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

SECMP0044:

User Security Assessment of a Shared Resource

What stage is this document in the process?

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

SECAS Contact:

Name:
Talia Addy

Number:
20 7090 1010

Email:
SEC.Change@gemserv.com

Summary

This modification seeks to make changes to the User Security Assessment process to improve efficiency and lower the impact on SEC Parties, Shared Resource Providers, the User Competent Independent Organisation (User CIO), Smart Energy Code Administrator and Secretariat (SECAs) and the Security Sub-Committee (SSC).

Working Group Conclusions

✓

- The Working Group **unanimously** believes that SECMP0044 should be **approved**.

Impacts

!

- Large and Small Suppliers
- Network Parties
- Other SEC Parties (Shared Resources)
- Data and Communications Company (DCC)
- There are no impacts on DCC Central Systems and/or Party interfacing systems anticipated

Administered by Gemserv, 8 Fenchurch Place, London EC3M 4AJ

SEC
Smart Energy Code

Content

About this Document

This document is the Final Modification Report (FMR) for SECMP0044. This document provides detailed information on the issue, solution, impacts, costs, industry consultation as well as Working Group and Panel discussions and conclusions on the modification.

This document has four attachments:

- **Attachments A** and **B** contain the draft legal text changes to support this modification;
- **Attachment C** contains the responses to the Working Group Consultation; and
- **Attachment D** contains the responses to the Modification Report Consultation.

The Change Board will consider this modification at its meeting on 25th July 2018, where it will determine whether SECMP0044 should be approved or rejected.

Gemserv

1. Summary

What is the issue?

Under the current arrangements, DCC Users are required to undergo User Security Assessments to be eligible to use DCC Central Systems. These assessments can be cumbersome where a DCC User has elected to use a Shared Resource Provider for its User Systems. For example, a Small Supplier (supplying energy to 250,000 or less Domestic Premises) is required to undergo a Full User Assessment in its first year, with a reduced level of assessment in the second and third years. However, if a Small Supplier elects to use a Shared Resource that, in aggregate, supplies gas or electricity through Smart Metering Systems to more than 250,000 Domestic Premises, the Small Supplier is required to undergo a Full Assessment every year. Furthermore, a Shared Resource Provider is currently required to undergo one full assessment for each User that it serves each year. In some cases, this means a Shared Resource Provider is required to undergo several dozen assessments in one calendar year.

What is the Proposed Solution?

This modification seeks to make changes to the User Security Assessment process to improve efficiency and lower the impact on SEC Parties, Shared Resource Providers, the User CIO, SECAS and the SSC.

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.

Implementation Costs

The total estimated implementation cost to deliver SECMP0044 is approximately **£1,200** in SEC Administration effort.

Implementation Date

The Working Group recommends an implementation date of **10 Working Days** following approval.

Working Group's views

The Working Group unanimously believes that SECMP0044 better facilitates SEC Objectives (a), (e) and (g). It therefore believes that this Modification Proposal should be **approved**.

Panel conclusions

The Panel unanimously agree that due process has been followed and that SECMP0044 should progress to Modification Report Consultation (MRC).

2. What is the issue?

Background

User Security Assessments

To become eligible to use the DCC Systems, SEC Parties need to pass a User Security Assessment conducted by the User CIO. The User CIO undertakes User Security Assessments on behalf of the SEC Panel and produces User Security Assessment Reports. SEC Parties and/or DCC Users will be assessed for compliance against SEC Sections G3 to G6. A methodology and guidance is provided in the Security Controls Framework (SCF), a document which has been developed by the SSC to ensure consistency across all User Security Assessments.

Prior to becoming a User, all SEC Parties are required to have an initial Full User Security Assessment. After this, there is an annual Assessment cycle, and the type of User Security Assessment that is required depends on the number of domestic premises that they interact with via their User System.

The SEC is explicit in what type of risk assessment is required for Supplier Parties, Network Parties and Other Users. There are four types of assessments defined in the SEC:

- A Full User Security Assessment – carried out by the User Independent Security Assurance Service Provider in respect of a User. This identifies the extent to which that User is compliant with each of its obligations under SEC Sections G3 to G6 in each of its User roles;
- A Verification Security Assessment – carried out by the User Independent Security Assurance Service Provider in respect of a User. This identifies any material increase in the security risk relating to the Systems, Data, functionality and processes of that User falling within SEC Section G5.14 (Information Security: Obligations on Users) since the last occasion on which a Full User Security Assessment was carried out in respect of that User;
- A User Security Self-Assessment – carried out by a User, the outcome of which is reviewed by the User Independent Security Assurance Service Provider. This identifies any material increase in the security risk relating to Systems, Data, functionality and processes of that User falling within SEC Section G5.14 since the last occasion on which a User Security Assessment was carried out in respect of that User; and
- A Follow-Up Security Assessment – where the SSC considers it appropriate, it requests the User Independent Security Assurance Service Provider to carry it out.

The table below indicates what type of assessment each Party is required to undertake, including the time frames.

	No. of Domestic Premises[1]	User Entry / Year One	Year Two	Year Three
Supplier Parties	More than 250,000	Full Assessment	Full Assessment	Full Assessment
	250,000 or less	Full Assessment	Verification Assessment	Self-Assessment
Network Parties	More than 250,000	Full Assessment	Verification Assessment	Verification Assessment
	250,000 or less	Full Assessment	Verification Assessment	Self-Assessment
Other Users	n/a	Full Assessment	Self-Assessment	Self-Assessment

The current SEC arrangements were intended to adopt a proportionate approach in relation to User Security Assessments. Large Suppliers (those supplying energy through Smart Metering Systems to more than 250,000 Domestic Premises) are subject to a Full User Security Assessment every year, reflecting the increased security risks associated with larger volumes of connected Devices. Small Suppliers (those supplying energy through Smart Metering Systems to 250,000 or less Domestic Premises) are required to undergo a Full User Security Assessment in the first year, but then a reduced level of assessment in the second year (a Verification User Security Assessment) and a Self-Assessment in the third year, before repeating the cycle. This arrangement for Small Suppliers was implemented in response to the proportionately lower security risks associated with smaller volumes of connected Devices.

Assessment using a Shared Resource Provider

A Shared Resource Provider is an organisation who provides the User Systems and manages the messaging capabilities (Service Requests (SRs)) between Users and the DCC on behalf of multiple Users (SEC Parties and/or DCC users). Several Small Suppliers have chosen to use a Shared Resource Provider to deliver the User System required to support Smart Meters.

The SEC is explicit in that, when considering whether a Supplier is Large or Small, the number of Domestic Premises served will need to include the Domestic Premises served by other DCC Users that also use the Supplier's chosen Shared Resource. This means that, once the number of Smart Metering Systems communicated via Shared Resource surpasses 250,000 Domestic Premises, each DCC User Using that Shared Resource Provider will be subject to a Full User Security Assessment every year, as though they were a Large Supplier. The

[1] Number of Domestic Premises supplied with gas or electricity through one or more Smart Metering Systems

Shared Resource Provider will also be assessed as part of each individual Supplier's assessments.

What is the issue?

Under the current arrangements, if a Small Supplier elects to use a Shared Resource Provider to provide their User System, that, in aggregate, handles the supply of energy through Smart Metering Systems to more than 250,000 Domestic Premises, the Small Supplier is required to undergo a Full User Security Assessment every year in the same way as a Large Supplier. The rationale behind this was to ensure that Users who engage with a Shared Resource Provider take responsibility for the increased volume of connected Devices, since Shared Resources are not, at present, required to be SEC Parties.

The majority of Small Suppliers are currently using a Shared Resource Provider to provide their User System that, in aggregate, handles more than 250,000 Domestic Premises through Smart Metering Systems. The original concept of a proportionate approach for Small Suppliers is not therefore being realised.

Furthermore, a Shared Resource Provider is currently required to be assessed as part of the Full User Security Assessment for each User that it serves each year. In some cases, this means a Shared Resource Provider is required to undergo several dozen separate assessments in each calendar year. This creates inefficiency for the Shared Resource Provider, the User CIO, SECAS and the SSC.

The SSC considers that this issue needs to be addressed because, at present:

- the Shared Resource Provider is assessed multiple times per year by the User CIO, as part of each User's Security Assessment. This results in duplication of the User CIO's observations, increased cost being incurred, and a large amount of time and effort being spent by the User CIO, the Shared Resource Provider, SECAS and the SSC to no real advantage; and
- a Small Supplier supplying energy through Smart Metering Systems to 250,000 or fewer Domestic Premises will be subject to an annual Full User Security Assessment if its Shared Resource Provider is, in aggregate, supplying energy through Smart Metering Systems to more than 250,000 Domestic Premises. This seems disproportionate when considering the risk for an individual Small Supplier.

3. Proposed Solution

Proposed Solution

The SSC raised SECMP0044 'User Security Assessment of a Shared Resource' on 15th December 2017.

This modification seeks to make changes to the User Security Assessment process to improve efficiency and lower the impact on SEC Parties, Shared Resource Providers, the User CIO, SECAS and the SSC.

Shared Resource Providers

Under the current arrangements Shared Resource Providers may be required to undergo several dozen separate assessments in each calendar year. In order to alleviate this issue, this modification will make amendments to SEC Section G to ensure that any organisation that falls into the definition of a Shared Resource Provider will only be required to undergo one User Security Assessment every calendar year.

This modification defines Shared Resources and Shared Resource Providers as:

> *"G10.1 Where any resources which form part of the User Systems of a User also form part of the User Systems of any one or more other Users, those resources shall be known as "Shared Resources"."*
>
> *"G10.2 For the purposes of this Part G, a "Shared Resource Provider" shall mean any Party which makes available Shared Resources to one or more Users, for use by them or on their behalf, in accordance with any agreement entered into or arrangement made with each such User."*

The combination of the above two provisions means that:

- any organisation that provides Shares Resources (**that make up part of a User System**) to one or more Users can ***elect*** to become a Shared Resource Provider by becoming a SEC Party; and
- any organisation that provides Shared Resources (**that make up the whole of a User System**) for one or more Users ***will*** be considered a Shared Resource Provider and will therefore have to become a SEC Party (as only an organisation that is a SEC Party can become a Shared Resource Provider).

Payment for User Security Assessments

Under this modification, Shared Resource Providers will be required to make a payment for the cost of its annual User Security Assessments. This will be done in the same way

as a DCC User under SEC Section G8.51. How the Shared Resource Provider recovers this cost is outside the scope of this modification.

User Security Assessment Reports for Shared Resource Providers

SECMP0044 requires that any User Security Assessment Report for a Shared Resource Provider (and any other User Security Assessment Response it may provide), together with any assurance status set or observations made by the SSC, will be made available by the Shared Resource Provider to all Users who have engaged the Shared Resource Provider.

This will ensure transparency between the Shares Resource Provider and the User, given that the User remains accountable for the SEC security obligations applicable to them.

SEC Parties providing User Systems to affiliates

Under this modification there is a possibility for SEC Parties (with affiliates) to fall into the definition of a Shared Resource Provider. For example, if a Large Supplier (as a parent company) develops its own User System and then provides that User System to its affiliates, the Large Supplier will be performing in two roles: Large Supplier and Shared Resource Provider.

Although the User System in question will need to be audited for both purposes it does not mean that the Large Supplier will need to go through two separate User Security Assessments. This is because there are no ring-fencing provisions in the draft legal text (Attachments B and C to the Modification Report Consultation) which require the Party to separate its Supplier activity from its Shared Resource Provider activity for assessment purposes. When the organisation is audited by the User CIO, it will be audited in relation to more than one User Role, which will include the role of Shared Resource Provider. Furthermore, the result of the audit can then be used by the User CIO and the SSC for all relevant purposes, including being relied upon in respect of the other group companies who use the Shared Resources which the Large Supplier provides to them.

Shared Resource Provider seat on the SSC

SECMP0044 proposes to add an additional Member seat to the SSC, representing Shared Resource Providers. This new SSC member will be appointed in line with current requirements and processes as set out in Section G7 ‘Establishment of the Security Sub-Committee’. It should also be noted that the new member must be impartial, representing all Shared Resource Providers and not their own organisation’s

interests. Full details on the requirements and processes for electing this new SSC member can be found in G7.12 of the draft legal text in Attachment C of the Modification Report Consultation.

Users engaging a Shared Resource Provider servicing 250,000 or more premises

Any Small Suppliers (supplying energy through Smart Metering Systems to 250,000 or fewer Domestic Premises) that have engaged a Shared Resource Provider will be subject to a Verification Assessment in the second year and to a Self-Assessment in the third year, irrespective of how many other Domestic Premises the Shared Resource Provider is handling for other Users.

Any User of a Shared Resource Provider that has been subject to a User Security Assessment under the proposed arrangements will be able to rely on the assurance status set by the SSC in the first year and on the outcome of the SSC review in the second and subsequent years in respect of its User System that is being provided by that Shared Resource Provider.

Details of the impacts and benefits of this modification for SEC Parties can be found in **Section 4** below.

Draft legal text and guidance

The proposed legal text changes to SEC Sections A and G are provided in **Attachment B** and **Attachment C** of the Modification Report Consultation.

As part of the implementation of this modification, the Security Controls Framework will be updated to clarify the requirements introduced by this modification and advise how the processes will work in practice for SEC Parties and Shared Resource Providers.

4. Impacts

The following section sets out the impacts associated with the implementation of SECMP0044.

SEC Party impacts

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

This modification affects all Users who are using a Shared Resource Provider to provide their User System.

Small Suppliers will benefit the most from this Modification Proposal as it will remove the need for a Full User Security Assessment in the second and third years following the first User Security Assessment.

Large Suppliers will still be required to have a Full User Security Assessment if they supply energy through Smart Metering Systems to more than 250,000 Domestic Premises, but they will be assessed independently of their Shared Resource Provider.

Network Operators who use a Shared Resource will benefit in a similar way to Small Suppliers where (on their own) they provide services to 250,000 or fewer Domestic Premises.

Other SEC Parties who are not Users will be unaffected by the implementation of this modification. However, Other SEC Parties who meet the requirements of a Shared Resource Provider (or who choose to be a shared resource provider) will benefit by having a single User Security Assessment rather than one for each of their User customers.

Other Users are not affected by the criteria relating to energy being supplied through Smart Metering Systems to more or less than 250,000 Domestic Premises but will benefit from the single assessment of the Shared Resource Provider in the same way as Small Suppliers.

This modification is also expected to have a very minor impact on the **DCC**, as they will be required to make minor changes in their reporting arrangements.

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 Sections A 'Definitions and Interpretations' and Section G 'Security' will be impacted by this modification.

Impacts on other industry codes

No impacts anticipated on other industry codes.

Greenhouse Gas Emission impacts

There are no Greenhouse Gas Emissions impacts anticipated.

5. Costs

Estimated Implementation costs

The total estimated implementation cost to deliver SECMP0044 is approximately £**1,200** in SEC administration time and effort. 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. Review and update any impacted SEC guidance materials.	Two	£1,200[2]

Although there are minor impacts on the DCC, the costs associated with this are negligible.

6. Implementation

Recommended implementation date

The Working Group is recommending an implementation date for SECMP0044 of:

- **10 Working Days** following the end of the 10 Working Day referral window that applies after the Change Board vote.

This is to enable the Small Suppliers and Shared Resource Providers who are due a second User Security Assessment in the near future to benefit from the implementation of this Modification Proposal. Should the implementation be delayed, these Small Suppliers and Shared Resource Providers will be required to undergo full User Security Assessments under the existing SEC arrangements. Furthermore, other Small Suppliers and Shared Resource Providers will benefit from a later implementation which will create undue discrepancies in the treatment between these different Parties.

[2] SEC man day effort based on a blended rate of £600 per day.

7. Working Group Discussions

Terms of Reference

The Working Group has considered and answered the questions put forward in the SECMP0044 Terms of Reference. A summary of its discussions and conclusions are detailed below.

What is the impact of making Shared Resources SEC Parties?

The Working Group considered whether there were any potential issues associated with Shared Resource Providers becoming SEC Parties. The Proposer and the Working Group noted that all existing Shared Resource Providers are already SEC Parties, and, so far, there have been no issues associated with this.

The Working Group also questioned whether Shared Resource Providers will need to be DCC Users, as this would have an impact on the industry and the DCC. Following discussion, the Working Group agreed that it is unlikely that a Shared Resource will ever need to become a DCC User.

What are the impacts on other Parties if the Shared Resource is non-compliant with the security obligations?

The Working Group discussed a potential scenario where a Shared Resource Provider is found to be non-complaint with SEC security obligations following the SSC review of the outcome of a User Security Assessment. It agreed that there could be severe consequences for the Shared Resource Provider and for both Small Suppliers and Large Suppliers using said Shared Resource Provider depending on the severity of the non-compliance(s). In these circumstances, the SSC will investigate the nature and severity of the non-compliance(s) and any proposed remediation plan, and will make a recommendation to the SEC Panel relating to Event of Default under the existing arrangements in SEC Sections G8.54 to G8.60. However, the Working Group also debated that any User choosing to use a Shared Resource Provider does so by commercial choice, and therefore they are expected to have business continuity arrangements in place to tackle such issues.

Concerning an Event of Default as a result of a Panel decision on non-compliance with security obligations, the Working Group noted that Shared Resource Providers are not subject to an Energy Supply Licence. However, as a SEC Party, they are subject to the consequences of an Event of Default set out in in SEC Section M8.4 which could include suspension of rights (described in SEC Section M8.5), instructing the DCC to suspend services, or to be expelled from the Code.

Since the User is accountable under the SEC for the Shared Resource Provider, any consequences of an Event of Default will also affect the User. The legal text makes it

clear that where a Shared Resource Provider which is a Party provides a User with Shared Resources for its User Systems, both it and the User shall be jointly and separately liable for any failure to comply with an obligation which relates to those Shared Resources (subject to certain caveats outlined in the legal drafting).

What is the pattern of assessment for a Shared Resource Provider with 250,000 or less customers in aggregate?

The pattern of assessments for a Shared Resource Provider supplying gas or electricity through one or more Smart Metering Systems to 250,000 Domestic Premises or fewer would be the same as for a Supplier i.e. a Full User Security Assessment in the first year, a Verification Assessment in the second year and a Self-Assessment in the third year and then repeat the three-year cycle.

Q4: What implications are there if a Shared Resource Provider is also used by a Large Supplier?

The Proposer informed the Working Group that all Shared Resources currently have Large Supplier Customers. The Working Group considered the issue of a default impacting Large and Small Suppliers. For example, if a Shared Resource Provider went into default all its customers (both Large and Small Suppliers) would be impacted and would need to migrate their portfolios to another service provider. In this instance it could potentially take longer for a Large Supplier to complete this migration due to the large volume.

Other discussions

Scope of SECMP0044

The Working Group considered whether the modification should be more open to ensure that it can be applied to all SEC Parties that may choose to use a Shared Resource Provider. The Working Group and the Proposer agreed that it would be pragmatic to broaden the scope of the modification to ensure that it is applicable to all Users, i.e. Large Suppliers, Small Suppliers, Network Operators and Other Users.

Discussions concerning the draft legal text

Definition of Shared Resource and Shared Resource Provider

At present, the SEC defines a Shared Resource in SEC Section G5.25 as any resource which provides ‘part of the User System’. This SEC Modification maintains a definition of a Shared Resource as providing a part of a User System. However, the main aim of the SEC Modification is focussed on those Shared Resources that provide the whole of

the User System. Therefore, the proposed legal text includes a new definition for 'Shared Resource Provider' which (among other things) means any Share Resource that provides the whole User System.

The Working Group discussed a scenario where a Shared Resource provides part of a User System to multiple Users (e.g. third-party software or services that form a part of a User System), such as the providers of Unique Transaction Reference Number (UTRN) generation. The Working Group considered whether these Shared Resources should also have the opportunity to become SEC Parties and to be subject to an annual User Security Assessment. It was agreed by the Working Group that because the current definition of Shared Resource covers examples such as UTRN generators, then provision should be made for them to have the option of becoming a SEC Party and to be subject to an annual User Security Assessment in their own right should they choose to do so.

The Working Group recognised there is potential for the example described to occur, but considered this to be an edge case, noting that the SSC has not seen any examples to date and were not aware of any intentions of Shared Resources to offer such services or for Suppliers to require them in the way described. However, it makes sense to future-proof the Modification to provide Shared Resources with this option should they wish to take it.

The legal text was therefore updated to allow any Shared Resource providing part of a User System to become a SEC Party and opt in to the conditions of 'Shared Resource Provider'.

Section G5.10

A Working Group member questioned Section G10.5 of the draft legal text, seeking clarification on how this drafting is different from the current arrangements. The legal adviser explained that, at present, neither Shared Resources nor Shared Resource Providers are required to be Parties; however under this legal drafting Shared Resource Providers will be obliged to be a SEC Party, with Shared Resources having the option to be. Once a Shared Resource Provider becomes a SEC Party (or any Shared Resource that wishes to do so) they will be treated as if they were a User and hence will be required to comply with the same obligations as a User. In other words, there will be at least two Parties, that are required at the same time, to comply with the same set of obligations. The legal text deals with this as being 'jointly and severally liable'.

The Working Group pointed out the importance of this modification and legal text not be a substitute for due diligence and good practice for supply chain risk management. Therefore, following the implementation of this modification the Working Group encouraged that Users should continue to review the performance of their Shared

Resources and Shared Resource Providers, and not simply rely on the report they will receive.

Shared Resource as an SSC Member

The solution proposes to add an additional Member to the SSC, representing Shared Resource Providers. The Proposer informed the Working Group that the SSC discussed this and agreed that it will be beneficial to have representation from Shared Resource Providers. The Working Group agreed with this approach.

The Working Group requested the current provisions of becoming an SSC Member be summarised in the modification report to ensure Shared Resource Providers are aware of the process for electing a member to the SSC.

SEC Section G7 states that in order to be appointed as a member of the SSC, the following high-level process must be followed:

- to be elected by those Other SEC Parties which are Shared Resource Providers;
- to have been nominated by a company or organisation, with the individual who submitted the nomination holding a senior position within that company;
- to have been confirmed by the nominating organisation to have relevant security expertise in relation to the category of membership;
- to have been confirmed by the nominating organisation to have completed a BS7858[3] security assessment; and
- to be approved by the SSC as having met all of the SEC requirements for membership.

Should this modification be implemented, the new SSC Member nominee will follow the same approach as other Members. The newly introduced Member must be impartial i.e. they will not be representing their own organisation but will be representing all of the Shared Resource Providers.

Notifications and User Security Assessment Reports

The Working Group discussed how Shared Resource Providers and the User CIO share their report with Shared Resource users as well as the confidentiality of these reports. It was pointed out that, currently, Shared Resources go through their assessments together with their Users. However, going forward, these assessments will be separate and therefore there will be separate reports. The Working Group questioned whether

[3] BS7858 – Security screening of individuals employed in a security environment. Code of Practice

this situation may cause contractual and disclosure agreement issues for Shared Resource Providers.

The Working Group agreed that, given the SEC accountability of the Shared Resource User for their Shared Resource Provider, any User CIO observations relating to the User Security Assessment of the Shared Resource Provider need to be made available to all the Shared Resource Users who are customers of the Shared Resource Provider. Similarly, the Shared Resource Users need to be able to see the management response to those observations by the Shared Resource Provider as well as the outcome of the review by the SSC. The legal drafting achieves the necessary transparency by ensuring that the originator of the report / management response / SSC outcome provides copies to the Shared Resource Provider and all the associated Shared Resource Users.

Following this discussion, the Working Group requested the legal text be made clear and state that the Shared Resource Provider 'shall provide' the report (rather than 'make available' the report'). The Working Group also asked that a line be added to note that it is still the responsibility of the relevant Party to ensure they received a copy. The Proposer agreed with this approach.

One Working Group member requested clarification on Section G10.7(d) of the draft legal text as to the nature of the reports to the SSC that the Shared Resource Provider is required to provide to its Shared Resource Users. It was clarified that, after review by the SSC, there could be remediation actions (steps to be taken), which, under SEC Section G8.28(b), the Shared Resource Provider is required to: report progress against to the SSC; and/or to report completion of the steps with a timetable; or to report failure to complete the steps required. The drafting in Section G10.7(d) requires any such reports to also be provided to each Shared Resource User. The member asked if it is the Shared Resource Provider's responsibility to deliver the document, and it was clarified that, as G10.7 states, the responsibility lies with whoever generates the document.

The Working Group noted that it is an existing SEC obligation (SEC Section G5.27(a)) for a Shared Resource User to notify the SSC as soon as reasonably practicable to do so when they begin to employ a Shared Resource Provider. A Working Group member questioned if it would be an appropriate approach to add a clause which requires a Shared Resource Provider to notify the SSC of the Shared Resource Users it has contracted with as well as when it obtains or loses a customer. The legal adviser confirmed that this is a simple addition to Section G10 of the draft legal text. It was agreed that it would be sensible to have an accurate list and to update it on regular basis which should ensure that any sensitive information is being shared with the right Shared Resource Users.

Transition period

The Working Group also recognised that there could be a period of transition in terms of reporting, following the implementation of this modification. The SSC, the Shared Resource Providers and the Shared Resource Users are keen to implement the modification as soon as possible so that all current Shared Resource Providers can undertake the next User Security Assessment in their own right. This will ensure a fair and equitable approach across the Shared Resource Providers and also avoid the inefficiency and expense of multiple User Security Assessments of the same Shared Resource Provider that occurs at present.

At present, the SEC requires the second and subsequent User Security Assessment to be **scheduled** within 12 months of the security status being set. The SEC does not define the period between the scheduling and the actual User Security Assessment. That time is defined in the Security Controls Framework which sets out the User Security Assessment Methodology and is under the jurisdiction and approval of the SSC (SEC Section G7.16(a)). The SSC will therefore need to determine the timing of the User Security Assessments for individual Users who could be adversely affected by the implementation timing of the modification.

Further discussions

The Working Group also identified what they saw as a potential compliance issue with the current wording of the SEC, noting that should a Small Supplier exceed the 250,000 threshold *more than 12 months* after their Initial Full User Security Assessment, they will be obligated to comply with Section G8.41. However, Section G8.41 requires that they schedule their next User Security Assessment *within 12 months* meaning they could therefore become non-compliant. The Working Group accepted that this seems to be an issue, but the Proposer noted that Section G8.49 clarifies that the number of Domestic Premises relating to the next assessment is determined “at the time at which the nature of each annual security assurance assessment for the relevant User falls to be ascertained; and the DCC shall provide all reasonable assistance that may be requested by that User or the Security Sub-Committee for the purposes of making that determination”. Following discussions, the Working Group suggested that this may need to go to the SSC once the legal drafting is completed.

A Working Group member brought up that, in the future, as a result of the combination of deployed SMETS1 and SMETS2 meters following SMETS1 Enrolment and Adoption, a Small Supplier may reach the 250,000 threshold. Considering this scenario, the Working Group questioned whether the proposed solution is future-proof. The Proposer informed the Working Group that, subject to the Department for Business, Energy and Industrial Strategy (BEIS) SEC changes post Enrolment and Adaption, both SMETS1 and SMETS2 will count towards the 250,000 Domestic Premises threshold, and therefore no further action is needed.

Another Working Group member asked whether consideration should be given to the NIS Directive[4] (the Directive on Security of Network and Information Systems) that will be introduced. The Working Group agreed that if there are any interactions between this modification and the NIS Directive identified, they need to be noted, but those will sit outside of this modification.

[4] https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive

8. Working Group Conclusions

The Working Group's **unanimous** view is that SECMP0044 better facilitates General SEC Objectives (a), (e) and (g), and should be **approved**.

Benefits and drawbacks of SECMP0044

The Proposer and the Working Group have identified the following benefits and drawbacks related to SECMP0044:

Benefits

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

- Small Suppliers will benefit the most from this modification as this modification will remove the need for them to carry out a Full User Security Assessments each year, and instead allow them to carry out a Verification Assessment and Self-Assessment in years two and three, which will ultimately save time and money.
- Network Operators who use a Shared Resource will benefit in a similar way to Small Suppliers where (on their own) they provide services to 250,000 or fewer Domestic Premises.
- Other SEC Parties who meet the requirements of a Shared Resource Provider (or who choose to be a shared resource provider) will benefit by having a single User Security Assessment rather than one for each of their User customers, which will ultimately save time and money.
- This modification will also make the security assessments slightly shorter and less costly, and will provide clarity on the assessments and reporting arrangements.

Drawbacks

No drawbacks have been identified by the Working Group.

Views against the General SEC Objectives

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

- **Objective (a)**[5] - by reducing the duplication and achieving a more efficient and less costly User Security Assessment process.
- **Objective (e)**[6] **-** by ensuring compliance with SEC security obligations through an improved and proportionate process for Suppliers and Shared Resources.
- **Objective (g)**[7] - removing the current duplication in administration that arises by SECAS being required to repeat dozens of similar management responses from a Shared Resource and from the SSC having to review repeated assessments of the same Shared Resource.

For the avoidance of doubt, the WG believe that SECMP0044 is neutral against the remaining Objectives.

Draft legal text changes

The WG unanimously believes that the draft legal text changes deliver the intention of this Modification Proposal.

Implementation approach

The WG unanimously recommends an implementation date for SECMP0044 of:

- **10 Working Days** following the end of the 10 Working Day referral period that applies after a Change Board vote.

[5] Facilitate the efficient provision, installation, and operation, as well as interoperability, of Smart Metering Systems at Energy Consumers' premises within Great Britain.
[6] 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.
[7] Facilitate the efficient and transparent administration and implementation of this Code.

9. Panel discussions & conclusions

Panel conclusions

The Panel **unanimously** agree that due process has been followed and that SECMP0044 should progress to MRC.

The Panel also agreed:

- that SECMP0044 is a Path 3 'Self-Governance Modification Proposal';
- that the draft legal text changes to the SEC deliver the intention of the modification; and
- with the recommended implementation of 10 Working Days following the end of the 10 Working Day referral period that applies after a Change Board vote.

Appendix 2: Glossary

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

Acronym	Defined Term
BEIS	Department for Business, Energy and Industrial Strategy
DCC	Data and Communication Company
DMR	Draft Modification Report
MRC	Modification Report Consultation
SCF	Security Controls Framework
SSC	Security Sub-Committee
SR	Service Request
User CIO	User Competent Independent Organisation
UTRN	Unique Transaction Reference Number
WG	Working Group