

SEC Section G3.18 – G3.20 provisions concern:

- SEC Parties
- Data and Communications Company
- Registered Supplier Agents
- SEC Panel
- The Authority

What is SEC G3.18 – G3.20?

A section of the SEC which outlines the obligations of users to ensure arrangements are in place, so they become aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of their User System or any Smart Metering System (Excl. a Communications Hub Function or Gas Proxy Function) and take appropriate action.

What is my responsibility regarding material security vulnerabilities under SEC G3.18 - G3.20?

The SEC requires Energy Suppliers:

- to notify Device manufacturers of any security vulnerabilities they identify (e.g. in live operations) **[G3.17 & G3.18]**;
- to take reasonable steps to ensure that the cause of the vulnerability is rectified, or its impact mitigated as soon as reasonably practicable **[G3.18]**;
- to be notified by their Device manufacturers of any security vulnerability identified **[G3.20]**;
- to notify the Security Sub-Committee (SSC) of the steps being taken and the timetable for completion **[G3.9 & G3.18]**.

A User shall not be required to notify a manufacturer or developer in accordance with Section G3.18(a) where it has reason to be satisfied that the manufacturer or developer is already aware of the matter that would otherwise be notified. **[G3.18]**

How can I ensure I comply with SEC G3.18 – G3.20 prior to my User Security Assessment?

To satisfy the SEC security obligations, it is necessary to have contractual arrangements with your Meter Asset Provider (MAP) or Device manufacturer which clearly states a duty to notify each other as soon as reasonably practical of any material security vulnerability in, or likely cause of a material adverse effect on the security of any hardware, software or firmware which forms part of the Smart Metering System.

Please find below suggested wording for Energy Suppliers to contract with the MAP to flow to Device manufacturer:

Where [X] Energy Supplier becomes aware of any material security vulnerability in, or likely cause of a material adverse effect on the security of any hardware, software or firmware which forms part of its Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function) for which it is the Responsible Supplier, it shall, wherever it is reasonably practicable to do so, notify the manufacturer of the Device or the developer of the software or firmware (as the case may be), and take reasonable steps to ensure that the cause of the vulnerability or likely cause of the material adverse effect is rectified, or its potential impact is mitigated, as soon as is reasonably practicable.

MAP [Y] or Device manufacturer [Z] of any Smart Metering System (excluding a Communications Hub Function or Gas Proxy Function) supplied to [X] Energy Supplier undertakes to notify [X] Supplier and all other Suppliers operating that Device as soon as reasonably practical of any material security vulnerability in, or likely cause of a material adverse effect on the security of those Devices including, such hardware, software, firmware that is supplied. MAP [Y] or Device manufacturer [Z] will provide details of the Device version and firmware version and of the vulnerability and any steps being planned or undertaken to ensure that the cause of the vulnerability or likely cause of the material adverse effect is rectified, or its potential impact is mitigated together with a timetable for when this is likely to be achieved to all those Energy Suppliers using the affected Devices. In discharging this obligation, [Z] Device manufacturer may use secure, centralised processes and information provided by the SEC Security Sub-Committee (SSC).

NOTE: This is guidance only and SEC Parties are under no obligation to use this exact wording.

Disclaimer

These guides are intended to provide a simple overview of the SEC and any supporting or related arrangements and do not replace or supersede the SEC or these related arrangements in any way. The author does not accept any liability for error, omission or inconsistency with the SEC.

During a User Security Assessment, if there are any User CIO observations relating to SEC G3.18 – G3.20 what am I expected to provide?

If the User CIO deems any contracts in place do not ensure sufficient compliance with SEC G3.18 – G3.20, the User CIO may raise this as a concern and the User will be able to address this in their Management Response and Director's Letter.

The User Management Response and Director's Letter is expected to confirm that the User will not install SMETS2 Devices without a contract being in place that satisfactorily meets the SEC obligation to notify and to be notified of material security vulnerabilities and to confirm what reasonable steps would be taken to rectify those vulnerabilities. SECAS is therefore likely to ask to see the following to provide SSC with assurance:

- a definition of 'material security vulnerability' to enable MAP/MAM/Device Manufacturers determine what the User deems to be "material";
- a Letter of Intent (LoI) from the MAP or manufacturer stating that wording and definition have been accepted and will be incorporated into the agreement(s);
- an explicit commitment in the Director's Letter* that the User will not be installing meters until contracts containing the relevant clause to satisfy G3.18 – G3.20 have been signed;
- an explicit commitment in the Director's Letter that no meters will be operated in inherit mode without having a signed contract in place as soon as reasonably practicable and within the six months defined in the Licence Conditions; and
- a clear acknowledgement that actions on G3.20 and by extension G5.18 are still outstanding if no contracts have been signed by the time the Director's Letter is sent to SECAS. **[SCF Part 2 User Assessment Guidance v1.15, Appendix E: Follow-up action prior to commencing live operations]**

** The Director should be either an Officer of the Company listed at Companies House; or an Authorised Director who has been given authority by the Board to commit the Company to completing the actions in the User management response. In the latter case, the Director's Letter should clarify below the signature "Authorised to sign on behalf of [Name of Company]".*

Relevant Licence Conditions

These Conditions apply in respect of any Domestic Premises at which there is, at the date of a Supplier Transfer in respect of that Domestic Premises, a Smart Metering System installed

- old supplier must notify new supplier of MAP that relates to asset (**LC50.3 - Electricity**) (**LC44.3 - Gas**);
- old supplier must notify MAP of the new supplier (**LC50.3 - Electricity**) (**44.3 - Gas**);
- new supplier must take reasonable steps to contract with MAP to provide the metering equipment within six months (**LC50.5 - Electricity**) (**44.5 - Gas**); and
- where terms cannot be agreed then asset must be returned within one month (**LC50.6 – Electricity**) (**44.7 - Gas**).

Further reading

Smart Energy Code:

<https://smartenergycodecompany.co.uk/download/10462/>

Security Controls Framework Part 2 – User Assessment Guidance (v1.15):

<https://smartenergycodecompany.co.uk/download/7109/>

Licence Conditions:

<https://www.ofgem.gov.uk/licences-industry-codes-and-standards/licences/licence-conditions>

Contact Us:

For all enquires or further advice, please contact SECAS at:

W: smartenergycodecompany.co.uk

T: 020 7090 7755

E: secas@gemserv.com

Disclaimer

These guides are intended to provide a simple overview of the SEC and any supporting or related arrangements and do not replace or supersede the SEC or these related arrangements in any way. The author does not accept any liability for error, omission or inconsistency with the SEC.