex C

**SIGNATURE AND CONTACT INFORMATION**

By signing this document, the signing party attests to the truth of the answers given.



Jeong Hyun-Cheol

December 14, 2017

[title] **Vice President**

[name of organization] **Korea Internet & Security Agency**

[Address of organization] **9, Jinheung-gil, Naju-si, Jeollanam-do, Korea, 58324**

[Email address] **hcjeong@kisa.or.kr**

[Telephone number] **82-61-820-1800**

The first APEC recognition for an Accountability Agent is limited to one year from the date of recognition. Recognition for the same Accountability Agent will be for two years thereafter. One month prior to the end of the recognition period, the Accountability Agent must resubmit this form and any associated documentation to the appropriate government agency or public authority or as soon as practicable in the event of a material change (e.g. ownership, structure, policies).

***NOTE: Failure to comply with any of the requirements outlined in this document may result in appropriate sanctions under applicable domestic law.***