SEC
Smart Energy Code

MP326

'Changes to G2.22A and G2.22B to improve DCC Service Provider Security testing requirements'

Modification Report

Version 1.0

21 July 2026

This document has a Classification of Clear

About this document

This document is a Modification Report. It currently sets out the background, issue, solution, impacts, costs, implementation approach and progression timetable for this modification, along with any relevant discussions, views and conclusions.

Contents

This document also has one annex:

- **Annex A** contains the redlined changes to the Smart Energy Code (SEC) required to deliver the Proposed Solution.

Contact

If you have any questions on this modification, please contact:

Lydia Bentley

020 3922 0748

lydia.bentley@talan.com

1. Summary

This proposal has been raised by Gordon Hextall on behalf of the SEC Security Sub-Committee (SSC).

The Modification aims to address deficiencies in the current security testing arrangement for services provided and/or procured by the Data Communications Company (DCC), where those services are able to affect the Supply of Energy into a consumer's property. The current arrangements do not fully encompass the aforementioned services and so must be amended. Additionally, as the DCC act as both the Dual Control Organisation (DCO) and the Enduring Change of Supply (ECoS) Provider, this distinction must be addressed within the scope of the Modification.

This Modification Proposal has been raised with legal drafting contributed by the Department of Energy Security & Net Zero (DESNZ), with support from the SSC and the DCC, and aims to minimise the risk of conflicts of interest between different "arms" of the DCC's various service provisions, whilst providing increased confidence to Users of DCC Services, and consumers.

This modification impacts the DCC only, with the cost to implement limited to SEC implementation costs. The modification is targeting an ad hoc SEC Release, one Working Day following the closure of the appeal window.

2. Issue

What are the current arrangements?

SEC Section G 'Security' Requirements

SEC Section G 'Security' provides for arrangements to prevent critical systems from being subject to vulnerabilities. This is achieved through obligations on SEC Parties and Users in respect of their responsibilities as service users and providers, with specific reference to those services provided by the DCC. Security obligations on the DCC are found in SEC Section G clauses G2, G5, G6 and G9, including those relating to security arrangements in respect of the DCC Live System.

Paragraph G2.22B details requirements on the DCC in respect of paragraphs (b) and (c) of the DCC Live System definition (see below), and creates, amongst others, the following obligations:

> *G2.22B The DCC shall ensure that:*
>
> *(f) any independent security testing of a relevant system that is used to provide assurance must be carried out by an organisation which is a CHECK approved service provider or a CREST certified tester but is not an organisation that:*
>
> *(i) designed or developed any relevant system; or*
>
> *(ii) is an Affiliate or Related Undertaking of an organisation that has designed or developed any relevant system.*

This requirement is in place in to ensure appropriate security provisions in respect of services provided by the DCC. CHECK is the scheme under which National Cyber Security Centre (NCSC)

assured companies can conduct authorised penetration tests of public sector and Critical National Infrastructure (CNI) systems and networks[1]. CREST is an international not-for-profit, membership body representing the global cyber security industry[2]; they provide accreditation for groups who perform, amongst other things, penetration testing.

G2.22B(f)(i) requires that the DCC do not allow testing on a system by any individual involved in the design or development of any relevant system. Relevant system is defined as follows:

> *G2.22A The requirements set out in Section G2.22B apply in relation to:*
>
> *(a) the part of the DCC Total System which is referred to in paragraph (b) of the definition of DCC Live Systems in Section A1 (Definitions); and*
>
> *(b) the part of the DCC Total System which is referred to in paragraph (c) of the definition of DCC Live Systems in Section A1 (Definitions),*
>
> *each of which is as a '**relevant system**' for the purposes of Section G2.22B.*

Relevant Systems & The DCC Live System

The DCC Live System is defined in SEC Section A 'Definitions & Interpretations' as follows:

> *means those parts of the DCC Total System which are used for the purposes of:*
>
> *a. (other than to the extent to which the activities fall within paragraph (b), (c), (f), (g), (h), (i) or (j) below) processing (including Countersigning of SMETS1 Responses, SMETS1 Alerts and S1SP Alerts, but not Countersigning of SMETS1 Service Requests) Service Requests, Pre-Commands, Commands, Instructions, Service Responses and Alerts, holding or using Registration Data for the purposes of processing Service Requests and Signed Pre-Commands, and providing the Repository Service;*
> *b. Threshold Anomaly Detection (other than that carried out by a DCO, a SMETS1 Service Provider or the CoS Party) and (other than to the extent to which the activity falls within paragraph (d), (f), (g), (h), (i) or (j) below) Cryptographic Processing relating to the generation and use of a Message Authentication Code and Countersigning SMETS1 Service Requests;*
> *c. discharging the obligations placed on the DCC in its capacity as CoS Party;*
> *d. providing SMKI Services;*
> *e. the Self-Service Interface;*
> *f. creating, using, storing or destroying the Contingency Private Key, the Contingency Symmetric Key or the Recovery Private Key (except where each such key is being stored in an unusable form because it is or is being split into multiple parts as described in Appendix L (SMKI Recovery Procedure) or in the Organisation CPS;*
> *g. the Production Proving Systems;*
> *h. discharging the obligations of any SMETS1 Service Provider in its capacity as such;*
> *i. discharging the obligations of any DCO in its capacity as such; and*
> *j. discharging the obligations of the CSS Provider in its capacity as such.*

When the above definition and the definition of a 'Relevant System' (as found in G2.22A) are taken together, the requirements given in G2.22B apply to those parts of the DCC Total System which are

[1] CHECK penetration testing | National Cyber Security Centre
[2] Who Is CREST Global Cyber Security Accreditation Body

used for Threshold Anomaly Detection, and those parts of the DCC Total System used in the Change of Supply Party capacity. This means that any individual who has been involved in one of these systems may not be part of testing of that same system, or the other system. No other elements of the DCC Total System or DCC Live System are therefore in scope of the testing obligations given in G2.22B.

What is the issue?

DCC Service Providers (SP) who have the capability to affect the flow of energy to consumers (Data Service Providers (DSP), the Dual Control Organisation (DCO) and the Enduring Change of Supplier (ECoS) Provider) should be subject to penetration testing by a CHECK accredited organisation or a CREST certified tester. However, Section G does not sufficiently provide for this in its current iteration.

Notably, as G2.22A only refers to parts (b) and (c) of the DCC Live System definition, some parts of the DCC Total System are exempt from the testing regime obligated by G2.22B, such as the Dual Control Organisation (DCO), a function that may, by some of its actions, affect the flow of energy into a consumer's home.

Furthermore, any change to expand the scope of the testing requirements to encompass the DCO would need to recognise that the DCO and the ECoS Party, referred to in part (c), are functionally the same organisation, as both roles are filled by the DCC. The current wording of G2.22B would create a distinction between the DCO and the ECoS Party, which would be unnecessary and inappropriate as it would create an artificial distinction within the DCC that may affect the application of testing.

Additionally, the current provisions do not apply in respect of the DCC's Data Service Provider(s). A new clause is required to ensure that they are subject to the same testing arrangements as other obligation groups as per G2.22A.

As a result, the current drafting:

- Does not encompass the DCO and the DCC's DSPs;
- Does not provide for sufficient distinction between the ECoS Provider and the DCO (were it to be included), even though both of these roles are currently filled by the DCC; and
- would not be able to provide for testing independence between the DCC SPs, which is needed to satisfy concerns related to conflicts of interest.

What is the impact this is having?

Without the Proposed Solution, there is an unmitigated risk of conflict of interest with respect to certain penetration testing scenarios. As such, it is important to identify and implement a means by which the testing regimes for critical systems are made more robust.

Impact on consumers

No consumer impact has been identified.

What is the priority of this modification?

The priority of this modification has been determined as **Standard**. This rating is based on perceived impacts on:

- Code Reform & Net-Zero
- Smart & Retail Operations
- Digitalisation

Please refer to Appendix 3 for a full breakdown of how the priority score was calculated.

3. Solution

Proposed Solution

The Proposer is seeking to make changes to SEC Section G, G2.22A and G2.22B, to improve DCC Service Provider security testing requirements. These drafting changes will affect the following:

- Expansion of the scope of the current testing arrangements to include the DCO, the ECoS Party and the DCCs Data Service Provider(s), as bodies with the ability to affect the flow of power to a consumer's property;
- separation between the DSP and the DCO, and between the DSP and the ECoS Party;
- a demarcation between the DCO and the ECoS Party as separation between them is unnecessary for security purposes is;
- a requirement for independent CHECK or CREST Penetration Testing for all three Service Providers (DSP, DCO, ECoS Provider); and
- a requirement that security testing must not be done by an affiliate i.e. part of an organisation that has designed or developed the systems they are testing.

The changes to the SEC required to realise the Proposed Solution have been drafted by DESNZ, in collaboration with the Security Sub-Committee, and the DCC's Chief Information Security Officer (CISO).

4. Impacts

This section summarises the impacts that would arise from the implementation of this modification.

SEC Parties

SEC Party Categories impacted			
	Large Suppliers		Small Suppliers
	Electricity Network Operators		Gas Network Operators
	Other SEC Parties	✓	DCC

There are no direct impacts on any SEC Party arising from the Proposed Solution. Whilst certain elements of the DCC Total System will be subject to modified security testing arrangements, neither the DCC nor its Service Providers will need to make any active changes to their System or operations to accommodate the new testing approach.

DCC Systems

DCC System changes

There are no impacts on the DCC System or traffic across the DCC System because of this Modification Proposal.

DCC System traffic

There are no impacts on the DCC System or traffic across the DCC System because of this Modification Proposal.

SEC and subsidiary documents

The following parts of the SEC will be impacted:

- Section G 'Security'

The changes to the SEC required to deliver the proposed solution can be found in Annex A.

Devices

No Device impacts are expected to arise from the Proposed Solution.

Consumers

There are no impacts on Consumers because of this modification.

Other industry Codes

There are no impacts on other industry Codes because of this modification.

Greenhouse gas emissions

There are no impacts on greenhouse gas emissions because of this modification.

5. Costs

DCC costs

No DCC costs have been identified in relation to the Proposed Solution, as this is a legal text-only Modification that does not require any DCC System changes.

SECAS costs

The estimated SEC implementation cost to implement this as a stand-alone modification is one days of effort, amounting to approximately £600. This cost will be reassessed when combining this modification in a scheduled SEC Release. The activities needed to be undertaken for this are:

- Updating the SEC and releasing the new version to the industry.

SEC Party costs

No SEC Party costs are anticipated as a result of the Proposed Solution.

6. Implementation approach

Recommended implementation approach

The Change Sub-Committee have approved an implementation date of:

- **Ad hoc SEC Release** 1 Working Day following the closure of the Self-Governance appeal window

The SEC Change Team recommended this approach as this is a legal text only Modification with no DCC technical impact, and with no impact (either operationally or financially) on any SEC Party. Furthermore, without this change being implemented in the SEC, the risk of unresolved conflicts of interest remains with respect to the testing arrangements in place for critical systems.

7. Assessment of the proposal

Areas for assessment

Sub-Committee input

The SEC Change team has determined what input is required from the Finance Sub-Commmittee (FSC), Operations Group (OPSG), the Performance Assurance Board (PAB), the Privacy Sub-Committee (PSC), the Smart Meter Device Assurance Sub-Committee (SMDASC), the SSC, the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA), the Technical Architecture and Business Architecture Sub-Committee (TABASC) and the Testing Advisory Group

(TAG) to confirm. The SEC Change team believes the following Sub-Committees will need to provide the following input to this modification:

Sub-Committee input	
Sub-Committee	**Input sought**
FSC	No input sought on the basis that there is no impact on the functions of this Sub-Committee.
OPSG	No input sought on the basis that there is no impact on the functions of this Sub-Committee.
PAB	No input sought on the basis that there is no impact on the functions of this Sub-Committee.
PSC	No input sought on the basis that there is no impact on the functions of this Sub-Committee.
SMDASC	No input sought on the basis that there is no impact on the functions of this Sub-Committee.
SMKI PMA	No input sought on the basis that there is no impact on the functions of this Sub-Committee.
SSC	The Modification Proposal has been raised by the Security Sub-Committee, and the Chair does not consider that it needs return for any further discussion unless any clarification requests are raised.
TABASC	No input sought on the basis that there is no impact on the functions of this Sub-Committee.
TAG	No input sought on the basis that there is no impact on the functions of this Sub-Committee.

Observations on the issue

Prior to the Modification being raised, the underlying issue was discussed at the SSC. During these discussions, the scope of the problem was identified, and the Proposed Solution was expounded. The issue was discussed on three separate occasions by the SSC, each month from February 2026 to April 2026.

The Proposed Solution was iterated upon and developed at the SSC, with amendments made to the legal drafting following feedback. During the SSC discussion on 25 March 2026, a concern was raised that there could be an unintended consequence that would prevent the DCO and ECoS Party from being the same Provider. The legal drafting was then amended to resolve this concern.

This Modification was then discussed at the SEC Issues group meeting in June 2026, where SEC Parties and attendees were encouraged to provide feedback on the Issue. Namely, the SEC Change team prompted feedback on two points; whether the Issue has been sufficiently developed, and whether the proposed to take this Modification forward directly from being raised to Report Phase was appropriate. On these points, no feedback was offered against either position by the Issues group.

8. Case for change

Business case

There are no costs associated with the Proposed Solution, either for the DCC or for any SEC Party. Furthermore, no system changes are required, and no changes in operating practices by any party of the DCC or any SEC Party are required in order to accommodate the Proposed Solution. Furthermore, there are anticipated benefits to the SEC arising from the Proposed Solution in respect of the improvements to security arrangements governing critical systems.

Taken together, this presents a clear business case in favour of approval of this Modification Proposal, and therefore it is considered that a cost-benefit test has been met.

Views against the General SEC Objectives

Proposer's views

The Proposer considers that this Modification Proposal supports the sixth General SEC Objective to ensure the protection of Data and the security of Data and Systems in the operation of the Code;

Industry views

This Modification Proposal was presented at the SEC Issues Group in June 26. No issues, problems, risks or concerns were identified, and no individual present presented any views against the Modification Proposal.

Views against the consumer areas

Improved safety and reliability

This modification has a neutral impact on improving safety, however, the Proposed Solution will mitigate the risk of an adverse impacts on energy supply to consumers, and is therefore anticipated to support reliability.

Lower bills than would otherwise be the case

This modification has a neutral impact on lowering bills than would otherwise be the case.

Reduced environmental damage

This modification has a neutral impact on reducing environmental damage.

Improved quality of service

This modification has a neutral impact on quality of service.

Benefits for society as a whole

This modification has a neutral impact on benefits for society as a whole.

Final conclusions

This is a legal text-only Modification Proposal with universal support from all affected SEC Parties, raised by the Security Sub-Committee with drafting changes provided by DESNZ. No DCC System changes are required, there is no material impact on any SEC Party, and no costs have been identified. Furthermore, the Proposed Solution will provide a tangible benefit for SEC Parties by enabling greater confidence in the operation of vital DCC systems by applying a “common-sense” improvement to their arrangements governing the security of those systems.

Appendix 1: Progression timetable

Timetable	
Event/Action	**Date**
Draft Proposal raised	14 July 26
Modification Report approved by Change Sub-Committee (CSC)	21 July 26
Modification Report Consultation	*22 July 26 – 13 August 26*
Change Board Vote	*26 August 26*

Italics denote planned events that could be subject to change

Appendix 2: Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	**Full term**
CNI	Critical National Infrastructure
CSC	Change Sub-Committee
DCC	Data Communications Company
DCO	Dual Control Organisation
DESNZ	Department of Energy Security & Net Zero
ECoS	Enduring Change of Supply
DSP	Data Service Provider
FSC	Finance Sub-Committee
NCSC	National Cyber Security Centre
OPSG	Operations Group
PAB	Performance Assurance Board
PSC	Privacy Sub-Committee
SEC	Smart Energy Code
SMDASC	Smart Meter Device Assurance Sub-Committee
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TAG	Testing Advisory Group

NB – CREST and CHECK are names rather than acronyms or initialisms and are therefore not recorded in the above table.

Appendix 3: Prioritisation Matrix

Strategic Direction Statement Prioritisation				
SDS Alignment	**Importance**	**Complexity**	**Overall Total**	**Priority**
1	2	1	4	**STANDARD**

SDS Alignment – The Proposed Solution of this modification would support two aspects of the Strategic Direction Statement (SDS), which are:

- Consumers, Vulnerability and PSR; and
- Continue to drive benefits of smart meters through regulatory oversight of rollout and data flows.

Importance – This will allow the SEC to ensure that robust security arrangements are in place in respect of bodies who have the power to adversely affect the flow of energy into a consumer's property.

Complexity – This is a low-complexity Modification, on account of it having been raised with legal drafting provided, and scoping already completed by the SSC.