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.

Paper Reference:	**SECP_67_1204_17**
Action:	**For Information**

SEC Panel Sub-Committee Report

1. Purpose

This paper provides the Panel with an update on recent activities from the Panel Sub-Committees. It highlights the key issues discussed and details specific points the Sub-Committees would like to bring to the Panel's attention. The Panel are requested to note the updates.

2. Operations Group

2.1 Operations Group Meeting Highlights

SMETS1 Live Service Criteria (LSC)

The DCC provided an update on progress for the SMETS1 LSC. The Ops Group expressed disappointment that the DCC has not yet shared drafts of the artefacts that will comprise the evidence it intends to provide to the Ops Group to show it has met the LSC. The Ops Group noted that time is diminishing to review and provide feedback in advance of the LSC submission.

Data Quality Sub Group

SECAS updated the Ops Group with progress on the issues from the Panel Request for Information (RFI). SECAS noted that investigation of the Wide Area Network (WAN) coverage issue was not believed to be systemic, but rather individual issues for Parties. The Ops Group noted progress had been made with investigation of multiple meters on single Meter Point Administration Numbers (MPANs) identifying that the decommissioning process for removed meters was not being followed correctly by Parties.

The DCC is following up with Parties to provide guidance and insights and this is showing an improvement. In addition, the Data Quality Sub Group will carry out a review of the remaining issues to determine which could be rapidly progressed using available data to allow reprioritisation as appropriate.

3. Security Sub-Committee and SMKI PMA

3.1 Assurance Status Decisions

The Security Sub-Committee (SSC) set two assurance status' in March 2019. Details can be found in confidential Appendix A.

3.2 Verification Assessments

As part of their wider obligations, the SSC review the outcomes of Verification User Security Assessments. If the SSC believe that a User is non-compliant, or potentially non-compliant, with obligations contained in SEC Sections G3-G6, then they will notify the Panel.

During March 2019, the SSC reviewed four Verification User Security Assessments (VUSAs) in which Compliance Status' were set. Details of the VUSAs can be found in confidential Appendix A.

3.3 Director Letters

The SSC reviewed four Director's Letters in March 2019 which were approved and can be found in confidential Appendix A.

3.4 Security Self-Assessments

No Security Self-Assessments were reviewed by the SSC in March 2019.

3.5 SSC Highlights

Commercial Product Assurance Security Characteristics

BEIS confirmed that the SSC are now responsible for managing and maintaining the Commercial Product Assurance (CPA) Security Characteristics. The SSC considered a draft version of the Security Characteristics methodology, which included the process for making amendments to the Security Characteristics. The SSC were given one week to provide comments on the documents, after which it will be published to the SEC website. This document has also been provided to the SEC Panel under SECP_67_1204_04.

SMETS1 Segmentation

The SSC considered two options which were previously presented by the DCC relating to the SMETS1 approach for segmentation of XML certificates. Following consideration of potential costs, timescales and impacts on DCC Users, SSC Members did not vote for an alternative option and reluctantly agreed to proceed with the option that is in the current design for Initial Operating Capability (IOC). Supplier Members were strongly critical of this approach since it is complicated for Suppliers to operate and SSC were not specifically consulted on the design.

SMETS1 (Appropriate Standards)

The SSC were provided with an update in order to develop guidance for Users and the User CIO on how to interpret SEC obligations in SEC G3.26, G3.27 and G3.28, in respect of the application of an 'Appropriate Standard' of security to be applied to SMETS1 Smart Metering Systems. As such, the SSC are currently developing guidance to be published in the Security Controls Framework following review by SSC on 10 April 2019, as well as a further guidance document on SMETS1 Device Assurance which will in turn be published to the SEC Website.

SECMP0013 Meter Triage

The SSC considered and discussed the business requirement for SECMP0013 'Smart meter device diagnostics and triage', and the TABASC Chair and DCC representatives are currently working together to develop use cases of when meter resets need to take place.

3.6 SMKI PMA Highlights

SOC2 Changes for SMETS1 MOC

The SMKI PMA were informed of this update which was previously brought to SSC in relation to SOC2 procurement, specifically in relation to FIPS 140-2 compliance and the cryptographic implications. The SMKI PMA then acknowledged the multiple iterations raised by BEIS in relation to Section G of the SEC, specifically G2.44 (Cryptographic Processing).

Obtaining SMKI Device Certificates – Agreed Interpretations

The SMKI PMA were provided with an update in relation to Draft v.17 of the Agreed interpretations which have been made available for both Security Sub-Committee and SMKI PMA members to review and comment on. The SMKI PMA noted Section 8 of this document had been drafted whereby, SMKI PMA members were then asked to review and provide comments where necessary, specifically in relation to SEC Appendix D.

4. Technical Architecture and Business Architecture Sub-Committee (TABASC) and Testing Advisory Group (TAG)

4.1 TABASC Highlights

SMETS1 Services Release Business Architecture Document (BAD) & Technical Architecture Document (TAD)

In advance of SMETS1 Services Release going live later this year, the TABASC are continuing to undertake the review of the BAD and TAD to ensure that the Technical Architecture and Business Architecture is up to date and aligned with the SMETS1 Services Release content. The updated documents are expected to be issued shortly for industry review.

Modifications Proposals support

The TABASC provided the following support and advice on three different Modification Proposals:

- The TABASC discussed the Issue Resolution Process (IRP) list to be included in SECMP0055 'Incorporation of multiple Issue Resolution Proposals into the SEC' and agreed that the concerns from Meter Manufacturers should be resolved prior to providing its feedback.
- The TABASC considered that the SECMP0067 'Service Request Traffic Management' Business Requirements should include the objective of an alternative queueing functionality requirement.
- The TABASC discussed SECMP0069 'EU Exit Changes' and supported that the SEC and SEC Schedules should not be changed to remove Euros.

4.2 TAG Highlights

Release 2.0

The DCC provided an update to the TAG on the progress with CSP North Dual Band Communications Hub (DBCH) Systems Integration Testing (SIT) status using sub-GH Devices. The DCC noted that the fixes applied to resolve an outstanding defect had introduced changes that impacted ZigBee certification. The route to resolution and required regression testing was discussed with the TAG. Subsequently, the DCC has initiated their governance processes to assert that the fixes are successful and hope to see a conclusion to SIT in the near future.

The DCC also provided an update on the challenges they have faced in gaining sub-GHz Devices to complete Release 2 Device Integration Testing.

SMETS1

The TAG met twice during March with a view to reviewing completion of SIT for SMETS1 IOC. The TAG had concerns regarding the status of testing, which the DCC has been working to resolve. A further TAG meeting was scheduled for 4 April, which provides input to Panel paper SECP_67_1204_05, which sets out the TAG's recommendation to the Panel regarding completion of IOC for SIT.

The DCC is now engaging again regarding the Migration Testing Approach Document (MTAD). There are significant concerns about the late availability of this document. Similar concerns are held regarding the Systems Capacity Testing Approach Document (SCTAD). Both are critical to the confidence in the ability to successfully migrate and operate SMETS1 meters via the DCC Systems – and in the case of the SCTAD, that SMETS2 operation will not be impacted.

The DCC is engaging with TAG regarding the testing that will be undertaken for Middle Operating Capability, with TAG welcoming the earlier engagement.

5. Recommendations

The Panel is requested to **NOTE** the content of this paper.

Rebecca Jones

SECAS Team

5 April 2019

Attachments:

- Appendix A: User Security Assessments – Identified Non-Compliances (**RED**)