This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

SEC Security Sub-Committee (SSC)

SSC CPA Issue Resolution Sub-Group (SCIRS) Terms of Reference V1.21

1. Purpose

The SSC CPA Issue Resolution Sub-Group (SCIRS) was formed by the Security Sub-Committee (SSC) to facilitate the CPA evaluation process. It now facilitates the SSC in their duties as CPA Scheme Owner with overall responsibility set out in the Smart Energy Code (SEC) for the delivery, operation and maintenance of the CPA Scheme for defined Device security assurance and for meeting the relevant SEC obligations applying to CPA Certification. The SSC, as the CPA Scheme Owner, is responsible for appointing a CPA Scheme Operator, for appointing CPA Test Labs, for maintaining the CPA Policies and Procedures, for publishing CPA Certificates and for approving the 'CPA Test Lab Framework Agreement' and the 'CPA Manufacturer Standard Agreement'.

SCIRS provides a working level industry engagement forum through which SSC, DESNZ, and the CPA Scheme Operator can work together with key industry partners to:

- maintain the CPA Policies and Procedures;
- review the CPA Manufacturer Standard Agreement;
- review any changes to the CPA Security Characteristics;
- review any changes to the SSC Guidance on Device Security Assurance and Triage;
- review issues arising from, or in anticipation of, CPA evaluations; and
- to reach a consensus where possible on:
    - the application of security controls; and
    - the interpretation and implementation of the CPA Security Characteristics and any associated Guidance to facilitate the CPA evaluation process.

Recommendations from the SCIRS' reviews are then submitted to the SSC for approval.

The sub-group operates under the governance of the SEC Security Sub-Committee and in line with SEC Section G7.16(b):

"the Security Sub-Committee Chair shall invite to attend Security Sub-Committee meetings any persons that the Security Sub-Committee determines it appropriate to invite in order to be provided with expert advice on security matters."

2. Scope

The scope of the sub-group includes any issues raised relating to:

a) matters relating to the CPA Policies and Procedures;

b) generic issues arising from the CPA evaluation or anticipated evaluation of smart metering products (but excluding Manufacturer or product specific evaluation questions);

c) generic issues relating to the progress of any Use Cases for Device Triage and refurbishment through the CPA process or relating to security considerations including the CPA Build Standard;

d) any proposals for changes to SSC Guidance, the CPA Security Characteristics (SCs) or to proposals for consideration of any new Use Cases for Device Triage and refurbishment in line with the methodology published by the SSC.

Any SCIRS participant, Sub-Committee Member or SEC Panel Member can raise an issue to be considered by the SCIRS, and the agenda for each meeting is approved by the SSC.

3. Out of Scope

The role of the sub-group does not include becoming involved in specific CPA evaluations and excludes the following:

a) approval of decisions that are within the remit and authority of the SSC or, DESNZ;

b) raising SEC Modifications;

c) raising issues that are unrelated to the scope; and

d) discussion of information having a commercially sensitive or competitive impact.

4. Proceedings of the SCIRS

a) SCIRS will normally meet on a monthly basis (with ability to cancel standing meetings) but will meet less frequently and on an ad-hoc basis if required.

b) SCIRS will be chaired by the SSC Chair. Secretariat and administrative functions will be performed by SECAS;

c) Sub-group members are expected to be able to meet at relatively short notice (either by video-conference or face to face) at the request of SSC;

d) Sub-group members will assist in maintaining the CPA Policies and Procedures, in the analysis and resolution of issues and the review of proposed advice and guidance to Manufacturers, CPA Test Labs, the CPA Scheme Operator and Triage Facility Providers. Device Manufacturers in particular will be given the opportunity to discuss existing and new issues;

e) Sub-group members will assist in the analysis and resolution of proposed changes to CPA Security Characteristics and proposals for Use Cases relating to Device Triage and refurbishment;

f) Whilst attendance may not be necessary for all interested parties, papers and outcomes will be made available to the wider SCIRS membership;

g) A summary of issues addressed, the outputs and any advice from the sub-group will be presented to the SSC at the following SSC meeting for consideration and any formal approval where necessary;

h) In the event that a consensus cannot be reached within the wider group, the normal SEC arrangements will apply to decision-making by SSC voting members;

i) Any submission to NCSC as a conclusion of any specific issue resolution will be formally made via SSC, DESNZ or the CPA Scheme Operator.

j) It is the responsibility of each SCIRS member to declare to the SSC Chair any actual or perceived conflict of interest with their duties as a SCIRS member. The SSC Chair may also request that a member absents themselves from a discussion where a conflict of interest is actual or perceived.

k) The sub-group will operate in accordance with the Confidentiality and Disclosure Protocol outlined in Appendix 1.

5. Deliverables

The sub-group will be expected to provide informed advice and recommendations to SSC and the CPA Scheme Operator, on the content, interpretation and implementation of the CPA evaluation process or Use Case implementation that is consistent with maintaining security controls and in the interests of national security.

Minutes and documentation will be stored on Egress maintained by SECAS and available for access by SCIRS members and wider as required.

6. Membership

Core membership of the sub-group will be SSC. Wider membership is open to:

- The CPA Scheme Operator;
- Device Manufacturers;
- CPA Test Laboratories;
- Triage Facility Providers
- energy suppliers;
- the DCC and its CSPs;
- Meter Asset Providers who are involved in achieving CPA Certification for products or are otherwise impacted operationally or financially by the CPA process and/or CPA Certification;
- Associated trade organisations including BEAMA, EUA and CMAP; and
- Other specialist parties, including NCSC, may also be invited to join the sub-group at the discretion of the Chair in line with SEC Section G7.16(b).

7. Rules of Participation

Meetings will be conducted under SEC SSC governance;

Outcomes of issues considered by the sub-group are expected to meet SEC objectives;

Any discussion in meetings and views expressed or implied in such discussions or associated documents are without prejudice to and shall not limit the discretion of the SSC with regard to final decisions. Equally, views expressed by participants during meetings will not prejudice any relevant consultation responses.

SCIRS members are subject to removal from the sub-group in line with the circumstances outlined in SEC Section C4.5 and C4.6 or by breaching the Conflict and Disclosure Protocol (Traffic Light Protocol – TLP).

Appendix 1: Conflict and Disclosure Protocol (Traffic Light Protocol – TLP)

Given the potentially sensitive nature of the work of the SCIRS meetings, the agendas, papers and discussions will be assigned an information sharing level of either CLEAR, GREEN, AMBER, AMBER-STRICT or RED. The SSC will add any necessary clarifications for security purposes.

Classification	Definition	Criteria
RED	For the eyes and ears of individual members of the governance group only, no further disclosure. RED information must not be shared with anyone else; information is limited to those individual members of the governance group including alternates (Panel/ Sub-Committee/ Working Group) and direct recipients of the material. Agenda items marked as RED will be discussed in a closed, confidential session and discussions will only be included in minutes marked as RED. Any documentation classified as RED shall be distributed using the agreed secure storage and distribution platforms.	RED Data indicates significant risk for the security, privacy, reputation or operation of organisations involved. RED is the equivalent to DCC Confidential, as defined by Section M4.22 of the SEC. Any DCC Confidential documents which are circulated to the Panel, it's Sub-Committees or Working Groups, will be treated the same as a RED SECAS document. RED-classified information is to be shared with members of the SSC and SCIRS governance group via the Egress Switch Platform containing Security or Privacy content. All RED documents should be shared in a non-editable format (e.g. PDF) unless the author requires direct input into the development of the document.
AMBER-STRICT	Limited disclosure, recipients can only distribute this on a strict need-to-know basis within their SEC Party Category to protect and prevent harm. This information can be restricted to a specified, narrower audience in some cases which should be clearly articulated on the document. An example would be anonymised details of a security incident or vulnerability that needs to be communicated on a strict need-to-know basis to enable appropriately qualified security specialists to implement prevention or mitigation actions. An example of Amber-Strict as applied to the Security Architecture document is: **Amber-Strict**. Limited disclosure and restricted to SSC Members and those who have a strict need to know in order to design, build or test components of the end-to-end smart metering system or to undertake security risk assessments and implement mitigations and security controls or to provide assurance of security risks and to protect and prevent harm.	AMBER-STRICT is the equivalent to DCC Controlled, as defined by Section M4.23 of the SEC. Any DCC Controlled documents which are circulated to the Panel, it's Sub-Committees or Working Groups must be marked as AMBER-STRICT if the desired audience is limited to sharing within the SEC Party category and not with third-party stakeholders who are not SEC Parties. The SSC and SCIRS will use Egress as the principal platform for distributing all AMBER-STRICT information. All AMBER-STRICT documents should be shared in a non-editable format (e.g PDF) unless the author requires direct input into the development of the document.

AMBER	Limited disclosure, recipients can only distribute this within their SEC Party Category and third-party stakeholders (who have a contractual relationship with that SEC Party) including Trade Associations on a need-to-know basis to protect and prevent harm. Agenda items marked as AMBER or AMBER+STRICT will be discussed in a closed, confidential session and discussions will only be included in the Confidential minutes marked as AMBER. Examples of third-party stakeholders include Trade Associations and contracted organisations within the supply chain (such as service providers, vendors, or a third party which has a contractual relationship with a SEC Party).	AMBER applies when information requires support to be effectively acted upon, yet carries risk to security, privacy, reputation, or operations if shared outside of the organisations involved. It can be broadly categorised as information which is restricted to a certain governance group. AMBER documents can be shared beyond the target governance group to those who have a need to know in order to take action and can only be shared by members within their SEC Party Category and third-party stakeholders such as Trade Associations. AMBER-classified information may be shared with members of the SSC and SCIRS governance group via the Egress Switch Platform or as an attachment to a secure, encrypted email. All AMBER documents should be shared in a non-editable format (e.g PDF) unless the author requires direct input into the development of the document.
GREEN	Limited disclosure, recipients can distribute this information to SEC Parties and SMIP stakeholders but not made publicly available. GREEN will be the default classification for any discussions unless otherwise notified. In practice, GREEN documentation is stored on the SEC website with password restrictions so SEC Parties can only access the documents after logging in. Agenda items marked as GREEN will be included in the minutes marked as GREEN.	GREEN applies when information is useful to increase awareness with SEC Parties. GREEN Data is information which should be shared for the benefit of SEC Parties but cannot be made completely public. GREEN is the equivalent to DCC Controlled (SEC Parties). Any DCC Controlled (SEC Parties), documents which are circulated to the Panel, it's Sub-Committees or Working Groups, will be treated the same as a GREEN SECAS document. Green-classified information may be shared with SEC Parties via the SEC website restricted to SEC Parties. All GREEN documents should be shared in a non-editable format (e.g PDF) unless the author requires direct input into the development of the document.
CLEAR	Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright. Agenda items marked as CLEAR will be included in the Non-Confidential minutes marked as CLEAR.	Sources may use CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. CLEAR is the equivalent to DCC Public. Any DCC Public documents which are circulated to the Panel, it's Sub-Committees or Working Groups, will be treated the same as a CLEAR SECAS document.

Classification Table