

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.

Stage 03: Final Modification Report

SECMP0057:

Users to notify SSC of a second or subsequent User System

What stage is this document in the process?

- 01 Initial Assessment
- 02 Refinement Process
- 03 Modification Report**
- ▶ 04 Decision

SECAS Contact:

Name:
Cordelia Grey

Number:
020 7090 1072

Email:
SEC.Change@gemserv.com

Summary

This modification seeks to ensure that Users inform the Security Sub-Committee (SSC) when they are seeking to utilise a second or subsequent User System which may or may not be provided or operated by a Shared Service Provider.

Working Group Conclusions



- The Working Group **unanimously** believe that SECMP0057 should be **approved**.

Impacts



- All Party Categories
- There are no impacts on Data Communications Company (DCC) Central Systems and/or Party interfacing systems

SECMP0057

Final Modification Report

12 December 2018

Version 1.1

Page 1 of 17

This document is classified as **White**

© SECCo 2018



Content

1. Summary	3
2. What is the issue?	5
3. Proposed Solution	6
4. Impacts	8
5. Costs	9
6. Implementation	10
7. Working Group Discussions	11
8. Working Group Conclusions	14
9. Panel discussions & conclusions	16
Appendix 1: Glossary	17

About this Document

This document is the Final Modification Report (FMR) for SECMP0057. This document provides detailed information on the issue, solution, impacts, costs, industry consultation as well as the Working Group (WG) and Panel discussions and conclusions on the modification.

This document has three attachments:

- Attachment A contains the legal text changes to support this modification;
- Attachment B contains the full responses received to the Working Group Consultation; and
- Attachment C contains the full responses received to the Modification Report Consultation.

The Change Board will consider this modification at its meeting on 19 December 2018, where it will determine whether SECMP0057 should be approved or rejected.

1. Summary

What is the issue?

Under the current arrangements there is no obligation on Users to notify the SSC or any other party before they begin to utilise a second or subsequent User System. Nor is there a requirement for there to be a User Security Assessment of a second or subsequent User System.

Due to the interconnected nature of the DCC Central Systems there is a risk to the overall security of smart metering if a second or subsequent User System is introduced without any formal consideration of the security risks.

What is the Proposed Solution?

This modification seeks to require all Users to notify the SSC before they begin to utilise a second or subsequent User System. This will enable the SSC to consider the security risks and to advise the User accordingly once the SSC has made its decision on whether to wait to review the second or subsequent User System at its next annual review or to arrange an ad-hoc review.

Impacts

Party

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

System

There are no impacts on DCC Central Systems or Party interfacing systems and there is no testing required as part of the implementation of this modification.

Implementation Costs

The estimated cost to implement SECMP0057 is approximately £2,400 and is limited to SEC administration time and effort to deliver the necessary SEC changes.

SECMP0057

Final Modification Report

12 December 2018

Version 1.1

Page 3 of 17

This document is classified as **White**

© SECCo 2018



Implementation Date

The Panel agreed an implementation date of:

- **28 February 2019** (February 2019 SEC Release), if a decision to approve is made by 14 February 2019; or
- 10 Working Days following approval if a decision is received after 14 February 2019.

Working Group Establishment

The Panel agreed at the August 2018 Panel meeting, that the SSC should act as a Working Group for SECMP0057.

Working Group's views

The Working Group believed unanimously that SECMP0057 better facilitates the SEC Objectives (a), (e) and (g).

The Working Group therefore believed that this Modification Proposal should be **approved**.

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 4 of 17

This document is
classified as **White**

© SECCo 2018



2. What is the issue?

Background

At present, there is no SEC requirement for a second or subsequent User System to go through a User Security Assessment before becoming operational, and there is no obligation to notify the SSC when a second or subsequent User System is to be utilised. The current SEC arrangements assume that a User will have a single User System which may be provided in-house or by a Shared Resource Provider, and the whole of the User Security Assessment process is based on that assumption.

What is the issue?

Due to the interconnected nature of systems supporting smart metering, there could be a risk to the overall security of smart metering if a second or subsequent User System is introduced by a User without any formal consideration of the security risks.

A further issue for consideration is around a potential scenario whereby a User may find themselves in an 'Event of Default' should any second or subsequent User System be found to be non-compliant at their annual review. To mitigate this, it would be beneficial to determine earlier whether this second or subsequent User System should be assessed.

The SSC has recently been made aware of Suppliers that have completed the User Security Assessment process for supplying gas and electricity to Domestic Customers and may wish to use a Shared Resource Provider to provide a second User System (either to continue to supply energy to Domestic consumers via a different engagement portal or to supply energy to Non-Domestic customers via a different User System). It believes that provisions need to be made for it to be notified of these subsequent systems before they become operational, to allow it to determine if an assessment is required.

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 5 of 17

This document is
classified as **White**

© SECCo 2018



3. Proposed Solution

Solution

The SSC raised [SECMP0057 'Users to notify SSC of a second or subsequent User System'](#) on 10 July 2018.

Under the proposed solution, all Users will be required to notify the SSC before they begin to utilise a second or subsequent User System. This Modification will make this obligation on Users clear and enforceable in the SEC. This notification will enable the SSC to consider the security risks and to advise the User accordingly.

Upon notification of a second or subsequent User System, the SSC will review the notification. It will determine whether the User System should undergo an ad-hoc User Security Assessment prior to the User System becoming operational, or whether this can become operational now and any review carried out under the next annual assessment. The SSC will provide this determination within eight weeks of the notification being made.

In the scenario where a second or subsequent User System being considered by a User has already completed a User Security Assessment (e.g. as part of the assessment of a Shared Resource Provider), the SSC may consider that no additional User Security Assessments are necessary until the next annual review is due. However, in the scenario where the second or subsequent User System has never been assessed, the SSC may require a User Security Assessment using the obligation in SEC Section G8.13 that “each User shall do all such things as may be reasonably requested by the Security Sub-Committee...for the purposes of facilitating an assessment of that User’s compliance with its obligations under Sections G3 to G6.”

If the SSC determines that an assessment must be completed prior to the User System going live, the User must comply with this. They cannot set their subsequent system to operational until the assessment is complete, and the SSC has reviewed the results.

Draft legal text

The proposed legal text changes to SEC Section G3.9 are provided in **Attachment A**.

As part of the implementation of this modification, the Security Controls Framework (SCF) will be updated to clarify the requirements introduced by this modification and advise how the processes will work in practice for SEC Parties. The SCF is intended to provide the basis for enabling a consistent level of review across all Users, and to provide a guide to the types of evidence which could be provided by a User to demonstrate compliance with its obligations.

Additionally, following feedback from the Working Group Consultation, the Agreed Interpretations will also be updated to clarify what constitutes ‘any new or materially changed component or functionality of a User System’. The Agreed Interpretations will

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 6 of 17

This document is
classified as **White**

© SECCo 2018



not replace or alter SEC obligations but should offer clarity and context to specific defined terms.

The SCF and the Agreed Interpretations can be found on the [Security Controls Framework web page](#) on the SEC website.

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 7 of 17

This document is
classified as **White**

© SECCo 2018

4. Impacts

The following section sets out the impacts associated with the implementation of SECMP0057.

SEC Party impacts

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

Central System impacts

There are no impacts on DCC Central Systems or Party interfacing systems anticipated.

Testing

No testing is required as part of implementation of this modification.

SEC and Subsidiary Document impacts

SEC [Section G 'Security'](#) will be impacted by this modification, as well as the SCF and the Agreed Interpretations.

Impacts on other industry codes

No impacts anticipated on other industry codes.

Greenhouse Gas Emission impacts

There are no Greenhouse Gas Emissions impacts anticipated.

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 8 of 17

This document is
classified as **White**

© SECCo 2018

5. Costs

Estimated Implementation costs

The potential costs to implement SECMP0057 will be limited to the Code Administration time and effort for:

- Making the necessary amendments to the SEC;
- Releasing a new version of the SEC to SEC Parties; and
- Publishing this on the SEC website.

SEC costs

The estimated SEC implementation cost is detailed in the table below:

SECAS implementation costs		
Implementation Activity	Effort (man days)	Cost
Application of approved changes to the SEC. Publication of new version of the SEC on the SEC Website and issuing this to SEC Parties. Application of approved changes to the SCF and the Agreed Interpretations.	Four	£2,400 ¹

¹ SEC man day effort based on a blended rate of £600 per day.



6. Implementation

Recommended implementation date

The Working Group and the Panel have agreed an implementation date of:

- **28 February 2019** (February 2019 SEC Release), if a decision to approve is made by 14 February 2019; or
- 10 Working Days following approval if a decision to approve is made after 14 February 2019 (if this modification is approved under Self-Governance, it will be implemented 10 Working Days after the end of the 10 Working Day referral period commencing after the Change Board vote).

The Proposer has requested for the modification to be implemented as soon as possible, as currently the SSC is relying on Users informing them without any obligation to do so. An absence of a notification to the SSC could mean the User goes ahead and utilises a second or subsequent User System with no formal consideration of the wider security risks. As a result, it would be beneficial to implement this modification as soon as possible.

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 10 of 17

This document is
classified as **White**

© SECCo 2018

7. Working Group Discussions

Are there any valid reasons why a User will be unable to notify SSC prior to utilising a second or subsequent User System?

The Working Group considered whether there could be any justified reasoning for why a User is unable to notify the SSC prior to employing a second or subsequent User System. As part of this, it also considered whether a User would not wish to inform the SSC of a subsequent system or how they intend to use it.

Members considered the scenario of a User undergoing a merger or acquisition where they may not be permitted to share details of a second or subsequent User System due to confidentiality agreements. They noted that, should this be the case, then by the time the User System was to become operational they would have to go public, by default; withholding information would not allow them to become operational. The Working Group confirmed the SSC did not release personal details of Users during normal proceedings and would always refer to Users in a way in which they could not be identified.

The Working Group highlighted, should the disclosure of information have a market impact, then this could be halted by external governing bodies.

The Working Group concluded that the only valid reasons why a User could not notify SSC is where there are conditions of law at play and even in these circumstances the User will be still be obligated to provide the SSC with all necessary information as is requested of them.

With regards to providing information to the SSC, the Working Group advised that the SSC would wish to know how the User System was built and connected together before permitting the User System to become operational. Therefore, under these requirements, the User would have to inform the SSC on certain aspects of their User System. Without this information the SSC may not permit the subsequent system to become operational. Members reiterated the point that the SSC would discuss all such information confidentially and would not be able to identify who the applicant was.

The Working Group believed it would be beneficial to seek wider views on any further scenarios and suggested adding these questions to the list of consultation questions.

The first additional question asked whether respondents would be aware of any valid reasons 'why a User would not wish to disclose to the SSC how they are intending to utilise a second or subsequent User System'. All responses stated that they did not believe there would be any valid reasons why a User not wish to disclose this information. Additionally, one response stated that, as the SSC are bound by confidentiality requirements and non-disclosure agreements, then this would negate any reason why a user would not disclose this information.

The second additional question asked "do you think, as an organisation, you could be utilising a second or subsequent User System in the future and are you aware of what this architecture might look like? If so, would you be willing to share this information on future

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 11 of 17

This document is
classified as **White**

© SECCo 2018



architecture with the SSC?”. Two respondents stated that they did not have plans to utilise a second or subsequent User System, one respondent stated that they would likely be utilising one but the designs and architecture were yet to be defined and the remaining respondent stated there was scope in their plans to utilise a second User System but any further information was an unknown at this time.

What is the definition of “employ”?

The Working Group was asked to consider the definition of “employ” in terms of the User notifying the SSC before they begin to employ a second or subsequent User System.

The Working Group felt that, as the proposed legal text did not refer to a User beginning to employ a second or subsequent User System, then there was no requirement for this to be clarified. However, it would need to be established what constituted the point at which a User would need to notify the SSC, aside from when the SEC states “as reasonably practicable”. The Working Group agreed that a User would need to notify SSC when they were “starting to develop a second or subsequent User System”.

Additionally, the Working Group felt that the terminology was consistent with what was already included within the SEC, noting references made within SEC Sections G5.25 to G5.27 where “employ” is used in relation to Shared Resources. The Working Group highlighted that “as soon as reasonably practicable” could be referred to.

The Working Group highlighted the word “employ” may not be suitable and “utilised” may be a better fit.

The feedback was provided to the SEC Lawyers who noted there is no mention of either “employ” or “utilise” in the proposed legal drafting. The drafting instead refers to a System “being incorporated into its User Systems for the first time”. References to “employ” are however used in Section G5.25 – G5.28 in relation to “a User which begins to employ User Systems which consist in whole or in part of Shared Resources”. Additionally, the term “employ” is also included In Section G8.6 which references “employs consultants”.

Should it be agreed that the SEC should remove references to “employ”, then a new modification would need to be made to Section G.

What are the timescales for submitting notifications to the SSC?

The Working Group agreed that the User would need to submit their notification before they began utilising a second or subsequent User System. Members agreed that the notifications should be submitted at least eight-weeks in advance, to allow the SSC to assess the necessary next steps. The SSC would then decide either to accept the notification and to assess the User at their next scheduled User Security Assessment, or to request an ad-hoc User Security Assessment take place. Should the latter commence, the SSC would need

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 12 of 17

This document is
classified as **White**

© SECCo 2018



time for the assessment to take place and for it to review the outcome and decide whether the User System will be permitted to become operational by providing explicit approval.

The Working Group agreed that the User should not be permitted to become operational unless the SSC had first provided this explicit approval for the addition to the User System. Users would therefore need to ensure that they notified the SSC sufficiently in advance for all the above steps to take place prior to their desired go-live date.

The Working Group agreed the eight-week notification for Users should be included in the SCF, and not in Section G. This would allow the SSC to vary this if the timescales needed to change.

Working Group's consideration of industry consultation responses

Consideration of the draft legal text

There were four responses to the Working Group Consultation. Three of the responses were in favour of the modification and legal text as presented. One respondent requested clarification to the legal text to ensure Users were not obligated to inform SSC when they incorporated a new or materially changed component or functionality and were only required to inform SSC when they incorporated a System into its User Systems for the first time.

The Working Group discussed the proposed legal text and agreed the location of the text in G3.9 was appropriate but it needed to be made clear that explicit consent needed to be provided to the User by SSC prior to the second or subsequent User System becoming operational.

The Working Group discussed ways to mitigate any unintended mis-interpretation surrounding the legal text and decided to incorporate an explanation into the Agreed Interpretations, to state that the User would not be obligated to inform SSC when they replaced a component of an existing User System, that had already been subject to a User Security Assessment.

On this basis, the Working Group unanimously agreed to keep the proposed legal drafting from the SEC Lawyers.

The Working Group decision and proposal was provided to the respondent who raised the clarification request. The respondent has confirmed that the amendment to the Agreed Interpretations satisfactorily addressed their concerns.

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 13 of 17

This document is
classified as **White**

© SECCo 2018

8. Working Group Conclusions

The Working Group's **unanimous** view is that SECMP0057 better facilitates General SEC Objectives (a), (e) and (g) and should be **approved**.

Benefits and drawbacks of SECMP0057

The Proposer and the Working Group have identified the following benefits and drawbacks related to SECMP0057:

Benefits

In addition to those identified below in relation to the relevant SEC Objectives, the Working Group believes the implementation of this modification will provide the following benefits:

- SECMP00057 would provide clarity to Users and remove any unintended ambiguity by having the obligations around second and subsequent systems documented clearly in the SEC.
- Additionally, having the timescales provided in the accompanying documentation, such as the SCF and Agreed Interpretations, would better inform Users and would highlight that the second or subsequent User System may need to go through a security assessment. This would allow Users to be able to prepare accordingly in sufficient time.

Drawbacks

The Working Group identified the following drawbacks:

- There could be an additional cost to Users should the modification be approved, due to potentially needing to undergo additional assessments.
- The SSC would also need to spend more time and resource assessing these potential risks, once highlighted.
- Finally, there could be a risk of Users being treated differently depending on how they initially describe their subsequent systems to the SSC, which could result in similar setups being assessed differently. However, the Working Group noted that it would be for Users to ensure they provide sufficient detail to the SSC to enable it to make a suitable determination.

Views against the General SEC Objectives

The Working Group **unanimously** believes that this modification better facilitates SEC Objectives (a), (e) and (g):

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 14 of 17

This document is
classified as **White**

© SECCo 2018



Objective (a)²

- The Working Group unanimously believes this modification would better facilitate Objective (a) as it would allow for the SSC to give consideration of any new or additional security risks to the end-to-end smart metering system that could impact on other Users, Consumers and inter-operability due to a subsequent User System.

Objective (e)³

- The Working Group unanimously believes this modification would better facilitate Objective (e) as it would ensure that any unforeseen developments in the use of any second or subsequent User Systems can be identified as these would be properly assessed for security risks in delivering secure and sustainable energy supply.

Objective (g)⁴

- The Working Group unanimously believes this modification would better facilitate Objective (g) as it will provide clarity in the SEC about how the User Security Assessment process will apply to Users intending to utilise a second or subsequent User System. This will enable SECAS to advise Users and the User CIO accordingly.

For the avoidance of doubt, the Working Group believe that SECMP0057 is neutral against all other Objectives.

² Facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain.

³ Facilitate such innovation in the design and operation of Energy Networks (as defined in the DCC Licence) as will best contribute to the delivery of a secure and sustainable Supply of Energy.

⁴ Facilitate the efficient and transparent administration and implementation of this Code.



9. Panel discussions & conclusions

Panel discussions and conclusions

The Panel **unanimously** agreed that due process has been followed and that SECMP0057 should progress to Modification Report Consultation.

The Panel also agreed that SECMP0057 is a Path 3: Self-Governance Modification Proposal and that the draft legal text changes to the SEC deliver the intention of the modification.

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 16 of 17

This document is
classified as **White**

© SECCo 2018

Appendix 1: Glossary

The table below provides definitions of the terms used in this document.

Acronym	Definition
DMR	Draft Modification Report
MRC	Modification Report Consultation
SCF	Security Controls Framework
SEC	Smart Energy Code
SECAS	Smart Energy Code Administration and Secretariat
SSC	Security Sub-Committee

SECMP0057

Final Modification
Report

12 December 2018

Version 1.1

Page 17 of 17

This document is
classified as **White**

© SECCo 2018