This document is classified as **White** in accordance with the Panel Information Policy. Information can be shared with the public, and any members may publish the information, subject to copyright.

SEC Modification Proposal Form – SECMP0065

Mod Title

SMETS1 Security obligations

Submission Date

5th October 2018

Details of Proposer	
Name:	Gordon Hextall
Organisation:	SEC Security Sub-Committee (SSC)
Contact Number:	+44 (0) 7774 179320
Email Address:	Gordon.hextall@seccoltd.com
Details of Representative (if applicable)	
Name:	Nick Blake
Organisation:	SECAS
Contact Number:	+44 (0)20 7090 7745
Email Address:	Nick.blake@gemserv.com

1. What issue are you looking to address?

To meet the original policy intent for the SMETS1 security obligations in SEC Section G, and particularly those in SEC Sections G3.26 to G3.28, to apply only from the date on which SMETS1 Devices start to be enrolled into the DCC. This will avoid the potential for Parties to be in breach of SEC obligations.

2. Why does this issue need to be addressed? *(i.e. Why is doing nothing not an option?)*

On 27 March 2018, BEIS issued a consultation letter seeking views on proposals to amend the SEC, the DCC Licence and energy supply licences to enable the provision of a SMETS1 Service by the DCC.

The Consultation document made it clear that the obligations were only intended to apply post enrolment of SMETS1 Devices – see extract below:

"Section 3.7. Aside from those contained within the technical specification itself, SMETS1 device security obligations currently sit within Conditions 40 and 46 of the gas and electricity supply licence standard conditions, respectively. These conditions apply only to systems operating outside the DCC, and there is therefore a need to ensure energy suppliers continue to be subject to obligations regarding device security and testing post enrolment."

Following consideration of stakeholder responses, BEIS published its conclusions on 4 June 2018 and laid the regulatory changes before Parliament in line with the procedure under Section 89 of the Energy Act 2008, with the changes coming into legal effect on 18 July 2018.

Unfortunately, the SEC drafting doesn't make it clear that the obligations only apply post enrolment. The legal effect is that the obligations apply now and do not allow time for the necessary planning by Users, the SSC and the User CIO. An example of the impact is:

"SMETS1 Smart Metering Systems

G3.26 Each Supplier Party shall use its best endeavours to ensure that each SMETS1 SMS for which it is the Responsible Supplier is at all times Secure.

G3.27 Each Supplier Party shall retain documentary evidence sufficient to demonstrate its compliance with the obligation at Section G3.26.

G3.28 For the purposes of Section G3.26:

*(a) a SMETS1 SMS is "**Secure**" if it is designed, installed, operated and supported so as to ensure, to an Appropriate Standard, that it is not subject to any event which results, or is capable of resulting, in any Device of which it is comprised being Compromised to a material extent; and*

*(b) an "**Appropriate Standard**" means a high level of security that is in accordance with good industry practice within the energy industry in Great Britain, and is capable of verification as such by the User Independent Security Assurance."*

The implications of these obligations are that:

- The SMETS1 Device volumes should be aggregated with the SMETS2 Device volumes to determine the type of the next User Security Assessment. Thus, Suppliers with more than 250,000 SMETS1 and SMETS2 Devices in aggregate will be subject to a Full User Security Assessment; this has not yet been planned for by Users or the User CIO;
- The SSC has an obligation (G7.19) to maintain the Security Controls Framework (SCF) to provide guidance to Users and the User CIO *"to ensure that security assurance assessments are proportionate, consistent in their treatment of equivalent Users and equivalent User Roles and achieve appropriate levels of security assurance…."* The SEC obligations have not allowed time for the SSC to develop the SCF to provide the necessary advice and guidance on what constitutes an 'Appropriate Standard';
- The User CIO assessors will need training on assessing whether SMETS1 Devices are secure to an 'Appropriate Standard' and this cannot be undertaken until the SSC advice and guidance is available;
- Without the SEC Modification, the existing SEC obligations could result in Parties being in breach of the SEC if they are operating SMETS1 Devices that cannot be assessed by the User CIO during scheduled User Security Assessments because the appropriate guidance to underpin the assessment has not yet been developed.

Since 2012, Suppliers have been subject to the SMETS1 Device security obligations in Conditions 40 and 46 of the gas and electricity Supply Licence, and these obligations continue to be in force.

The SSC is therefore satisfied that there is no increased security risk if the SMETS1 SEC obligations are deferred until post enrolment, which was the clear policy intent which has been re-confirmed by the BEIS Smart Metering Head of Delivery.

3. What is your Proposed Solution?

The SSC wishes to implement a SEC modification to defer the SMETS1 security obligations until the date from which SMETS1 Devices are enrolled into the DCC.

This will enable the necessary planning to take place by the SSC, Users and the User CIO and for the SCF to be updated to provide advice and guidance on an 'Appropriate Standard'.

As a precursor to developing the SCF guidance, the SSC has already initiated a survey of energy Suppliers with a questionnaire that was issued on 27 September 2018 to identify existing industry good practice as referenced in SEC G3.28(b).

4. What SEC objectives does this Modification better facilitate?

This change would help to facilitate SEC Objective (g) (to facilitate the efficient and transparent administration and implementation of this Code) by providing clear guidance for energy Suppliers on the nature of their SEC User Security Assessments.

5. What is the requested Path type?	Path 3

Path 3: Self Governance:

The Proposer does not believe this modification will result in a material impact on competition or create undue discrimination between classes of Party, as per the requirements in SEC Section D2.6 for needing an Authority determination.

6. Are you requesting that the Modification Proposal be treated as Urgent?	Yes

The Proposer is seeking for this modification to be implemented urgently. The rationale is that, if the User CIO undertakes User Security Assessments of SMETS1 Devices without clear advice and guidance on an 'Appropriate Standard' being provided in the SCF, then there is likely to be different standards applied to different Suppliers.

This Change would facilitate the following urgency criteria set by Ofgem;

- (a[1]) A significant commercial impact on parties, consumers or other stakeholder(s) as Supplier Parties could have a larger User Security Assessment than expected.
- (c[2]) A party to be in breach of any relevant legal requirements as Supplier Parties may wrongly believe that they are in breach of SEC Section G of the SEC.

7. What is your desired implementation date?

Early November 2018.

8. Which SEC Parties are expected to be impacted? (Please mark with an X)

Large Supplier Parties	x	Small Supplier Parties	x
Electricity Network Parties		Gas Network Parties	
Other SEC Parties			

This modification will affect all Non-Domestic Suppliers who are affected by the BEIS Government Response.

9. Which parts of the SEC will be impacted?

SEC Section G

[1] A significant commercial impact on parties, consumers or other stakeholder(s).
[2] A party to be in breach of any relevant legal requirements.

10. Will there be an impact on Central Systems? (Please mark with an X)			
DCC Systems		Party interfacing systems	
Smart Metering Systems		Communication Hubs	
Other systems			
Not applicable.			

11. Will there be any testing required?
None

12. Will this Modification impact other Energy Codes?	No
Not applicable	

13. Will this Modification impact Greenhouse Gas Emissions?	No
Not applicable	