NCC Group Security Services, Inc.

Risk Management & Governance

CBPR and PRP Program Details (Recertification)

February 09, 2023, Version 1.0

650 California Street, Suite 2950

San Francisco, CA 94108

www.nccgroup.trust/us/

February 9, 2023

Neema Guliani, Deputy Assistant Secretary for Services

Krysten Jenci, Director, Office of Digital Services Industries

Shannon Coe, Director Global Data Policy

International Trade Administration, U.S. Department of Commerce

1401 Constitution Ave. NW, Room 4324

Washington, DC 20230

Re: Recertification of APEC CBPR and PRP Accountability Agent Application (via EMAIL)

NCC Group Security Services, Inc. is proud to have the opportunity to submit its recertification application to continue to be an Accountability Agent under the APEC Cross Border Privacy Rules (CBPR) System and the APEC Privacy Rules for Processors (PRP) System.

NCC Group Plc was originally formed in June 1999, when the National Computing Centre sold its commercial division to its existing management team. The company was admitted to trading on AIM on July 12, 2004. NCC Group Plc made a move to the London Stock Exchange's main market in July 2007. iSEC Partners Inc, a leading US-based security testing services provider joined the Group in 2010. iSEC Partners, Inc. changed their name June 1, 2015 to NCC Group Security Services, Inc., a For Nevada Profit Corporation. NCC Group Security Services, Inc. (will be referenced throughout this document as "NCC Group") offers a number of different security services, including a dedicated team of professionals that perform compliance and audit related services through its Risk Management and Governance (RMG) Division located in the United States. As a for-profit corporate entity of the US, NCC Group is under the direct regulatory enforcement authority of the United States Federal Trade Commission (FTC). The FTC is the APEC regulatory enforcement authority for the United States.

To complete the recertification application process as required to maintain the APEC CBPR and PRP Accountability Agent status and to continue to perform CBPR and PRP certification functions under the APEC CBPR and PRP System Programs, NCC Group intends to demonstrate its continued fulfillment of the requirements by addressing the Accountability Agent Recognition Criteria outlined in Annex A of the APEC Accountability Agent Application utilizing the Accountability Agent Recognition Criteria Checklist found in Annex B. NCC Group provides responses to continue to meet the requirements of each of the following criteria items [Note: Respective documentation and evidence to support the responses are provided accordingly.]:

- Conflicts of Interest
- Program Requirements
- Certification Process
- On-going Monitoring and Compliance Review Process
- Re-Certification and Annual Attestation
- Dispute Resolution Process
- Mechanisms for Enforcing Program Requirements

Please accept this recertification application packet to recognize NCC Group as maintaining its Accountability Agent status under the CBPR and PRP Systems. For additional information or any questions, please contact Kurt Osburn, Practice Director at Kurt.Osburn@nccgroup.com.

Sincerely,

Nick Rowe, Chief Operating Officer, US

1 CBPR/PRP PROGRAM/ACCOUNTABILITY AGENT RECOGNITION CRITERIA

1.1 Program Contacts

Program Owners

Name	Title	E-mail	Phone
Mike Zhang	Manager	M.Zhang@nccgroup.com	402-630-6029
Kurt Osburn	Practice Director	Kurt.Osburn@nccgoup.com	205-907-7607
Joe Meyer	Global Deputy Lead, Compliance	Joseph.Meyer@nccgroup.com	402-680-9649

1.2 Conflicts of Interest

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

NCC Group Security Services, Inc. ("NCC Group") performs compliance and audit related services through its Risk Management and Governance (RMG) Division located in the United States. Members of NCC Group's RMG team maintain multiple industry recognized certifications such as CISSP, CISM, CISA, CIPP, Senior ISO Lead Auditor/Implementer, and HITRUST CCSFP/CHQP. NCC Group is an approved assessor firm for HITRUST, approved FedRAMP 3PAO Assessor, and preferred assessor for SECURETexas. Through these affiliations and to maintain required credentials, NCC Group and its assessors must adhere to strict codes of ethics, objectivity, and integrity when performing assessment services. This includes ensuring assessments are performed without any conflict of interests.

NCC Group takes certification very seriously and only provides its certification marks to organizations demonstrating full compliance with all requirements. Authorizing the use of NCC Group's CBPR or PRP certification mark to an organization not meeting all certification program requirements could lead NCC Group to a claim by the Federal Trade Commission (FTC) under section 5(a) of the Federal Trade Commission Act (FTC Act) (15 USC § 45) reference to "unfair or deceptive acts or practices in or affecting commerce".

NCC Group could take other actions under our commitment as a CBPR and PRP Accountability Agent such as notifying a foreign regulator in the case of a foreign organization utilizing our seal. NCC Group will assist the Joint Oversight Panel (JOP) or other economy in their efforts in obtaining information or investigations as necessary pertaining to the CBPR and PRP programs.

NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs. [As of the date of this recertification application, there has been no material changes to written policies and documentation.]

Supporting Evidence

- Conflicts of Interest Policy is included under Section 2 of this document.
- NCC Group is an approved HITRUST CSF Assessor abiding by HITRUST CSF Assurance Requirements that require separation of duties when performing assessments. See list of approved assessor firms here: https://hitrustalliance.net/csf-assessors/
    - Founded in 2007, the HITRUST Alliance is a not for profit organization with the goal to assist the healthcare industry in the protection of their information. The HITRUST Alliance develops and maintains the HITRUST CSF, a framework that encompasses a multitude of regulations and standards to assist organizations with their security posture. HITRUST Alliance validates and certifies organizations on its HITRUST CSF through its assurance program utilizing approved assessors to perform assurance services. HITRUST Alliance required approved assessors to maintain certain requirements to participate in validating organizations to include

having experienced and trained assessors on staff, maintaining ethics and conflicts of interest, and ensuring a high level of quality of services.

- NCC Group is an Accredited FedRAMP 3PAO organization abiding by conflict of interest requirements when performing assessments. See list of currently accredited organizations here: https://customer.a2la.org/index.cfm?event=directory.detail&labPID=25C8EA8E-BE8D-4DBA-A107-3A140B661D12

Screenshot of FedRAMP 3PAO Accreditation

  - *The Federal Risk and Authorization Management Program (FedRAMP) is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. A Third Party Assessment Organization (3PAO) is a certified organization that helps cloud service providers meet FedRAMP compliance requirements. A 3PAO must be accredited by the American Association for Laboratory Accreditation (A2LA) that follows the ISO/IEC 17020:2012 Requirements for the Operation of Various Types of Bodies Performing Inspection. To qualify as a 3PAO, an organization must have an independence and quality management system in place in accordance with the ISO/IEC 17020 standards, information assurance competence that includes FISMA experience and testing of security controls, and competence in the security assessment of cloud-based information systems.*

- *NCC Group is a SECURETexas Preferred Vendor that must abide by conflict of interest requirements when performing assessments. See list of SECURETexas Preferred vendors here: https://www.thsa.org/privacy-security-certification/securetexas-preferred-vendors/*
  - *The Texas Health Services Authority (THSA) was formed under the Texas Health and Safety Code Chapter 182 to promote, implement, and facilitate the secure electronic exchange of health information in the State of Texas. THSA accomplishes this through its state-level health information exchange, privacy and security certification, and supporting programs. THSA partners with multiple vendors to assist with the SECURETexas certifications.*

Checklist Item #2. Applicant Accountability Agent 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.

NCC Group will refrain from any potential or actual conflicts of interests identified in 2(b) of Annex A as addressed under the Introduction of the Conflicts of Interest Policy. "NCC Group expects that its colleagues, at all levels, perform their duties in a fair and unbiased way, and that the decisions they make are not affected by self-interest, private affiliations or the likelihood that they, or those close to them, will gain or lose financially or otherwise. The perception that a conflicting interest has influenced an outcome or a decision can undermine confidence in the integrity of the company and the employee. If left unresolved, some conflicts can result in reputational damage or even legal action, so it is crucial that we seek to recognize the associated risks and put measures in place to identify and manage conflicts as they arise."

Conflict of interests would be in violation of these prohibited acts subjecting an employee to disciplinary actions up to and including termination.

If it is determined a board member or person in leadership of NCC Group also sits on the board or holds financial interest (beyond common stock) in a company requesting CBPR or PRP Certification, NCC Group will excuse itself from performing such certification and refer the organization to another recognized accountability agent. NCC Group will notify the JOP accordingly to this matter.

In addition, according to the NCC Group North America Employee Handbook under Outside Employment, "While employed by NCC Group, employees are expected to devote their energies to their jobs with NCC Group… The Following type of outside employment are strictly prohibited: Employment that creates a conflict of interest or is incompatible with the employee's employment with NCC Group."

Finally, NCC Group abides by an Anti-Corruption Policy provided in the NCC Group North America Employee Handbook indicating NCC Group has a zero tolerance position in relation to corruption and/or bribery, wherever and in whatever form encountered. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Conflicts of Interest Policy is included under Section 2 of this document.
- NCC Group prohibited conduct:

38. Committing a fraudulent act or a breach of trust under any circumstances.

39. Engaging in any conduct that is not in the best interest of NCC Group.

Snippet of the Employee Handbook under Other Prohibited Conduct Section

- NCC Group outside employment restrictions:

C. OUTSIDE EMPLOYMENT

While employed by NCC Group, employees are expected to devote their energies to their jobs with NCC Group. For this reason, second jobs are strongly discouraged. The following types of outside employment are strictly prohibited:

1. Employment that conflicts with an employee's work schedule, duties and responsibilities;
2. Employment that creates a conflict of interest or is incompatible with the employee's employment with NCC Group;
3. Employment that interferes with the protection of NCC Group's proprietary or confidential information;
4. Employment that impairs or has a detrimental effect on the employee's work performance with
5. Employment that requires the employee to conduct work or related activities for outside employment on NCC Group's property during the employee's working hours or using NCC Group's facilities and/or equipment in relation to the employee's outside employment;
6. Employment that directly or indirectly competes with the business or the interests of the employer.

Employees who wish to engage in outside employment must submit a written request to NCC Group explaining the details of the outside employment. If the outside employment is authorized, NCC Group assumes no responsibility for the outside employment. No work related to an employee's outside employment may be performed during NCC Group time, with NCC Group property or equipment, or on NCC Group premises. NCC Group shall not provide workers' compensation coverage or any other benefit for injuries occurring from or arising out of outside employment. Authorization to engage in outside employment can be revoked at any time.

Snippet of the Employee Handbook under Outside Employment Section

- NCC Group's Anti-Corruption Policy:

H. ANTI-CORRUPTION POLICY

NCC Group is committed to ensuring it carries out business fairly, honestly and openly. Not only is the prevention of corruption a moral issue but it is also a legal requirement. Breaches of the anti-corruption laws in place in the country where NCC Group operates can lead to unlimited fines for NCC Group and imprisonment for individuals, as well as endangering the NCC Group's reputation.

In light of the above, NCC Group has a zero tolerance position in relation to corruption and/or bribery, wherever and in whatever form that may be encountered.

This policy should be read in conjunction with the Gifts Policy and Open Door Policy for employees, each of which can be located in this handbook, and can be requested in a hard copy by any interested parties.

NCC Group employees and agents are prohibited from offering, promising, authorizing the payment of or paying or providing anything of value to any employee, agent, or representative of another company to induce or reward the improper performance of any function or any business-related activity.

The most prevalent forms of bribery stem from:

- Payments to a company's employees or their relatives, or to those of a third party, to secure advantage in business transactions;
- Political contributions made to secure advantage in business transactions
- Charitable sponsorships used to secure advantage in business transactions
- Facilitation payments or kickbacks made to secure or accelerate routine or necessary business actions.
- Gifts, hospitality and expenses payments made to secure advantage in business transactions

Employees, directors and associated persons must never:

- Participate in any form of corrupt behavior
- Use company funds, in the form of payments or gifts and hospitality for any unlawful, unethical or improper purpose
- Authorize, make, tolerate or encourage, invite or accept, any improper payments to obtain, retain or improve business
- Engage in any activity that might create a conflict of interest for NCC Group
- Permit anyone to offer or pay bribes or make facilitation payments on NCC Group's behalf, or do anything else NCC Group would not be permitted to do itself.
- Offer or give anything of value to a public official to induce or reward them for acting improperly in the course of their public responsibilities.

It is the responsibility of each employee to ensure compliance with the terms of this policy. If any employee believes that the terms of this policy are not being correctly adhered to then they must raise any concerns with their line manager or in accordance with the terms of NCC Group's Open Door Policy for employees. Under the terms of NCC Group's Open Door Policy, employees are encouraged, without fear of retaliation, to raise any concerns they may have regarding the conduct of NCC Group's business in order that such concerns may be properly investigated.

Snippet of the Employee Handbook under Anti-Corruption Policy Section

G. BUSINESS CONDUCT AND ETHICS

No employee may accept nor extend a gift or gratuity valued in excess of $200.00 from or to any customer, vendor, supplier, or other person doing business with the Company. Please discuss expenses paid or extended to such persons for business meals or trips with the Company in advance. In no event may a gift, gratuity, or expense payment influence a business decision, transaction, or service.

Receiving hospitality:

An employee may occasionally accept hospitality, for example meals, theatre/music/sports events, from a client or vendor provided that the following procedure is followed:

- The employee must first obtain authorization from their line manager before accepting the hospitality and an authorization form must be completed and signed by both the employee and the employee's line manager. HR can provide this form. Authorization for business lunches or dinners is not required if the value of such lunch or dinner is less than $200 per person.
- The purpose of the hospitality must be to hold a bona fide business discussion or to develop better business relations.
- Employees or personnel from the vendor or client must be present at the event.

Hospitality must be politely refused if:

- It could be considered over and above the usual course of business by a reasonable person (i.e. holidays, short breaks, overseas travel) or is lavish, extravagant or disproportionate to the type of business dealing to which it relates.
- Tender or contractual negotiations are on-going with the vendor or client in question.
- The acceptance or offer of the entertainment could be interpreted as a reward, inducement or encouragement for a favor or preferential treatment.

Offering gifts and hospitality:

NCC Group does not permit employees to offer gifts to vendors or clients and an employee must obtain his/her line manager's consent prior to sending any gift by completing an authorization form. In determining whether the giving of a gift is appropriate, the line manager will consider who the recipient is, the value of the gift and the reason for giving it.

Reasonable hospitality may be offered to any vendors or clients provided always that:

- Authorization is first sought by the employee's line manager by completing the authorization form - authorization is not required for business lunches or dinners where the value of such lunch or dinner is less than $200 per person.
- The offer of entertainment could not be interpreted as a reward, inducement or encouragement for a favor or preferential treatment.

A copy of any completed authorization forms must be sent to the HR Manager or a member of the HR team.

Breach of policy:

Any breach of the gifts policy will be regarded as misconduct, leading to disciplinary action up to and including termination.

Note that the gifts policy set out above, in so far as it exceeds any statutory requirement, does not form part of your contract of employment and may be changed by the Company in its absolute discretion at any time.

Snippet of the Employee Handbook under Business Conduct and Ethics Section

Checklist Item #3. Applicant Accountability Agent should describe the disclosure/withdrawal mechanisms to be used in the event of any actual conflict of interest identified.

The disclosure/withdrawal mechanism in place at NCC Group in the event of any actual conflict of interest is covered under the Conflicts of Interest Policy in Section 2 as well as discussed previously under criteria 1 and 2 above. In basic terms, if NCC Group determines there to be a conflict of interest, it will withdraw from performing any

certification or on-going participation activities. Any conflict or potential conflict of interest will be reported to the Joint Oversight Panel (JOP) as required. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Conflicts of Interest Policy is included under Section 2 of this document.

1.3 Program Requirements

Checklist Item #4. Applicant Accountability Agent 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.

NCC Group will utilize all relevant template documentation developed by APEC to include the CBPR and PRP Intake Questionnaire, the CBPR and PRP Program Requirements, CBPR and PRP Program Requirements Map, and more specifically requirements detailed in Annex C to perform the certification. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Program Requirements is included under Section 3 of this document.
- Publicly available documentation on NCC Group's website: https://www.nccgroup.com/us/what-is-the-apec-cbpr/

1.4 Certification Process

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

NCC Group has a comprehensive process to review an Applicant organization's policies and practices with respect to the Applicant organization's participation in the CBPR or PRP systems in order to verify compliance with NCC Group's program requirements. NCC Group follows its SMARTS Assessment process for Certification detailed in Section 4 Certification Process. SMARTS stands for scope, map, analyze, review, test, and submit. There are specific tasks and activities within each of these areas to perform the certification. NCC Group will utilize the CBPR or PRP Intake Questionnaire as the self-assessment form completed by the Applicant organization. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Certification Process is included under Section 4 of this document.

1.5 On-going Monitoring and Compliance Review Processes

Checklist Item #6. Applicant Accountability Agent 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).

NCC Group maintains written procedures to ensure integrity of the certification process as described under Section 4 Certification Process and to monitor the participant's compliance with the program requirements under Section 5 On-going Monitoring and Compliance Review Processes.

After the initial assessment, content of the self-assessment form will be verified to include examining evidence, performing interviews analyzed against documented policies/procedures, and testing/sampling activities such as observations of systems, scans of websites, and use of manual and automated tools to validate the effectiveness of control implementation. NCC Group will continue on-going monitoring of the Participant organization throughout the certification period. This on-going monitoring can include, but not limited to, technical testing (utilizing commercially available and proprietary manual/automatic tools), website reviews, random audits, and investigation of any reported

violations obtained through the complaint/dispute resolution process, via news reports, or other direct reports for any Participant organization carrying the NCC Group CBPR or PRP certification mark. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Certification Process is included under Section 4 of this document.
- On-going Monitoring and Compliance Review Processes under Section 5 of this document.
- Dispute Resolution Process under Section 7 of this document.

Checklist Item #7. Applicant Accountability Agent 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.

Upon a report of non-conformity or suspected breach of a Participant organization, NCC Group will conduct an investigation including a formal audit of compliance as described in Section 5.3 Investigation Process. Non-conformity or suspected breaches may be reported to NCC Group through public announcements, on-going monitoring activities/reviews, or directly through the Dispute Resolution Process described in Section 7.

Where non-compliance with any of the program requirements is identified, NCC Group will notify the Participant organization outlining the corrections the participant needs to make. An investigation can result in one of the following:

- Resolution Agreement between the Participant organization and NCC Group to resolve the non-conformity in a specified amount of time. NCC Group will validate that the issue has been resolved.
- Suspension/Withdrawal of Certification where non-conformities are not resolved in the specified time. NCC Group will inform the JOP at this point.
- Report to FTC in extreme cases or where otherwise deemed appropriate where non-conformities result in the need to report non-compliance issues to the US enforcement authority.

NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Investigation Process is included under Section 5.3 of this document.
- Dispute Resolution Process under Section 7 of this document.

1.6 Re-Certification and Annual Attestation

Checklist Item #8. Applicant Accountability Agent should describe their re-certification and review process as identified in 8 (a)-(d) of Annex A.

A Participant organization is required to recertify and attest on an annual basis their continued adherence to the CBPR or PRP program requirements. NCC Group will perform a recertification assessment on the Participant organization annually to ensure the Participant organization is meeting the APEC CBPR or APEC PRP Program requirements abiding by the procedures discussed in Section 6 Re-Certification and Annual Attestation and Section 4 Certification Process.

Participant organizations are required to notify NCC Group of any material changes to its privacy policies and/or in-scope environment OR if NCC Group discovers a material change through its on-going monitoring process prior to the annual re-certification/attestation, the change will be verified to be in compliance with the CBPR or PRP Program requirements.

NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Re-Certification and Annual Attestation under Section 6 of this document.
- Certification Process under Section 4 of this document.

1.7 Dispute Resolution Process

Checklist Item #9. Applicant Accountability Agent 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.

NCC Group has an existing Complaint and Dispute Resolution System in place mirroring the FedRAMP 3PAO requirements for dispute resolution addressed under Section 7 Dispute Resolution Process. NCC Group manages dispute resolutions in-house and does not contract with any external third-party service provider. NCC Group is committed to fully investigate and resolve complaints to the CBPR and PRP Certification process. The process implemented covers receiving complaints, notifying complainants, investigating complaints, notifying Participant organizations, obtaining consent, ensuring proper documentation along with maintaining statistics, and documenting/anonymizing case notes as required by the CBPR and PRP Certification program.

NCC Group recognizes proper complaint handling is an important element to the CBPR and PRP program in order to promote understanding of the programs, increase transparency, help identify trends, enable comparisons, and promote accountability along with building trust in Accountability Agents.

NCC Group intends to use best efforts within the limits of respective authority to cooperate with private sector organizations, self-regulatory bodies, non-participating Privacy Enforcement Authorities, and other Accountability Agents by abiding with the CPEA enforcement mechanisms related to enforcement of the APEC CBPR/PRP programs. NCC Group intends to refer complaints to organizational administrators or otherwise refer complaints as appropriate following procedures identified within the *APEC Cooperation Arrangement for Cross-Border Privacy Enforcement*.

NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Dispute Resolution Process under Section 7 of this document.
- APEC Cross-border Privacy Enforcement Arrangement (CPEA): https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx

Checklist Item #10. Applicant Accountability Agent 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.

NCC Group has an existing Complaint and Dispute Resolution System in place. The purpose of this process is to manage and progress complaints, audit non-conformities, non-conforming work, improvement suggestions, corrective actions, and preventive actions. This is to ensure issues are corrected as soon as practicable after they are discovered and ensure recurrences are minimized. It is also developed to ensure compliance with the CBPR and PRP Program requirements. The Complaint and Dispute Resolution System in place covers the following areas:

Receiving Complaints

NCC Group may receive complaints through multiple avenues such as contacting the Program Owners directly via email or by phone, complaints received through staff members, or complaints received through Corporate Help Desk support. If a verbal complaint is made, staff will request a written correspondence is sent by the complainant to the Privacy Practice Director. [As of the date of this recertification application, NCC Group has not received any complaints.]

Notifying Complainant of Determination

Complaints will be forwarded to the Privacy Practice Director for determination of whether the complaint concerns the Participant's obligations under the program and the complaint falls within the scope of the program requirements. [As of the date of this recertification application, NCC Group has not received any complaints.]

Investigating Complaints

NCC Group is committed to fully investigating and resolve complaints relating to the CBPR and PRP Certification Process. A detailed investigation process is described in Section 7.3 Investigating Complaints. [As of the date of this recertification application, NCC Group has not received any complaints.]

Resolving Complaints

After a formal and detailed investigation is completed, complaints will be resolved through resolution agreement, suspension/withdrawal of certification, or reported to the FTC as discussed in Section 5.3 Investigation Process. [As of the date of this recertification application, NCC Group has not received any complaints.]

Notification of Complaint Resolution

NCC Group will notify complainant and Participant organization of the resolution of any investigation unless they request otherwise. [As of the date of this recertification application, NCC Group has not received any complaints.]

Obtaining Individual's Consent

NCC Group will obtain an individual's consent before sharing individual's personal information with the relevant enforcement authority in connection with a request for assistance or complaint. This consent is obtained through a positive or negative response to the question of sharing the individual's personal information to resolve the request. [As of the date of this recertification application, NCC Group has not received any complaints.]

Complaint Statistics

NCC Group will make publicly available (on its website) statistics on the types of complaints received and the outcomes of the complaints. This information will be shared with relevant government agencies, the FTC, and the JOP. NCC Group will utilize the Complaint Statistics Template provided by the APEC CBPR and PRP programs. Complaint statistics must be reported to the JOP for publication on an annual basis. [As of the date of this recertification application, NCC Group has not received any complaints.]

Case Notes

NCC Group will release, in an anonymized fashion, Case Notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes. NCC Group will utilize the Case Note Template provided by the APEC CBPR and PRP programs. Case Notes must be reported to the JOP for publication on an annual basis. [As of the date of this recertification application, NCC Group has no Case Notes to report.]

NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Dispute Resolution Process under Section 7 of this document.
- Investigation Process under Section 5.3 of this document.
- CBPR Complaints under Section 7.6.1 of this document.
- PRP Complaints under Section 7.6.2 of this document.
- Case Notes under Section 7.7 of this document.

1.8 Mechanisms for Enforcing Program Requirements

Checklist Item #11. Applicant Accountability Agent should provide an explanation of its authority to enforce its program requirements against participants.

Applicants and Participant organizations must abide by NCC Group's Certification Program related to the CBPR and PRP certifications. These organizations must sign and agree to the terms and conditions set forth under NCC Group's Master Service Agreement (MSA) [See Appendix A for additional information] and Statement of Work (SoW) [See Appendix B for additional information]. Both the MSA and SoW identify that participants must comply with the applicable certification standards to include annual re-certification requirements, random audits, or investigations

into possible breaches or non-conformity complaints. Program requirements against Applicants and Participant organizations is enforced through contractual obligations.

NCC Group is a US for-profit corporation abiding by the Federal Trade Commission (FTC) regulatory authority. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Mechanisms for Enforcing Program Requirements under Section 8 of this document.
- Appendix A – Sample Master Service Agreement.
- Appendix B – Sample Statement of Work.

Checklist Item #12. Applicant Accountability Agent 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.

NCC Group must maintain a process to notify Participants immediately of non-compliance with NCC Program's requirements and for requiring Participant to remedy the non-compliance within thirty (30) days upon notification. See Section 7.4 Notifying Participant for additional information. Participants are required to communicate and maintain an active point of contact for the CBPR or PRP Certification program with NCC Group. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Mechanisms for Enforcing Program Requirements under Section 8 of this document.
- Notifying Participant under Section 7.4 of this document.

Checklist Item #13. Applicant Accountability Agent should describe the policies and procedures to impose any of the penalties identified in 13 (a) – (e) of Annex A.

NCC Group maintains policies and procedures in place to impose penalties proportional to harm (or potential harm) resulting from a violation of the CBPR or PRP Program requirements. Penalties may be assessed for participants failing to remedy non-compliance issues within a specified time as provided for under Section 5 On-going Monitoring and Compliance. Penalties may include requiring remediation through a resolution agreement, temporary suspension, removal from the program, publicizing non-compliance, reporting violations to the FTC (in circumstances where an identified issue violates law), and other penalties such as re-validation fees. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs.

Supporting Evidence

- Penalties under Section 8.1 of this document.
- On-going Monitoring and Compliance under Section 5 of this document.

Checklist Item #14. Applicant Accountability Agent 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].

If it is reasonably believed a Participating organization fails to comply with certification requirements, NCC Group will refer the matter to the appropriate public authority or enforcement agency (i.e. FTC) for review as well as possible law enforcement action where NCC Group has a reasonable belief a Participant organization's failure to comply with the APEC Cross-Border Privacy Rules (CBPR) System requirements has not been remedied within a reasonable time pursuant to NCC Group's established review process and procedures. See Section 7 Dispute Resolution Process for additional information. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs. [As of the date of this recertification application, NCC Group has made no reports to public authority or enforcement agencies.]

Supporting Evidence

- Penalties under Section 8.1 of this document.
- Dispute Resolution Process under Section 7 of this document.

Checklist Item #15. Applicant Accountability Agent should describe its policies and procedures to respond to requests from enforcement entities in APEC Economies where possible.

NCC Group will respond to requests from enforcement entities in APEC economies reasonably relating to the Economy and to the CBPR or PRP-related activities of NCC Group, where possible. NCC Group continues to meet the requirements for both the CBPR and PRP Certification programs. [As of the date of this recertification application, NCC Group has not received any requests for enforcement entities in APEC Economies.]

Supporting Evidence

- Enforcement Entity Requests under Section 8.2 of this document.

2 CONFLICTS OF INTEREST POLICY

2.1 General Requirements

NCC Group, as an Accountability Agent, will be free of any actual or potential conflicts of interests to perform its duties under the APEC Cross Border Privacy Rules (CBPR) System or the APEC Privacy Recognition for Processors (PRP) System. To this end, assessors assigned to performing tasks related to an Applicant or Participant organization's certification and ongoing participation in the CBPR or PRP System will be free from influences that would compromise their professional judgement, objectivity, and integrity.

Assessors assigned to APEC CBPR certification, APEC PRP certification, or ongoing participation tasks are required to be free of any conflicts of interests to include providing any previous sales, consulting, advisory, or technical security functions of an Applicant or Participant organization.

In addition, any assessor having any previous sales, consulting, advisory, or technical security roles/functions of an Applicant or Participant organization will not be assigned to any certification tasks or functions.

At no time may NCC Group have a direct or indirect affiliation with any Applicant or Participant organization prejudicing NCC Group's ability to render a fair decision with respect to the organization's certification and ongoing participation in the CBPR and PRP system. This includes, but not limited to:

- During the application review and initial certification process;
- During ongoing monitoring and compliance review;
- During re-certification and annual attestation; and
- During dispute resolution and enforcement of the Program Requirements against a participant.

Affiliations may include, but not be limited to, the Applicant or Participant organization and NCC Group being under common control such that the Applicant or Participant organization can exert undue influence on NCC Group. This relationship will constitute an automatic withdrawal.

The Assessors within NCC Group's RMG team will refrain from performing for its Applicants or Participant organizations services for a fee or any interest or benefit such as:

- Consulting or technical services related to the development or implementation of Applicant or Participant organization's data privacy practices and procedures;
- Consulting or technical services related to the development of its privacy policy or statement; or
- Consulting or technical services related to its security safeguards.

Services required to perform certification or on-going participation of an Applicant or Participant organization shall not be considered performing consulting services that may trigger a prohibition or conflict of interest.

2.1.1 Structural Safeguards

APEC CBPR Certification and APEC PRP Certification Team Members will be assigned from resources dedicated to the US Risk Management and Governance (RMG) Team. Within the RMG Group, the APEC CBPR Certification and APEC PRP Certification Teams fall under the Privacy Practice lead by a Director level manager. The Operations Management Group falls under the direction of the Global Operations Team. The Operations Management team is responsible for scheduling and managing projects. The Operations Management Team will ensure that certification team members assigned to any advisory or consulting engagements for an Applicant or Participant organization will not be assigned to certification duties or vice versa.

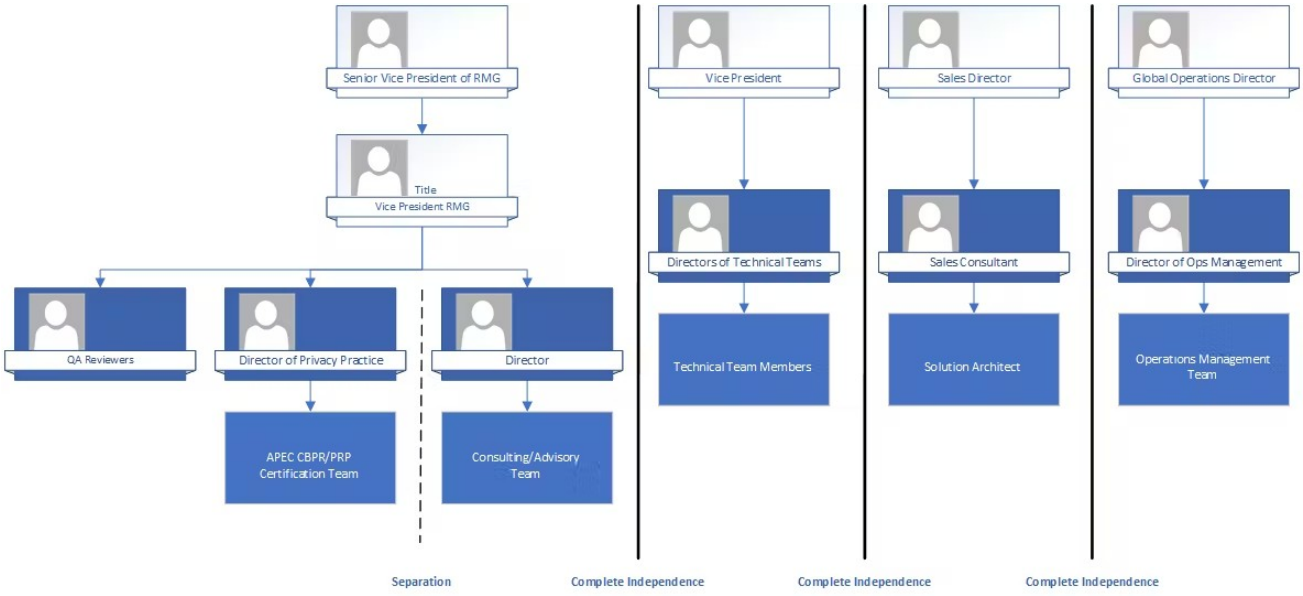
The Privacy Practice Director will review all assignments to an Applicant or Participating organization's certification in order to ensure there are no conflicts of interest. No official assignment of team members to a certification engagement will be performed until a review has been conducted by the Privacy Practice Director and approved by

the Privacy Practice Director. Any conflict of interests will be reported according to section *2.1.2 Reporting Conflict of Interests*.

The Senior Vice President will perform internal reviews of any potential conflicts of interest with Applicant and Participating organizations. Any conflict of interests will be reported according to section *2.1.2 Reporting Conflict of Interests*.

Technical services are provided to clients through a completely separate division within NCC Group. The technical services group reports up through a Vice President that has no direct reports through the RMG Team.

Separations of functions will be maintained at all times for resources handling privacy certification functions from resources handling sales and consulting functions.



Reporting Structure and Separation of Duties/Functions

2.1.2 Reporting Conflict of Interests

If a conflict of interest arises, team members must report the conflict to their respective Director or the Privacy Practice Director. A Director receiving a report of a conflict will report it to the Privacy Practice Director immediately. The Privacy Practice Director will withdraw from the engagement. The Practice Director will notify the Senior Vice President of RMG and the Sales Director in order to notify the Applicant or Participant organization of the conflict. NCC Group's legal team will also be notified of the conflict of interest.

Withdrawal of an engagement is automatic in cases where NCC Group is related to the Applicant or Participant organization to the extent the relationship gives rise to a risk of influence over the professional judgment, integrity, or objectivity of the certifying assessor.

NCC Group will notify the Joint Oversight Panel (JOP) for any Applicant or Participant organization NCC Group engages the organization in other consulting or technical services not related to the CBPR or PRP certification program. Where permitted, NCC Group will disclose the existence of the engagement and an explanation of the safeguards in place to ensure that NCC Group remains free of actual or potential conflicts of interest arising from the engagement such as segregating the personnel providing the consulting or technical services from the personnel performing the functions related to certification or on-going participation in the CBPR or PRP System.

Where permitted, NCC Group will also notify the Joint Oversight Panel (JOP) for any Applicant or Participant organization having previously engaged NCC Group in other consulting or technical services not related to the CBPR or PRP certification program. Where permitted, NCC Group will disclose the existence of the engagement and an explanation of the safeguards in place to ensure that NCC Group remains free of actual or potential conflicts of interest arising from the engagement such as segregating the personnel providing the consulting or technical

services from the personnel performing the functions related to certification or on-going participation in the CBPR or PRP System.

For affiliations cured by the existence of structural safeguards or other procedures taken by NCC Group, the existence of any such affiliations between NCC Group and the Applicant or Participant organization must be promptly disclosed to the Joint Oversight Panel (JOP) along with an explanation of the safeguards in place to ensure that the affiliation does not compromise NCC Group's ability to render a fair and impartial decision with respect to the Applicant or Participant organization.

Such affiliations include, but are not limited to:

- Officers of the Applicant or Participant organization serving on the NCC Group's Board of Directors in a voting capacity, and vice versa;
- Significant monetary arrangements or commercial relationship between NCC Group and the Applicant or Participant organization, outside of the fee charged for certification and participation in the APEC CBPR or PRP System; or
- All other affiliations which might allow the Applicant or Participant organization to exert undue influence on NCC Group regarding the Applicant organization's certification and participation in the CBPR or PRP System.

In addition to disclosing to the Joint Oversight Panel (JOP) all withdrawals related to an officer of the Applicant or Participant organization serving on the NCC Group's Board of Directors in a voting capacity, and vice versa, NCC Group shall also disclose to the JOP those activities or business ventures identified above considered to be a conflict of interest on its face, but did not result in withdrawal. NCC Group should include a description of the reasons for non-withdrawal and the measures NCC Group took to avoid or cure any potential prejudicial results stemming from the actual or potential conflict of interest.

2.1.3 Publishing Certification Standards

NCC Group will utilize all relevant template documentation developed by APEC to include the CBPR and PRP Intake Questionnaire, the CBPR and PRP Program Requirements, CBPR and PRP Program Requirements Map, and more specifically requirements detailed in Annex C to perform the certification. See Section 3 Program Requirements for additional information.

These certification standards are published on the CBPR/PRP website for Applicant and Participating organizations. The standards will be provided to the Applicant and Participating organization as part of the certification process. These standards will be published and available to organizations on the NCC Group's website. [https://www.nccgroup.com/us/what-is-the-apec-cbpr/]

2.1.4 Reporting to FTC

NCC Group will report to the Federal Trade Commission (FTC) or other appropriate public authority on certification of any new Applicant organization, audits of existing Participant organizations, or any dispute resolutions. NCC Group will maintain a list of certified companies on the NCC Group's website and send an updated list to the JOP on at least a monthly basis or whenever there is a material change.

2.1.5 Case Reports

NCC Group will abide by the process under Section 7.7 Case Notes for the mandatory publication of case reports under certain circumstances. Case notes and statistics must be reported to the JOP for publication on an annual basis.

2.1.6 Assessor Training

Assessors will be trained on all certification requirements prior to being assigned to a certification engagement. Assessor training will consist of on-line or in-class room training to cover these policies, procedures, use of tools, standards, and writing certification reports. Assessors will obtain a certificate of attendance to the training and will be authorized to perform a CBPR and PRP certification. Only current certified assessors will be permitted to perform

a CBPR and PRP certification on NCC Group's behalf. Assessor certifications will be valid for one year and re-training/refresher training will be provided on an annual basis.

3 PROGRAM REQUIREMENTS

3.1 Governance of the CPBR and PRP System

Objective

The CBPR and PRP Systems require governance mechanisms performing essential operations in the administration and maintenance of the System. In the development of the governance model, a number of basic principles were identified:

- Simplicity;
- Transparency;
- Low cost; and
- Accountability to APEC Economies.

As the APEC representative body established to deal with data privacy issues, the Data Privacy Sub-Group is responsible for the governance of the CBPR and PRP Systems. Governance mechanisms should enable the day-to-day running of the CBPR and PRP Systems without the continuous involvement of the Sub-Group, which only meets twice a year.

As APEC is a non-treaty organization with a small full-time staff, governance of the CBPR and PRP Systems cannot impose onerous duties on either the Secretariat or Economies.

Functions of the Governance Model

Regardless of these limitations, the governance model should nonetheless deal with the essential administrative functions required for the CBPR and PRP Systems to effectively operate. These essential functions include:

- Developing and maintaining a staffing and revenue structure to support the CBPR and PRP System;
- Managing the APEC-hosted compliance directory;
- Facilitating participation in the CBPR and PRP Systems by APEC Economies, including through capacity-building activities;
- Assessing and monitoring the compliance of recognized Accountability Agents against the Recognition Criteria;
- Managing the Cross Border Privacy Enforcement Arrangement and associated documents and procedures; and
- Developing education materials to facilitate a region-wide understanding of the elements of the CBPR and PRP Systems and its program requirements.

3.2 APEC Cross-Border Privacy Rules (CBPR) System Program Requirements

The baseline program requirements of the APEC Cross Border Privacy Rules (CBPR) System is to assist NCC Group in an Applicant's compliance review process and to ensure this process is conducted consistently throughout participating APEC Economies. NCC Group is responsible for receiving an Applicant's intake documentation, verifying an Applicant's compliance with the requirements of the CBPR System and, where appropriate, assisting the Applicant in modifying its policies and practices to meet the requirements of the CBPR System. NCC Group will certify those Applicant deemed to have met the minimum criteria for participation provided herein, and will be responsible for monitoring the Participants' compliance with the CBPR System, based on this criteria. The APEC Cross Border Privacy Rules Intake Questionnaire lists the acceptable qualifications to the provision of notice, the provision of choice mechanisms, and the provision of access and correction mechanisms referred to in this document.

NOTICE

Assessment Purpose – To ensure that individuals understand the applicant's personal information policies (subject to any qualifications), including to whom the personal information may be transferred and the purpose for which the personal information may be used. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of notice.

COLLECTION LIMITATION

Assessment Purpose - Ensuring that collection of information is limited to the specific purposes stated at the time of collection. 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.

USES OF PERSONAL INFORMATION

Assessment Purpose - Ensuring that the use of personal information is limited to fulfilling the specific 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 applicant for the purpose of granting credit for the subsequent purpose of collecting debt owed to that applicant.

CHOICE

Assessment Purpose - 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 part II of the CBPR Self-Assessment Guidelines for Organizations. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of choice mechanisms.

INTEGRITY OF PERSONAL INFORMATION

Assessment Purpose - 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.

SECURITY SAFEGUARDS

Assessment Purpose - The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses.

ACCESS AND CORRECTION

Assessment Purpose - 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 whereby the ability to access and correct information is provided may differ depending on the nature of the information and other interests, which is why, 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. Section II of the CBPR Self-Assessment Guidelines for Organizations 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. Refer to the APEC Cross Border Privacy Rules Intake Questionnaire for a list of acceptable Qualifications to the provision of access and correction mechanisms.

ACCOUNTABILITY

Assessment Purpose - The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant 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.

3.3 APEC Privacy Recognition for Processors (PRP) System Program Requirements

SECURITY SAFEGUARDS

Assessment Purpose - The questions in this section are directed towards ensuring that when individuals entrust their information to an applicant, that applicant will implement reasonable security safeguards to protect individuals' information from loss, unauthorized access or disclosure, or other misuses.

ACCOUNTABILITY

Assessment Purpose - The questions in this section are directed towards ensuring that the Applicant is accountable for complying with measures that give effect to the other Principles stated above. Additionally, when transferring information, the Applicant 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.

3.4 Elements of the CBPR and PRP System

The CBPR and PRP Systems consist of four elements: (1) self-assessment; (2) compliance review; (3) recognition/acceptance; and (4) dispute resolution and enforcement.

CBPR and PRP ELEMENT 1 – SELF-ASSESSMENT

Self-Assessment Questionnaire for Organizations

The CBPR and PRP System relies on an organization's self-assessment of their data privacy policies and practices against the requirements of APEC Privacy Framework using an APEC recognized CBPR and PRP questionnaire. This questionnaire will be provided by NCC Group, in accordance with established selection requirement.

Compliance Review

The completed questionnaire and any associated documentation will then be submitted to the NCC Group for confidential review against the baseline standards established in the CBPR program requirements.

The submission of this questionnaire is the first step in an evaluative process that will determine whether an organization's privacy policies and practices are consistent with the program requirements of the CBPR or PRP System. This process can also be used by organizations to help them develop privacy policies or revise existing privacy policies to meet the program requirements of the CBPR or PRP System.

This questionnaire may be supplemented by additional questions, documentation or requests for clarification as part of the NCC Group's review process.

Compliance Directory

An organization that is found to be compliant with the CBPR or PRP program requirements by NCC Group will be certified as CBPR or PRP compliant and will have relevant details of their certification published in an APEC-hosted website as well as on NCC Group's website so that consumers and other stakeholders can be made aware that the organization is an active participant in the CBPR or PRP System.

CBPR and PRP ELEMENT 2 – COMPLIANCE REVIEW

Accountability Agent Recognition Criteria

To become an APEC-recognized Accountability Agent, NCC Group will meet the established recognition criteria to the satisfaction of APEC Economies.

These criteria provide for the evaluation of NCC Group's program requirements, dispute resolution procedures, and policies and procedures for the avoidance of conflicts of interest as well as process issues, including the certification and re-certification processes, ongoing monitoring and compliance reviews and enforcement of program requirements.

As a condition of APEC recognition, NCC Group is required to release anonymized case notes and complaint statistics. Complaint handling is an important element of the CBPR and PRP Systems. These actions will:

- promote understanding and increase transparency about the CBPR and PRP Systems;
- aid consistent interpretation of the APEC Privacy Principles and the CBPR or PRP System;
- provide additional guidance to organizations on the application of the APEC Privacy Principles and CBPR or PRP System; and
- promote accountability of those involved in complaints handling and build stakeholders' trust in the process.

As a further condition of APEC recognition, NCC Group will consent to respond to requests from relevant government entities in any APEC Economy that reasonably relate both to that Economy and to the CBPR/PRP-related work of NCC Group, where possible.

NCC Group will endeavor to cooperate when appropriate and where possible in CBPR or PRP-related complaint handling matters with other recognized Accountability Agents.

Compliance Review Process of CBPRs or PRPs

When reviewing an organization's privacy policies and practices as described in the self-assessment questionnaire, NCC Group will assess them against the CBPR or PRP program requirements. These program requirements are designed to provide the minimum standard that applicant organizations should meet in order to ensure that the assessment process is conducted in a consistent manner across participating Economies. NCC Group's assessment process may exceed this standard, but may not fall below it.

CBPR and PRP ELEMENT 3 – RECOGNITION

Compliance Directory and Contact Information

APEC Economies will establish a publicly accessible directory of organizations that have been certified by NCC Group as compliant with the CBPR or PRP System. The directory will include contact point information that consumers can use to contact participating organizations. Each organization's listing will include the contact point

information for NCC Group that certified the organization and the relevant Privacy Enforcement Authority (i.e. FTC). Contact point information allows consumers or other interested parties to direct questions and complaints to the appropriate contact point in an organization or to NCC Group, or if necessary, to contact the FTC.

The directory and contact lists will be hosted by the APEC Secretariat and maintained by the Electronic Commerce Steering Group in accordance with the APEC Website Guidelines. This website may be expanded to contain FAQs and additional information on the CBPR or PRP System for potential applicant organizations and for consumers.

CBPR and PRP ELEMENT 4 – ENFORCEMENT

Cooperation Arrangement for Cross-Border Privacy Enforcement

The CBPR and PRP system should be enforceable by NCC Group and the Federal Trade Commission (FTC):

- NCC Group will enforce the CBPR or PRP program requirements through contract; and
- The FTC will have the ability to take enforcement actions under applicable domestic laws and regulations that have the effect of protecting personal information consistent with the CBPR or PRP program requirements.

The CPEA, which was endorsed by APEC Ministers in November 2009 and commenced on 16 July 2010, aims to:

- facilitate information sharing among Privacy Enforcement Authorities (PE Authorities) in APEC Economies (which may include Privacy Commissioners' Offices, Data Protection Authorities or Consumer Protection Authorities that enforce Privacy Laws);
- provide mechanisms to promote effective cross-border cooperation between authorities in the enforcement of CBPR program requirements and privacy laws generally, including through referrals of matters and through parallel or joint investigations or enforcement actions; and
- encourage information sharing and cooperation on privacy investigation and enforcement with PE Authorities outside APEC (including by ensuring that the CPEA can work seamlessly with similar arrangements in other regions and at the global level).

The CPEA creates a framework for the voluntary sharing of information and provision of assistance for information privacy enforcement related activities. Any PE Authority in an APEC Economy may participate. Participating PE Authorities will contact each other for assistance or to make referrals regarding information privacy investigations and enforcement matters that involve each other's Economies. For example, during an investigation, a PE Authority in Economy X may seek the assistance of a PE Authority in Economy Y, if certain evidence of the alleged privacy violation (or the entity being investigated) is located in Economy Y. In that case, the PE Authority in Economy X may send a Request for Assistance to the point of contact in the PE Authority in Economy Y. The PE Authority in Economy Y may then consider the matter and provide assistance on a discretionary basis.

35 Process for Certification of Organizations

Applicant organizations should make use of an Accountability Agent located within the jurisdiction in which the applicant organization is primarily located or an Accountability Agent recognized by APEC.

Once an applicant organization selects and contacts NCC Group, NCC Group will provide the self-assessment questionnaire to the organization for completion and will review the answers and any supporting documentation based on its assessment guidelines. NCC Group will make use of APEC recognized documentation and review procedures.

The proposed application process would be iterative and allow for back and forth discussions between the applicant organization and NCC Group.

The Accountability Agent Recognition Criteria describe the role of Accountability Agents as follows:

- The Accountability Agent is responsible for the self-assessment and compliance review phases of the CBPR or PRP System accreditation process. Applicant organizations will be responsible for developing their privacy policies and practices and may only participate in the CBPR or PRP System if these policies and practices are certified by the relevant Accountability Agent to be compliant with the requirements of the CBPR or PRP System. It is the responsibility of the Accountability Agent to certify an organization's compliance with these requirements.
- The self-assessment questionnaire and assessment guidelines are publicly-available documents and prospective applicant organizations will have access to the guidelines so that they can see how their responses to the self-assessment questionnaire will be assessed. In considering how best to assist prospective applicant organizations, a recognized Accountability Agent may wish to develop additional documentation outlining their review process.

3.6 Role of the FTC

The CPEA defines 'Privacy Enforcement Authority' as any public body that is responsible for enforcing Privacy Law, and that has powers to conduct investigations or pursue enforcement proceedings. 'Privacy Law' is then defined as laws and regulations of an APEC Economy, the enforcement of which have the effect of protecting personal information consistent with the APEC Privacy Framework.

- The Privacy Enforcement Authority must be able to review a CBPR complaint/issue if it cannot be resolved by the participating organization in the first instance or by the Accountability Agent and when appropriate, investigate and take enforcement action. The Privacy Enforcement Authority has the discretion to decide whether or not to deal with a Request for Assistance made by another Privacy Enforcement Authority.
- CPEA participation is the predicate step to any Economies' involvement in the CBPR System as the CPEA establishes that the Economy has a law in place "the enforcement of which, has the effect of implementing the APEC Privacy Framework."

4 CERTIFICATION PROCESS

4.1 NCC Group's SMARTS Assessment Process for CBPR and PRP Certification

4.1.1 (S)cope

The first phase of a CBPR or PRP Certification is to ensure the scope of the assessment is properly identified. It is important all systems are identified that may create, receive, maintain, or transmit personal information. Applicant organizations have the option to include or exclude certain applications, systems, or services from within the scope of the assessment; however, the applicant organization can only claim those applications, systems, or services within scope to be certified as applicable. Scoping is one of the most important steps in the certification process and one needing to be performed properly. The success of the certification process depends directly on scoping the assessment correctly. In addition, any conflict of interests will be reviewed and identified during the scoping phases and handled according to *Section 2 Conflicts of Interest Policy*.

The Applicant organization will also be risk rated based on the amount of personal data being created, maintained, received, or transmitted as well as whether the Applicant organization is a controller or processor of the data. The Applicant organization's risk will determine the level of testing required for certification. The riskier the organization, the more testing, documentation, and evidence required to substantiate compliance with the requirements.

4.1.2 (M)ap

After the Applicant organization's environment has been scoped, the Applicant organization will complete the required self-assessment questionnaire. The Applicant organization will be responsible to answer 'yes' or 'no' to the relevant question and map its current privacy policies and procedures to the respective questions.

4.1.3 (A)nalyze

The Applicant organization will forward the self-assessment questionnaire along with all evidence to NCC Group for analysis. Document evidence will be transferred through NCC Group's Secure File Exchange. The assigned certification assessor will analyze the answers to the questions along with relevant documentation. This will include verifying the contents of the self-assessment forms completed by the Applicant organization against the program requirements for NCC Group. This analysis may also include in-person or phone interviews, inspection of the personal data system, website scans, or automated security tools.

The Applicant organization will be notified of any gaps or deficiencies discovered during this initial analysis. The Applicant organization will be provided the opportunity to submit additional evidence to demonstrate compliance according to the response provided for each question.

4.1.4 (R)eview

The certifying assessor will review all documentation and evidence provided. Based upon the review, the assessor will assign a 'Compliant', 'Partially Compliant', or 'Not Compliant' rating to each requirement area. For any requirement not being 'Compliant', a recommendation will be provided for the Applicant organization to review. The Applicant organization should mitigate all requirements identified as 'Partially Compliant' or 'Not Compliant' in order to obtain certification. The certifying assessor will utilize the Assessment Criteria provided for by the CBPR or PRP System Programs.

4.1.5 (T)est

"To perform a health certification, the assessor must EAT".

The certifying assessor will follow the E-A-T process to determine the effectiveness of the policies/procedures/controls required.

- (E)xamine – The certifying assessor will examine and evaluate all document/evidence provided.
- (A)nalzye – The certifying assessor will interview subject matter experts and analyze procedures being implement are appropriate to carry out requirements. The certifying assessor will determine if processes match

evidence provided.

- (T)est – The certifying assessor will perform testing or sampling to demonstrate appropriate effectiveness of controls being implemented. The certifying assessor will abide by the following sampling guidelines:

Sampling Guidelines

Frequency or Population Size	Sample Size
Daily or several times a day	25
Weekly	5
Monthly	2
Quarterly	2
Population of 50 to 250	10% of population
Not weekly, monthly, or quarterly and less than 50	At least 5 or entire population

4.1.6 (S)ubmit

Only Applicant organizations receiving 'Compliant' ratings on all requirements will obtain CBPR or PRP certification. Assessments will be reviewed by NCC Group QA Reviewers to determine sufficiency and quality of the work performed by the certifying assessor. Upon approval by the QA Reviewer, the Applicant organization will receive a comprehensive report outlining NCC Group's findings regarding the Applicant organization's level of compliance with the program requirements.

If the assessment is fully compliant, the Applicant organization will obtain the CBPR or PRP certification identifying the Applicant organization is in compliance with NCC Group's program requirements This certification will include an attestation letter and a 'certification packet' explaining the terms and conditions of use of the certification logo. An Applicant organization receiving a certification will be referred to as a 'Participant' in the CBPR or PRP System.

If the assessment is not fully compliant, the report will include a list of changes the Applicant organization needs to complete for purposes of obtaining certification for participation in the CBPR or PRP System. The Applicant organization will have the opportunity to provide additional evidence to satisfy the requirement based on the previous recommendations provided. The Applicant organization will have thirty (30) days from the date of notification their assessment is not fully compliant to provide requested evidence in order to become compliant. The certifying assessor will verify any changes required under non-fulfillment of the program requirements have been properly completed by the Applicant organization.

If the Applicant organization is not able to provide the evidence requested in thirty (30) days, the assessment becomes "Not Compliant' and the Applicant organization must restart the certification process. Note: Additional fees will apply based on the level of re-testing required for the Applicant organization to obtain certification.

4.2 Grant of Service/Trade Marks

Beginning on the Certification Date of the Participant organization in the CBPR and/or PRP system and for so long as the Participant organization remains a CBPR or PRP Certified organization:

1. Participant organization grants to NCC Group a non-exclusive, non-assignable, non-transferrable, non-sublicensable, royalty-free limited license to use Participant organization's trademarks and service marks in relation to the CBPR and/or PRP Systems. Participant organization will provide NCC Group with digital versions of its service marks and trademark(s) and a summary description of its services for these purposes.
2. NCC Group grants the Participant organization a non-exclusive, non-assignable, non-transferrable, non-sublicensable, royalty-free limited license to:

a. identify itself as being (as appropriate):
    i. 'CBPR Certified by NCC Group'
    ii. 'PRP Certified by NCC Group'
b. use the NCC Group CBPR and/or PRP service marks (see (a) and (b) below respectively);
c. in promotional, business stationery (physical and digital) and educational materials according to the terms and conditions of the Certification Agreement (including the Requirements and Procedures) for the sole purpose of demonstrating compliance with the CBPR and PRP System. Accordingly, NCC Group will provide the Participant organization with digital versions of the service marks (as appropriate) and summary description of its services.

(a) NCC Group CBPR Service Mark:

(b) NCC Group PRP Service Mark:

43 Communication Guidelines

As required to become APEC CBPR or PRP Certified, an Applicant organization must obtain certification from an Accountability Agent. Once an Applicant organization is certified, the organization becomes a Participant in the CBPR or PRP Systems Program. The following are guidelines a Participant organization should follow once the organization is certified:

General Principles

1. Communication of the certification and process should be abide by the general governance principles as the follows:
    a. Communications should be simple and understandable;
    b. Communications should be honest and transparent;
    c. Communications should not be misleading about pricing, fees, or other costs associated with the certification process; and
    d. Communications should be accountable to the Federal Trade Commission.
2. The NCC Group CBPR or PRP Certification logo is restricted for use by Certified Participant organizations.
3. Participant organizations are able to present their views of the certification process in webinars, press releases, white papers, articles, and Internet-based Media except to provide defamatory content that could harm the reputation of the certification process or NCC Group.

5 ON-GOING MONITORING AND COMPLIANCE REVIEW PROCESSES

5.1 On-Going Monitoring

Once a Participant organization is certified, NCC Group will utilize a combination of methods to verify on-going compliance with the CBPR and PRP programs. Methods of monitoring may include, but not limited to:

1. *Technical Testing:* Non-disruptive technical testing of in-scope systems of Participant organization to ensure technical safeguards are in place such as the following:
    a. Authentication and access control
    b. Encryption
    c. Boundary protection
    d. Audit logging
    e. Monitoring
        i. Technical testing could consist of both commercial and proprietary tools utilized in vulnerability/penetration testing engagements. Note: There are too many tools available for use to list them all here and some are proprietary tools available only to NCC Group staff.
2. *Website Reviews:* Review of Privacy Policies and Terms of Conditions of use of Participant organizations website and/or in-scope systems.
3. *Random Audits:* Random reviews covering specific areas of requirements. Participant organizations will need to supply any updated evidence and participate in short interviews to verify compliance.
4. *Investigations of Any Complaints or Disputes*: See Section 7 Dispute Resolution Process for further information.

5.2 Compliance Review Process

Participant organizations are required to perform routine compliance reviews at least annually as part of on-going monitoring activities.

These compliance reviews could include, but not limited to:

1. Review of policies and procedures, updates, sign-off by staff, and changes based upon environment, regulatory requirements, and contractual obligations;
2. System configuration reviews;
3. Technical and non-technical compliance evaluations;
4. Security risk analysis;
5. Audit logging and monitoring activities to detect, prevent, and respond to attacks, intrusions, or other security failures; and
6. Reviews of staff training and security communications.

All compliance review activities should be documented by the Participant organization and provided as evidence in the Re-Certification process. See Section 6 Re-Certification and Annual Attestation for further information.

5.3 Investigation Process

If NCC Group believes there are reasonable grounds a Participant organization has engaged in a practice constituting a breach of the CBPR or PRP Program requirements, an immediate review process will be conducted at Participant's sole cost and expense. This review process will verify continued compliance with the CBPR and PRP Program requirements. Participant will self-report to NCC Group if it has reasonable grounds to believe it may have breached the CBPR or PRP Program requirements.

The Participant organization will agree to assist NCC Group to perform a compliance audit as part of the Terms and Conditions of Certification.

Reasonable grounds could be obtained through a report of a suspected breach in publicly available media outlets, discovered during the review process, or reported to NCC Group directly.

Section 7.3 Investigating Complaints details the steps required to be followed to complete an investigation.

Outcome of Investigation

Upon a report of a suspected breach or non-compliance issue, the Privacy Practice Director will conduct an investigation. A report will be generated providing the decision of the investigation. The outcome of an investigation can fall within one of the following areas:

- Resolution Agreement: Where non-compliance with any of the program requirements is identified, NCC Group will notify the Participant organization outlining the corrections the Participant needs to make and a reasonable timeframe within which the corrections must be completed based on the deficiencies identified. This timeframe will generally be thirty (30) days from the date of notification, but could be extended based upon the nature of the non-conformity.

  The Participant organization and NCC Group will come to an agreement over the issues that will result in the Participant organization resolving the non-conformities in the agreed upon timeframe. NCC Group will verify that the required changes have been properly completed by the Participant organization within the stated timeframe.

- Suspension/Withdrawal of Certification: A non-conformity requiring formal enforcement resulting in a Participant organization's suspension or notice to terminate certification for cause not resolved accordingly.
- Report to FTC: A non-conformity resulting in immediate termination of the CBPR or PRP program and depending on severity of the issue, reporting to the Federal Trade Commission (FTC).

See other enforcement Penalties in Section 8.2.

Any Participant organization found to be in non-compliance and subject to suspension, withdrawal, or reporting to the FTC must immediately remove the NCC Group CBPR or PRP Certification mark from public facing communications and/or w

6 RE-CERTIFICATION AND ANNUAL ATTESTATION

6.1 Re-Certification

The Participant organization must maintain the implementation of reasonable administrative, technical, and physical safeguards commensurate to the Participant's size and complexity, nature/scope of activities, and sensitivity of personal information collected, maintained, received, or transmitted.

Participant organizations are required to perform an annual certification by NCC Group in order to evaluate the continued protection of personal information from leakage, loss or unauthorized use, alteration, disclosure, distribution, or access. This review and reassessment of security measures is intended to evaluate the relevance and effectiveness of the safeguards implemented by the Participant organization.

NCC Group will follow its SMARTS Assessment Process discussed in Section 4 Certification Process for the re-assessment and annual certification process of a Participant organization. NCC Group will perform regular comprehensive reviews to ensure the integrity of the re-Certification.

The re-certification review includes:

- A compliance assessment to include verification of the contents of the self-assessment updated by the Participant organization. This assessment may include reviews, in-person or phone interviews, inspection of in-scope systems, website scans, or automated security testing.
- NCC Group will provide a report to the Participant organization outlining any findings regarding the participant's level of compliance with the CBPR or PRP program requirements.
    - The report will list any corrections the Participant organization needs to make to correct areas of non-compliance and the timeframe to correct the non-conformities to obtain re-certification. Note: Timeframe is generally thirty (30) days from the date of notification.
- NCC Group will verify any changes required have been properly completed by the Participant organization.
- NCC Group will provide notice to the Participant organization of their compliance and re-certification.

6.2 Annual Attestation

NCC Group will require Participant organizations to attest on an annual basis to the continuing adherence to the CBPR and PRP program requirements.

Where there has been a material change to the Participant's privacy policy (as reasonably determined by NCC Group in good faith), an immediate review process will be carried out.

As part of the re-certification process, Participant organizations will attest to the information being provided in the review is accurate and true subject to penalties enforced by the Federal Trade Commission (FTC).

7 DISPUTE RESOLUTION PROCESS

NCC Group will have a mechanism in place to receive and investigate complaints about Participant organizations as well as resolve disputes between complainants and Participant organizations in relation to non-compliance with the CBPR and PRP program requirements.

NCC Group will have a mechanism in place for cooperation on dispute resolution with other Accountability Agents recognized by APEC economies when appropriate and where possible.

The dispute resolution process will be performed internally within NCC Group.

7.1 Receiving Complaints

NCC Group may receive complaints through contacting the program owners via email or by phone. The program owners are listed under section 1.1 Program Contacts and listed here:

Name	Title	E-mail	Phone
Mike Zhang	Manager	M.Zhang@nccgroup.com	402-630-6029
Kurt Osburn	Practice Director	Kurt.Osburn@nccgoup.com	205-907-7607
Joe Meyer	Global Deputy Lead, Compliance	Joseph.Meyer@nccgroup.com	402-680-9649

These contacts as well as the contact information for the FTC (i.e. link to https://www.ftccomplaintassistant.gov/#crnt&panel1-1 or 1-877-FTC-HELP) are available via the NCC Group's website: https://www.nccgroup.com/us/what-is-the-apec-cbpr/

NCC Group may receive complaints through multiple avenues such as contacting the Program Owners directly via email or by phone, complaints received through staff members, or complaints received through Corporate Help Desk support. Complaints will be forwarded to the Privacy Practice Director, Joe Meyer.

Once a complaint is received, a determination will be made of whether a complaint concerns the Participant's obligations under the program and that the filed complaint falls within the scope of the program's requirements. NCC Group's legal counsel may be contacted to assist in this determination.

7.2 Notifying Complainant

NCC Group will notify the complainant of the determination.

7.3 Investigating Complaints

NCC Group is committed to fully investigate and resolve complaints related to the CBPR and PRP Certification process. The complainant is notified of the outcomes of the tests unless they request otherwise. If verbal complaints are made, staff will request written correspondence is sent by the complainant to the Privacy Practice Director confirming the complaint to enable the QA Manager to investigate further.

Nonconforming Assessment Policy

NCC Group considers the quality of its work a primary objective and any deviations identified in tests are to be investigated immediately. The work will be immediately quarantined and given to the Quality Manager. The investigation will include validating the work as nonconforming, identify the cause, and escalating corrective actions to prevent reoccurrence. The Participant organization will be kept informed if the nonconformity affects them. Any other tests identified as being nonconforming as a consequence will be recalled and the customers notified.

Corrective Action Policy

The Senior Representative will decide who will implement each corrective action identified. Each instance of nonconforming work or problem will have a root-cause analysis performed and appropriate corrective actions escalated to prevent reoccurrence

Purpose of the Process

The aim of this procedure is to manage and progress complaints, audit non-conformities, non-conforming work, improvement suggestions, corrective actions, and preventive actions. This is to ensure problems are corrected as soon as practicable after they arise and ensuring their recurrence is minimized.

Responsibility

The Senior Representative is responsible for processing effectively and efficiently to the complaint and/or Participant's satisfaction.

The Senior Representative is responsible for ensuring actions are performed in a timely manner. The Quality Manager will track and regularly report to NCC Group management team on the progress of actions

Inputs to the Process

- Complaints;
- Audit non-conformities;
- Faulty tools, software, or assessment analysis;
- Continuous improvement suggestions; and
- Management review actions.

Outputs to the Process

- Resolved complaints;
- Completed corrective and preventive actions;
- Implemented continuous improvement suggestions; and
- Outcome as indicated under section 5.3 Investigation Process

Training Staff

The Privacy Practice Director will train staff in the investigation and dispute resolution process.

Records

Documentation related to Complaints and Resolutions are kept for three (3) years and are identified by reference numbers.

The Quality Manager keeps a copy of complaints and resulting actions for three (3) years. Each action records contains:

- Reference number;
- Named actionee;
- Target completion date;
- A description of the action;
- Root cause explanation where appropriate;
- The tracking of the action progress;
- A reference back to what initiated this action (audit/ complaint/ review meeting etc.);

- Evidence of the action being implemented; and
- Closure of the action by the Quality Manager.

Process

Non-conformities may be identified by any member of staff and reported to the Senior Representative or raised by the Participant or other member of the public.

Appeals: Investigation and decision on appeals shall not result in any discriminatory actions.

The handling process for complaints and appeals includes the following elements and methods:

- A description of the process for receiving, validating, investigating the complaint or appeal, and deciding what actions are to be taken in response to it;
- Tracking and recording complaints and appeals, including actions undertaken to resolve them;
- Ensuring that any appropriate action is taken;
- The Privacy Practice Director on receipt of the complaint or appeal shall be responsible for gathering and verifying all necessary information to validate the complaint or appeal;
- Whenever possible, the Privacy Practice Director shall acknowledge receipt of the complaint or appeal, and shall provide the complainant or appellant with progress reports and the outcome;
- The decision to be communicated to the complainant or appellant shall be made by, or reviewed and approved by, individual(s) not involved in the original inspection activities in question; and
- Whenever possible, the Privacy Practice Director shall give formal notice of the end of the complaint and appeals handling process to the complainant or appellant.

The Quality Manager may initiate additional audits if they cast doubts on the Certification Team's competence to comply with the CBRP or PRP Program requirements or its own policies or procedures.

The Quality Manager will audit corrective actions where appropriate to see if they have been effectively implemented. The results are recorded. The additional audit will be logged as an action stating how long after the corrective action implementation it is to be performed.

All complaints and non-conformities are considered to be the highest priority and will be promptly worked on.

When several root causes of a problem are identified, corrective actions will be raised in proportion to the risk of the cause identified in the root cause investigation.

The Quality Managers input to the Certification Team's review will assess how effective previous implemented corrective actions have been.

7.4 Notifying Participant

NCC Group is committed to fully investigate and resolve complaints related to the CBPR and PRP Certification in a confidential and timely manner. Where non-compliance with any of the program requirements are discovered, NCC Group will notify the Participant organization outlining the corrections the Participant organization needs to make and the reasonable timeframe to make the corrections.

Actions resulting from complaints are managed as corrective actions. The complainant and the Participant organization will be notified of the outcomes of the investigation unless they request otherwise. If verbal complaints are made, staff will request written correspondence is sent by the complainant to the Privacy Director confirming the complaint to enable the QA Manager to investigate further.

7.5 Obtaining Consent

NCC Group will obtain an individual's consent before sharing individual's personal information with the relevant enforcement authority in connection with a request for assistance or complaint. This consent is obtained through a positive or negative response to the question of sharing the individual's personal information to resolve the request.

7.6 Complaint Statistics Procedure

NCC Group will make publicly available on its website statistics on the types of complaints received by NCC Group and the outcomes of such complaints. This information will be communicated to the relevant government agencies and privacy enforcement authority (i.e. FTC). Complaint statistics will be submitted to the JOP on an annual basis.

NCC Group must attest as part of the dispute resolution mechanism there is a process for releasing complaint statistics and for communicating information to the relevant government agency and privacy enforcement authority. The template below along with associated guidance will assist in meeting this requirement.

7.6.1 CBPR Complaints

Objectives of Reporting Complaint Statistics

Complaints handling is an important element of the Cross-Border Privacy Rules (CBPR) program. The recognition criteria for Accountability Agents include an obligation to publish and report statistics on complaints received in order to:

- promote understanding about the operation of the CBPR program;
- increase transparency across the CBPR system;
- help governments, business and others to see how a complaints system is working and to help identify trends;
- enable comparisons of parts of the CBPR program across the APEC region; and
- promote accountability of those involved in complaints handling and build stakeholder trust in Accountability Agents.

Commentary on the Template

The template provided by the CBPR program is the core minimum statistics that are required to be reported in each case to form a common and comparable minimum data set across all APEC Accountability Agent dispute resolution processes.

Complaint Numbers

The total number of complaints should be reported. Where no complaints are received, the complaint statistics template should be submitted indicating "none" to ensure it is clear that no complaints were received that year. A format for reporting will need to be adopted that makes clear the number of new complaints received as well as older complaints carried over from the previous reporting period.

To assist readers to understand the reported figures and to aid in comparability there should be a note as to how terms are being used. For instance, some matters may be on the borderline between an enquiry about a company's information practice of concern and a complaint about that practice. Such matters may be quickly sorted out with an explanation to the enquirer or perhaps a telephone call to the company. NCC Group will differentiate between complaints (those items that need to be investigated) and enquiries (those items that are treated less formally).

Complaint Outcomes

This part of the template provides a picture of the processing of complaints.

Complaints Type

The template asks Accountability Agents to provide informative breakdowns of the complaints by type. This will provide a statistical picture of who is complaining and why.

Some complaints will raise several different issues. The report should explain the basis upon which NCC Group is reporting. One approach is, for example, to identify the principal aspect of the complaint and treat it for statistical purposes as being only about that issue. An alternative is to count and classify all the allegations made in a complaint. If the latter approach is taken, the totals of complaint types will exceed the total number of complaints received and this will need to be explained or it may seem to be an anomaly.

Complaints Process Quality Measures

There statistics give a picture as to how well the complaints resolution system is working. At a minimum, some indication as to timeliness should be reported. At its simplest, this might be to highlight the number or complaints that took longer than a target date to resolve (e.g. number of complaints on hand that are older than, say, three months) while some complaints systems may be able to produce a variety of more detailed statistics (e.g. the average time to resolve certain types of complaints). In a more sophisticated system, other quality measures may be included and NCC Group might, for example, report against internal targets or industry benchmarks if these are available.

General

NCC Group will comment on the various figures reported. To set the statistics in context, it is useful to include three or four years of figures where these are available.

COMPLAINT STATISTICS TEMPLATE

Complaint Numbers

[Number of complaints received during the year with a comment by the Accountability Agent on the significance of the number. A note should explain how the term 'complaint' is being used in the reported statistics.]

Complaint Processing and Outcomes

[Complaints processed during the year broken down by the outcome.

Examples of typical outcomes include:

- complaints that could not be handled as they were outside the program's jurisdiction (e.g. against a company that is not part of the CBPR program);
- complaints referred back to a business that are resolved at that point;
- complaints settled by NCC Group;
- complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority;
- complaints for which NCC Group has made a finding (such as complaint dismissed, complaint upheld in part, complaint upheld in full).

When NCC Group has made findings upholding complaints, further statistical information should be given about the outcomes and any subsequent enforcement action.

NCC Group should include a comment on the significance of the complaints outcomes.]

Complaints Type

[Further statistics should be provided as to the type of complaints, including the subject matter of the complaint and characterization of the complainants and the respondents. Useful classifications will include:

- complaint subject matter broken down by APEC information privacy principle (notice, collection limitation, use, etc);
- basic information about complainants, where known, such as the economy from which complaints have been made;

- Information about the type of respondents to complaints – this will vary on the nature of a particularly CBPR program but may include industry classification (e.g. financial service activities, insurance), the capacity in which the respondent falls (e.g. information processor, employer, service provider), or size of company (SME, large company etc).

NCC Group should comment on the significance of the reported figures.]

Complaints Process Quality Measures

[An indication should be given as to about any quality measures used in relation to the particular CBPR program. A typical measure may relate to timeliness. NCC Group should offer a comment upon the figures reported.]

7.6.2 PRP Complaints

The Accountability Agent recognition criteria require applicant Accountability Agents to attest as part of their complaint processing mechanism they have a process for releasing complaint statistics and for communicating information to the relevant government agency and privacy enforcement authority.

The template below along with associated guidance will assist in meeting this requirement.

Objectives of Reporting Complaint Statistics

Complaints processing is an important element of the Privacy Recognition for Processors (PPR) program. The recognition criteria for Accountability Agents include an obligation to publish and report statistics on complaints received in order to:

- promote understanding about the operation of the PRP program;
- increase transparency across the PRP system;
- help governments, business and others to see how a complaints system is working and to help identify trends;
- enable comparisons of parts of the PRP program across the APEC region; and
- promote accountability of those involved in complaints processing and build stakeholder trust in Accountability Agents.

Commentary on the Template

The template provided by the PRP program is the core minimum statics that are required to be reported in each case to form a common and comparable minimum data set across all APEC Accountability Agent dispute resolution processes.

Complaint Numbers

The total number of complaints should be reported. Where no complaints are received, the complaint statistics template should be submitted indicating "none" to ensure it is clear that no complaints were received that year. A format for reporting will need to be adopted that makes clear the number of new complaints received.

To assist readers to understand the reported figures and to aid in comparability there should be a note as to how terms are being used. For instance, some matters may be on the borderline between an enquiry about a company's information practice of concern and a complaint about that practice. Such matters may be quickly sorted out with an explanation to the enquirer or perhaps a telephone call to the company. NCC Group will differentiate between complaints (those items that need to be investigated) and enquiries (those items that are treated less formally).

Complaint Outcomes

This part of the template provides a picture of the processing of complaints.

Complaints Type

The template asks Accountability Agents to provide informative breakdowns of the complaints by type. This will provide a statistical picture of who is complaining and why.

Some complaints will raise several different issues. The report should explain the basis upon which the NCC Group is reporting. One approach is, for example, to identify the principal aspect of the complaint and treat it for statistical purposes as being only about that issue. An alternative is to count and classify all the allegations made in a complaint. If the latter approach is taken, the totals of complaint types will exceed the total number of complaints received and this will need to be explained or it may seem to be an anomaly.

Complaints Process Quality Measures

These statistics give a picture as to how well the complaint processing system is working. At a minimum, some indication as to timeliness of complaint processing should be reported. At its simplest this might be to highlight the number or complaints that took longer than a target date to forward appropriately to the Participant or controller.

General

NCC Group should comment on the various figures reported. To set the statistics in context, it is useful to include three or four years of figures where these are available.

Compliant Statistics Template

Complaint Numbers

[Number of complaints received during the year with a comment by the Accountability Agent on the significance of the number. A note should explain how the term 'complaint' is being used in the reported statistics.]

Complaint Processing and Outcomes

[Complaints processed during the year broken down by the outcome.

Examples of typical outcomes include:

- complaints that could not be handled as they were outside the program's jurisdiction
- (e.g. against a company that is not part of the PRP program);
- complaints forwarded to the Participant;
- complaints forwarded to the applicable controller;
- complaints transferred to another Accountability Agent, Privacy Enforcement Authority or other enforcement authority, where applicable;

When NCC Group has made findings upholding complaints, further statistical information should be given about the outcomes and any subsequent enforcement action.

NCC Group should include a comment on the significance of the complaints outcomes.]

Complaints Type

[Further statistics should be provided as to the type of complaints, including the subject matter of the complaint and characterization of the complainants and the respondents. Useful Classifications will include:

- complaint subject matter broken down by APEC information privacy principle (security safeguards and accountability);
- basic information about complainants, where known, such as the economy from which complaints have been made.
- Information about the type of respondents to complaints – this will vary on the nature of a particularly PRP program but may include industry classification (e.g. financial service activities, insurance) or size of company (SME, large company etc).

NCC Group should comment on the significance of the reported figures.]

Complaints Process Quality Measures

[An indication should be given about any quality measures used in relation to the particular PRP program. A typical measure may relate to timeliness. NCC Group should offer a comment upon the figures reported.]

7.7 Case Notes

The Accountability Agent Recognition Criteria require applicants to attest as part of their dispute resolution mechanism they have a process for releasing, in anonymized form, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes.

NCC Group will release, in an anonymized format, case notes on a selection of resolved complaints illustrating typical or significant interpretations and notable outcomes. These case notes will be provided to JOP on an annual basis.

The template below along with associated guidance will assist in meeting this requirement

Objectives of Release of Case Notes

Complaints handling is an important element of the Cross-border Privacy Rules (CBPR) and Privacy Recognition for Processors (PPR) programs. The recognition criteria for Accountability Agents include an obligation to release case notes on a selection of resolved complaints in order to:

- promote understanding about the operation of the CBPR and PRP program;
- assist consumers and businesses and their advisers;
- facilitate consistency in the interpretation of the APEC information privacy principles and the common elements of the CBPR program and PRP program;
- increase transparency in the CBPR program and PRP; and
- promote accountability of those involved in complaints handling and build stakeholder trust in accountability agents.

Commentary on the Template

The template provided by the CBPR and PRP program is the core minimum elements required to be reported to produce a satisfactory case note.

General Heading

It is possible to combine the general heading and citation into a single heading or adopt a citation that stands in for a general heading. However, unlike a series of law reports directed exclusively at lawyers, case notes are useful as an educational tool for ordinary consumers and businesses. Accordingly, a general heading that communicates a clear straightforward message is recommended.

Citation

It is essential that all those that may wish to refer to a case note can do so by an accepted citation that unambiguously refers to the same note. All case notes should be issued with a citation including the following elements:

- a descriptor of the case;
- the year of publication ;
- a standard abbreviation for the accountability authority (i.e. FTC-US), and;
- a sequential number.

Case Report

The style and approach of case reports can differ substantially but there are several elements that almost certainly will appear. These include:

- an account of the facts (e.g. as initially asserted on a complaint and as found after investigation)
- the relevant requirement (which will include the elements of the CBPR or PRP program)
- a discussion of the issues of interest and how the law applied to the facts in question
- the outcome of the complaint.

Key Terms

It may be useful to include the standard terms used in traditional indexing or which will appear as tags in on-line environments.

CASE NOTE TEMPLATE

General Heading

Citation

- Case Description:
- Publication Year:
- Accountability Authority: FTC-US
- Number:

Case Report

- Facts
- Law
- Discussion
- Outcome

Date

Key Terms

- Tags

---

8 MECHANISMS FOR ENFORCING PROGRAM REQUIREMENTS

Applicants and Participant organizations must abide by NCC Group's Certification Program related to the CBPR and PRP certifications. These organizations must sign and agree to the terms and conditions set forth under NCC Group's Master Service Agreement (MSA) [See Appendix A for additional information] and Statement of Work (SoW) [See Appendix B for additional information]. Both the MSA and SoW identify that participants must comply with the applicable certification standards to include annual re-certification requirements, random audits, or investigations into possible breaches or non-conformity complaints. Program requirements against Applicants and Participant organizations is enforced through contractual obligations.

NCC Group is a US for-profit corporation that must abide by the Federal Trade Commission (FTC) regulatory authority.

NCC Group must maintain a process to notify Participants immediately of non-compliance with NCC Program's requirements and for requiring Participant to remedy the non-compliance within a specified time period. See Section 7.4 Notifying Participant for additional information. Participants are required to communicate and maintain an active point of contact for the CBPR or PRP Certification program with NCC Group.

8.1 Penalties

NCC Group will impose the following penalties proportional to the harm or potential harm resulting from a violation when a Participant organization has not complied with the CBPR or PRP Program requirements and failed to remedy non-compliance within a specified time period:

- Participant organizations are required to remedy non-compliance within specific timeframes and failing to do so, NCC Group will remove the Participant organization from the CBPR or PRP program.
- NCC Group may temporarily suspend the Participant organization's right to display NCC Group's seal.
- NCC Group may publicly name the Participant organization's non-compliance.
- NCC Group may refer the violation to the Federal Trade Commission (FTC) where a violation was identified to violate applicable law.
    - If it is reasonably believed that a failure to comply is a violation of applicable law, NCC Group will refer a matter to the appropriate public authority or enforcement agency (i.e. FTC) for review and possible law enforcement action where NCC Group has a reasonable belief that a Participant organization's failure to comply with the APEC Cross-Border Privacy Rules (CBPR) System requirements has not been remedied within a reasonable time pursuant to NCC Group's established review process and procedures. See Section 7 Dispute Resolution Process for additional information.
- NCC Group may not assess monetary penalties against a Participant organization; however, NCC Group reserves the right to charge a reasonable fee to perform retesting or revalidation work as part of a Participant organization's desire to maintain its CBPR or PRP Certification.

Failure to comply with an investigation or re-certification audit will be grounds for a Participant organization's automatic withdrawal from the CBPR or PRP Certification program.

8.2 Enforcement Entity Requests

NCC Group will respond to requests from enforcement entities in APEC economies that reasonably relate to the Economy and to the CBPR or PRP-related activities of NCC Group, where possible.