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.

Security Sub-Committee

Terms of Reference (ToR) Version 3.2

The Security Sub-Committee (SSC) shall be established pursuant to Section G7 of the Smart Energy Code (SEC).

Unless otherwise stated, defined terms have the same meaning as that which is attributed to them in the SEC.

1. Specific Duties of the Security Sub-Committee

The prescribed duties and powers of the SSC are set out in SEC Section G7.18 to G7.25.

The SSC will:

Document Development and Maintenance:

- maintain the User and DCC Security Controls Frameworks (SCF);
    - the SSC also maintains the Agreed Interpretations (AI), which are not listed in the SEC, to support the SCF.
- carry out reviews of the Security Risk Assessment at least once each year in order to identify any new or changed security risks to the End-to-End Smart Metering System;
- maintain the Security Requirements to ensure that it is up to date and at all times identifies the security controls which the Security Sub-Committee considers appropriate to mitigate the security risks identified in the Security Risk Assessment;
- maintain the End-to-End Security Architecture to ensure that it is up to date;
- develop and maintain a document to be known as the "Risk Treatment Plan", which shall identify the residual security risks which in the opinion of the Security Sub-Committee remain unmitigated taking into account the security controls that are in place;
- liaise and work with the NCSC to develop and maintain CPA Security Characteristics that set out the levels of security required for Smart Meters, Communications Hubs, SAPCs and HCALCs that are proportionate and appropriate taking into consideration the security risks identified in the Security Risk Assessment;

Security Assurance

- the SSC will periodically, and in any event at least once each year, review the Security Obligations and Assurance Arrangements in order to identify whether in the opinion of the Security Sub-Committee they continue to be fit for purpose;

- exercise such functions as are allocated to it under, and comply with, the applicable requirements of Section G8 (User Security Assurance) and Section G9 (DCC Security Assurance);
- provide the Panel with support and advice in respect of issues relating to the actual or potential non-compliance of any Party with the requirements of the Security Obligations and Assurance Arrangements;
- keep under review the NCSC CPA Certificate scheme in order to assess whether it continues to be fit for purpose in so far as it is relevant to the Code, and suggest modifications to the scheme provider to the extent to which it considers them appropriate;
- shall to the extent to which it considers it appropriate, in relation to any User (or, during the first User Entry Process, Party) which has produced a User Security Assessment Response that sets out any steps that the User proposes to take in accordance with Section G8.24(b); liaise with that User (or Party) as to the nature and timetable of such steps;
- provide advice to the Panel on the scope and output of the independent security assurance arrangements of the DCC in relation to the design, building and testing of the DCC Total System;
- provide advice to the Panel on the scope and output of the DCC assurance arrangements of the DCC Total System;
- provide advice to the Panel in relation to the appointment of the User Independent Security Assurance Service Provider, monitor the performance of the person appointed to that role and provide advice to the Panel in respect of its views as to that performance;
- provide advice and information to the Authority in relation to any actual or potential non-compliance with the CPA Security Characteristics of any Device or apparatus in respect of which a CPA Certificate is issued or required.

Monitoring and Advice

- provide such reasonable assistance to the DCC and Users as may be requested by them in relation to the causes of security incidents and the management of vulnerabilities on their Systems;
- monitor the (actual and proposed) Anomaly Detection Thresholds of which it is notified by the DCC, consider the extent to which they act as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems, and provide its opinion on such matters to the DCC;
- provide the Panel with support and advice in respect of Disputes for which the Panel is required to make a determination, insofar as such Disputes relate to the Security Obligations and Assurance Arrangements;
- provide the Panel, the Change Sub-Committee, the Change Board and any relevant Working Group with support and advice in relation to any Draft Proposal or Modification Proposal which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;

- advise the Authority of any modifications to the conditions of Energy Licences which it considers may be appropriate having regard to the residual security risks identified from time to time in the Risk Treatment Plan;
- respond to any consultations on matters which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;
- act in cooperation with, and send a representative to, the SMKI PMA, the Technical Architecture and Business Architecture Sub-Committee and any other Sub-Committee or Working Group which requests the support or attendance of the Security Sub-Committee;
- (to the extent to which it reasonably considers that it is necessary to do so) liaise and exchange information with, provide advice to, and seek the advice of the At HAN Forum on matters relating to the Alt HAN Arrangements which may affect the security of the End-to-End Smart Metering System or the effective implementation of the security controls that are identified in the Security Requirements;
- provide such further support and advice to the Panel as it may request;
- provide the Authority with such information and documents as it may reasonably request in relation to any matter referred by a Party to the Authority for determination pursuant to Section F2.7B;
- where a CPA Certificate for a Device Model expires or is withdrawn or cancelled by NCSC, then the Security Sub-Committee shall determine whether the Device Model is to be removed from the Central Products List;

Modifications

- establish a process under which the Code Administrator monitors Draft Proposals and Modification Proposals with a view to identifying (and bringing to the attention of the Security Sub-Committee) those proposals that:
    - are likely to affect the Security Obligations and Assurance Arrangements; or
    - are likely to relate to other parts of the Code but may have a material effect on the security of the End-to-End Smart Metering System,
- be entitled to submit Draft Proposals in respect of the Security Obligations and Assurance Arrangements where the Security Sub-Committee considers it appropriate to do so;
- notwithstanding and subject to the provisions of the Working Group Terms of Reference, the Security Sub-Committee shall be entitled to nominate a representative to be a member of any Working Group;
- for the purposes of Section D7.1 (Modification Report) written representations in relation to the purpose and effect of a Modification Proposal may be made by the Security Sub-Committee and/or any Security Sub-Committee member;

SMIRT

- oversee the management of any security incidents and vulnerabilities reported by industry, joining the Smart Metering Incident Response Team (SMIRT) as necessary.

2. Out of Scope

The role of the SSC does not include the following:

a) Any activity outside of those above unless otherwise directed by the Panel or transferred by a Transitional Group;

b) Activities that do not contribute to achievement of SEC objectives;

c) Setting policies that fall under the remit of the Panel or another Sub-Committee; and

d) Managing National Emergencies which fall under the remit of NCSC.

3. Proceedings of the SSC

3.1 Meeting Frequency

The SSC shall hold meetings with such frequency as it may determine or the SSC Chair may direct, but in any event shall meet at least every two months but as frequently as business demands. In practice, the SSC is meeting twice a month.

3.2 Quorum

No business shall be transacted at any meeting of the SSC unless a quorum is present at that meeting. The quorum for each SSC meeting shall be one half of all SSC Members appointed at the relevant time, at least one of whom must be the SSC Chair or the SSC Chair's nominated alternate.

3.3 Meeting Notice and Papers

Each meeting shall be convened by the Secretariat. A minimum of five Working Days' notice shall be provided (or such shorter notice as directed by the Panel, or the SSC Chair).

Notice of each meeting shall be accompanied by:

a) Time, date and location of the meeting;

b) Arrangements for those wishing to attend the meeting by means other than in person; and

c) Agenda and supporting papers.

3.4 SSC Chair

The SEC Panel shall approve the appointment of the SSC Chair in accordance with SEC Section G7.5 and shall review the appointment in three years from the date of appointment.

Selection of the SSC Chair shall be determined by the SEC Panel, providing the selection ensures that:

(a) the candidate selected is sufficiently independent of any particular Party or class of Parties;

(b) the Security Sub-Committee Chair is appointed for a three-year term (following which he or she can apply to be re-appointed);

(c) the Security Sub-Committee Chair is remunerated at a reasonable rate;

(d) the Security Sub-Committee Chair's appointment is subject to Section C6.9 (Member Confirmation), and to terms equivalent to Section C4.6 (Removal of Elected Members);

(e) provision is made for the Security Sub-Committee Chair to continue in office for a reasonable period following the end of his or her term of office in the event of any delay in appointing his or her

successor; and

(f) where the Security Sub-Committee Chair's appointment (and for the purposes of this Section and Section G7.5A all references to appointment shall encompass re-appointment) is to take effect on or after the date this Section G7.5(f) comes into force, the Panel shall:

(i) notify the Secretary of State of the appointment it proposes to make;

(ii) not make the appointment unless and until the Secretary of State has confirmed in writing that they do not object to the appointment being made;

(iii) ensure that the terms of the appointment include terms which provide for the Panel to terminate the appointment where directed to do so by the Secretary of State pursuant to Section G7.5A and from such date or within such period as may be specified in the Secretary of State's direction; and

(iv) where the appointed person has not, at the date of the appointment, passed (as a minimum) a Security Check (or equivalent), ensure that the terms of the appointment include terms which:

(A) require the appointed person to apply for a Security Check (or equivalent) within one month of the date of the appointment;

(B) provide for the Panel to terminate the appointment if a Security Check (or equivalent) is not passed by the appointed person within 12 months of the date of the appointment (or such longer period as the Secretary of State may approve following a request from the Panel).

G7.5A The Secretary of State may, in respect of any Security Sub-Committee Chair appointment which takes effect on or after the date Section G7.5(f) comes into force, direct the Panel to terminate the appointment of the Security Sub-Committee Chair where the Secretary of State considers it necessary to do for the purposes of preserving the integrity of, and in the interests of maintaining, the security of the End-to-End Smart Metering System (or any part of that system).

G7.5B The Panel shall comply with any direction given to it by the Secretary of State pursuant to Section G7.5A.

The SSC Chair shall not be entitled to vote unless there is a deadlock, in which case the SSC Chair shall have the casting vote.

3.5 Powers and Voting

In accordance with C6.9 of the SEC:

- each SSC Member shall be entitled to attend, and to speak and vote at, every meeting of the SSC;
- all decisions of the SSC shall be by resolution. In order for a resolution of the SSC to be passed at a meeting, a simple majority of those SSC Members voting at that meeting must vote in favour of that resolution. In the event of a voting deadlock, the SSC Chair shall have the casting vote; and
- a resolution in writing signed by or on behalf of all the SSC Members shall be as valid and effective as if it had been passed at a meeting of the SSC duly convened and held. Such a resolution may be signed in any number of counterparts.

3.6 Membership

The Panel shall invite applications from individuals to serve on the SSC in accordance with SEC Section G7. Those individuals shall be of suitable experience and qualifications required to fulfil the duties of the SSC.

Members shall act independently, not as a delegate, and without undue regard to the interests, of any Related Person and will act in a manner designed to facilitate the performance by the Panel of its duties under the SEC.

Members may propose another natural person to act as their Alternate by completing the necessary paperwork and notifying SECAS. The Alternate, once approved, may attend the SSC and must act in the capacity as Alternate to discharge the member's duties. The Alternate must complete the declaration as described in SEC C3.8 (a) and (c) prior to voting.

The membership of the SSC shall be composed of the persons outlined in SEC Section G7.3.

Smart Metering Incident Response Team (SMIRT) – A sub-group of the SSC, which includes SSC members but provides a forum of SSC security experts, together with other subject matter expertise as may be required (including Device manufacturers, HAN / WAN communications specialists, NCSC etc.). Its purpose is, when requested by the SSC, to monitor reports of major security incidents and vulnerabilities that have been reported to the SSC and to pro-actively assist in the management and resolution of security incidents where requested to do so by Users or the DCC. SMIRT has its own Terms of Reference approved by the SSC.

SSC CPA Issue Resolution Sub-Group (SCIRS) – A sub-group of the SSC, which includes all participants involved in or affected by the CPA process. This includes SSC members, Device Manufacturers, NCSC, DESNZ, CPA Test Laboratories, MAPs and Triage Facility Providers. Its purpose is to facilitate the CPA evaluation process by providing a working level forum through which SSC, DESNZ and NCSC can work together with key industry partners to 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. SCIRS has its own Terms of Reference approved by the SSC.

3.7 Term of Office

The SSC Chair will review membership of the Sub-Committee on a two-yearly basis, inviting applications from individuals in accordance with SEC Section C6.7. The normal term of office for each member is 24 months. For the first term of office half the membership will serve a 12-month term to preserve knowledge within the Sub-Committee. An annual Election will be scheduled for the Members whose end of term is approaching.

3.8 Other Interested Parties

In addition to the core SSC members, the SSC Chair is entitled to invite any persons the SSC determines it appropriate to do so. Such persons may include representatives of a SEC Party who are invited to discuss their User Security Assessment Report and response, and any such persons who will be able to provide the SSC with expert advice on security matters.

Representatives of the Secretary of State and the Authority are entitled to attend and speak at the SSC meetings and will be provided with copies of all agendas and supporting papers.

3.9 Member Confirmation

Before a person may serve on the SSC, that person shall provide written confirmation to SECCo that:

- they agree to serve on the SSC in accordance with the SEC, including Section G7;
- they will be available as reasonably required by the Sub-Committee to attend at least 50% of meetings and miss no more than 3 meetings in a row. Members should also be prepared to undertake some work outside of meetings;
- they shall act independently, not as a delegate, and act at all times in a manner designed to assist the performance by the SSC of its duties under the SEC;
- they shall be prepared to promptly give their expert view and contribute to discussions on matters within the scope of these Terms of Reference and seek views from their Party Category where appropriate and possible in accordance with the Panel Information Policy.

3.10 Conflict of Interest

Given that members have a duty to act independently, conflicts of interest should not regularly arise, but members may act in accordance with that of C5.24 – C5.26. In such cases the member shall absent themselves from the meeting for the purposes of that decision. It is the responsibility of each Member to declare to the SSC Chair any actual or perceived conflict of interest with their duties as an SSC Member. In such circumstances the Member may choose to absent themselves from proceedings or from voting, the SSC Chair may also request that a Member absents themselves. Any decision of the SSC Chair in this regard shall be final and binding.

Conflict of Interest Scenario	Outcome
Scenario 1 - The User Security Assessment for the employer of an SSC Member is being reviewed by the SSC. This could relate to an SSC member whose employer is a Supplier, Network Operator, Other User or a Shared Resource Provider.	Outcome 1 - SSC Members to declare a conflict of interest and to leave the room if requested to do so where the SSC is considering an assurance status or compliance status for their employing organisation.
Scenario 2 - The User Security Assessment for a Shared Resource Provider (SRP) is being reviewed by the SSC and the employers of other SSC Members have a contract with that SRP.	Outcome 2 - SSC Members to declare a conflict of interest and to leave the room if requested to do so by the SSC Chair where the SSC is considering an assurance status or compliance status for a Shared Resource Provider and the employer of an SSC Member has a contract with that SRP.
Scenario 3 - The User Security Assessment for a User who has a Shared Resource Provider (SRP) is being reviewed by the SSC and the employers of other SSC Members either has a contract or is contemplating a contract with that SRP.	Outcome 3 - Where an SSC Member's employing organisation has or is contemplating a contractual relationship with a Shared Resource Provider providing services to a User whose User Security Assessment is being reviewed, the SSC Member should declare that information to demonstrate transparency.
Scenario 4 – The SSC is considering removing a Device from the CPL and an SSC member has a direct relationship with the Device Manufacturer.	Outcome 4 - SSC Members to declare a conflict of interest to demonstrate transparency where the SSC is considering the removal of that Device from the CPL.
Scenario 5 – The SSC is considering Live Service Criteria for a new DCC service or enrolled SMETS1 DMC and an SSC member	Outcome 5 – Where the SSC is considering Live Service Criteria and the SSC member has a direct relationship with any of the parties involved, the SSC member should declare a conflict of interest

Conflict of Interest Scenario	Outcome
has a direct relationship with any of the parties involved.	to demonstrate transparency and leave the room if required to do so by the SSC Chair.

4. Membership of the SSC

The table below sets out the composition of the SSC, pursuant to section G7. Members and their Alternates must have sufficient experience, qualification, have been successfully screened in accordance with BS 7858 and hold security expertise.

Member Group	Numbers
Large Suppliers	6
Small Suppliers	2
Gas Networks	1
Electricity Networks	1
Other User	1
Shared Resource Providers*	1
DCC Representative	1

*The Shared Resource Provider representative will be appointed from the list of SEC Parties who have become fully qualified Shared Resource Providers in their own right (usually Other SEC Parties), having been approved by the SSC.

Representatives of the TABASC, Secretary of State and the Authority shall be invited to attend each and every SSC meeting. The SSC Chair is able to invite any persons that the SSC determines is appropriate as determined in Section 3.8.

5. Secretariat

SECAS will provide the secretariat and code management for the SSC. This includes but is not limited to:

- Prepare and maintain the SSC Member Pack (code of conduct and expenses policy);
- Timetable and organise the SSC , SCIRS and SMIRT meetings, including meeting rooms;
- Act as quality gatekeeper with the SSC Chair for accepting papers;
- Circulate agendas and papers for consideration at SSC meetings, 5 Working Days in advance of that meeting date;
- Monitor the quorum prior to meetings to ensure that decision matters are not frustrated or deferred;
- Circulate minutes of the meeting five working days after the meeting for the SSC's approval;
- Administer the circulation list for SSC papers and minutes;
- Manage the SSC decisions, actions and risks log;
- Manage the SSC section of the SEC website;

- Manage the appropriate tools utilised by DCC, Users and Manufacturers for security incidents and the management of vulnerabilities;
- Manage the SSC Egress Workspace; and
- Support the operation of the SSC and the fulfilment of its duties through:
    - co-ordination, and where directed by the SSC undertaking, all inputs, analyses, assessments and consultations required to support the SSC business;
    - preparation of the draft SSC input to the Panel's annual report (July) SEC 2.3(h) for the SSC's approval; and
    - the co-ordination of the SSC's role in the SEC Modifications Process through the relevant SECAS Modification lead(s) to ensure a holistic and efficient process exists between the SSC and the Change Board.

6. Review

The Terms of Reference, membership and operation of the SSC may be reviewed by the Chair at any time to ensure that they remain appropriate to reflect the duties and requirements of the SEC.

Amendments to these Terms of Reference will be reviewed by the SSC and approved by the Panel.

7. Confidentiality and Disclosure

Given the sensitive nature of the work of the SSC, agenda items, papers and discussions will be assigned an information sharing level of either CLEAR, GREEN, AMBER, AMBER-STRICT or RED and 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. All recipients must have signed an NDA stating their acceptance to abide by these terms. 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 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 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 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

Information sharing levels will be suggested by participants when providing information and determined by the Chair.

Each SSC Member will be asked to undertake in writing to abide by the confidentiality and disclosure provisions in relation to each information sharing level as described above, by signing the Confidentiality and Disclosure Agreement which will be shared by SECAS via DocuSign.

Individuals who the SSC Chair has invited to attend a meeting of the SSC will also be asked to sign the Confidentiality and Disclosure Agreement but will only be permitted to attend the SSC during discussions on agenda items relevant to their organisation or subject matter expertise.

SSC Members who breach the rules of the confidentiality and disclosure provisions under any information sharing level may have their SSC membership ceased. The confidentiality and disclosure agreement can be found in Appendix A.

8. Definitions

Term	Definition
CPA Security Characteristics	Means the documents published from time to time on the NCSC website that set out the features, testing and deployment requirements necessary to obtain a CPA Certificate in respect of one or more of the following: (a) 'Gas Smart Metering Equipment'; (b) 'Electricity Smart Metering Equipment'; (c) 'Communications Hubs'; (d) 'HAN Connected Auxiliary Load Control Switches'; (e). 'Standalone Auxiliary Proportional Controller'
DCC Total System	The Systems used by the DCC and/or the DCC Service Providers in relation to the Services and/or this Code, including the DCC User Interface, the SMETS1 SM Wide Area Network (WAN), the SMETS2+ SM WAN and Communications Hubs (CHs) except for those CHs which are: (a) SMETS1 CHs; (b) neither installed nor in the possession of the DCC; and/or (c) installed, but not Commissioned.
End to End Security Architecture	means a document that describes how the security controls in respect of smart metering relate to the architecture of the End-to-End Smart Metering System.
End to End Smart Metering System	The DCC Total System, all Enrolled Smart Metering Systems and all Registration Data Provider (RDP) Systems.
Enrolment	In respect of a Smart Metering System, the act of enrolling that Smart Metering System in accordance with the Enrolment Service (and the words "**Enrol**" and "**Enrolled**" will be interpreted accordingly).
Enrolled Smart Metering System	A Smart Metering System that has been Enrolled.
HCALC	means a HAN Connected Auxiliary Load Control Switch.
JICSIMP	means the Joint Industry Cyber Security Incident Management Plan. This document sets out the plan for the joint handling and management as necessary by the Smart Energy Code (SEC) and Security Sub-Committee (SSC), government and industry of cyber security incidents originating from, or impacting on, smart metering operations within Great Britain.
Standalone Auxiliary Proportional Controller (SAPC)	means a device installed (or to be installed) at a premises, which:(a) consists of the components or other apparatus identified in; and (b) as a minimum, has the functional capability specified by and complies with the other requirements of, a Version of the SAPC Technical Specification which was within its Installation Validity Period on the date on which the device was installed.
SSC CPA Issue Resolution Sub-Group (SCIRS)	A sub-group of the SSC, its purpose is to facilitate the CPA evaluation process by providing a working level forum through which SSC, DESNZ and NCSC can work together with key industry partners to 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
Smart Metering Incident Response Team (SMIRT)	Its purpose is, when requested by the SSC, to monitor reports of major security incidents and vulnerabilities that have been reported to the SSC and to pro-actively assist in the management and resolution of security incidents where requested to do so by Users or the DCC.

Term	Definition
Party Category	means, as the context requires, one of the following categories; (a) the Large Supplier Parties collectively; (b) the Small Supplier Parties collectively; (c) the Electricity Network Parties collectively; (d) the Gas Network Parties collectively; (e) the Other User Parties collectively; (f) the Shared Resource Providers collectively; and (g) the Other SEC Parties collectively.
Voting Group	In respect of each Party Category, each Party that falls into that Party Category collectively with that Party's Affiliates (if any) who also fall into that Party Category.

Appendix A – NDA Form

Confidentiality and Non-Disclosure Agreement (NDA)

I, the undersigned, have read and understood the Security Sub-Committee (SSC) Terms of Reference (ToR). I confirm that I have sufficient security expertise and understand that I must successfully achieve security clearance in accordance with BS 7858. I understand that I am required to comply with the confidentiality and disclosure obligations in respect of each of the five information sharing levels Clear, Green, Amber, Amber-Strict and Red), as set out in the Panel's Information Policy. I understand that I must declare any conflict of interest that I have to the SSC Chair whether it exists now or during my continued membership of the group, as soon as I become aware that such a conflict exists. I understand that should I fail to abide by the information sharing levels confidentiality and disclosure obligations or conflict arrangements (as set out in the SSC's ToR) I may be excluded from the SSC. Having understood and accepted the above statements, I therefore agree to abide by these ToR in my engagement with this Sub-Committee.
Name:
SEC Party Category (If Appropriate):
Primary/Alternative Participant (delete as appropriate)
Signature:
Date: