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_68_1005_16**
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

The Operations Group (Ops Group) will meet on the 7 May 2019. Any urgent matters arising will be advised to the Panel via a verbal update.

Agenda items to be covered by the Ops Group, (in addition to DCC reporting reviews) include;

- Major Incident reviews
- SEC Forecasting obligations
- DCC update and proposed approach to Mass Over The Air Communication Hub Firmware Updates
- SECAS Data Quality sub group update on progress
- SMETS1 enrolment Live Service Criteria (LSC) update from the DCC on the evidence they will be providing to the Ops Group
- Self Service Interface (SSI) update from the DCC
- Modifications update and utilisation of the Sub-Committee

3. Security Sub-Committee and SMKI PMA

3.1 Assurance Status Decisions

The Security Sub-Committee (SSC) set one Assurance status in April 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 April 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 two Director's Letters in April 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 April 2019.

3.5 SSC Highlights

Security Controls Framework and Agreed Interpretations

An update was provided to the SSC on proposed changes to the guidance for what constitutes a SMETS1 'Appropriate Standard' for inclusion in the Agreed Interpretations, and amendments to the Security Controls Framework (SCF) for the Assessment type, frequency for Supplier Parties and Other Users and expanding the Security obligations applicable to each User role guide.
The SSC subsequently agreed and approved the SCF V1.16 and Agreed Interpretations V1.7.

SEMP0013 Meter Triage

The SSC were provided with an update in relation to the Business Requirements previously discussed for SECMP0013 'Smart meter device diagnostics and triage'. The TABASC Chair confirmed that a use case has been developed which has been sent to the National Cyber Security Centre (NCSC) for review. This will in turn be forwarded to the Technical Specification Issue Resolution Sub Group (TSIRS) to confirm the viability from a technical point of view before coming back to the SSC.

SMETS1 Update

The SSC were provided with an update in relation to the Security Architecture V1.4 and XML Certificate Recovery. It was confirmed that the SSC comments on the SMETS1 Security Architecture V1.4 had been provided to DCC. The SSC were also provided with an update regarding XML Certificate Recovery whereby the SSC previously requested the DCC to explain the applicability of SEC Appendix L SMKI Recovery Procedures to SMETS1. It was confirmed this update would also be presented to the SMKI PMA on 16 April 2019.

SMETS1 Appropriate Standards

An update was provided to SSC members on the development of guidance for Users from the User CIO concerning how to prepare for User Security Assessments and how to interpret the SEC obligations in respect of the application of an 'Appropriate Standard' of security to be applied to SMETS1 Smart Metering Systems. Discussions are ongoing and bilaterals are planned with BEIS.

Change Items

An update was provided in relation to SECMP0024 'Enduring Approach to Communication Hub Firmware Management' which is currently undergoing the refinement process. Following feedback from the Proposer, the Working Group and the DCC, the business requirements have been

established, and solution design specifications for the proposed solution are being prepared for a DCC Preliminary Assessment. The SSC also requested the DCC to undertake a risk assessment.

3.6 SMKI PMA Highlights

SMKI Recovery in the Live Environment

An update was brought to the SMKI PMA on the DCC plans to undertake the recovery exercise currently expected to take place in June 2019, and the arrangements for early notification to key custodians who will need to be in attendance.

SMETS1 Update

The SMKI PMA were provided with an update regarding a scenario where SMETS1 Devices need to be replaced after Enrolment and Adoption. A further update was also provided by the DCC in relation to developments since the meeting with NCSC on Tuesday 9 April regarding DCC/nCipher proposals.

SEC Modifications

The SMKI PMA Chair provided an update on three SEC Modifications which are being proposed regarding changes to the SMKI Repository, Obtaining SMKI Device Certificates and changes arising from SMKI Recovery Scenarios Exercise, whilst seeking clarification against the wording for the problem statements in order to progress each Modification.

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)

The Business Architecture Document (BAD) and the Technical Architecture Document (TAD) have been updated with SMETS1 Services Release content and have been issued for industry review. Comments are due by 20 May 2019.

Modifications Proposals support

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

- The TABASC discussed SECMP0024 'Enduring approach to Communications Hub firmware management' business requirements and solution design specification, noting a number of queries and an overall observation that the business requirements need to be more detailed and handle non-happy day scenarios.
- The TABASC agreed the minor changes to the IRP list in SECMP0055 'Incorporation of multiple Issue Resolution Proposals into the SEC' and agreed that the implementation date should be moved to 7 November 2019.
- The TABASC agreed that the SECMP0067 'Service Request Traffic Management' Business Requirements are suitable for Preliminary Assessment.

Alt HAN Considerations

Following an Alt HAN update received last month, the TABASC discussed a number of points, and agreed to request specific confirmation when Alt HAN returns in June for a further update.

Elexon Half Hourly Settlement Update

ELEXON provided an update on the high-level solution design for Half-Hourly Settlements. The TABASC agreed to write to the Panel regarding concerns relating to the consequences on the smart metering infrastructure and its Users to support the changes.

4.2 TAG Highlights

Release 2.0

DCC provided an update on the resolution of the issues that have been impacting SIT completion for the northern region; the issues now appear to be resolved and a decision to agree whether SIT exit criteria are met should be imminent.

The DCC also provided an update on the challenges they have faced in gaining sub-GHz Devices to complete Release 2 Device Integration Testing, indicating that an amendment to the exit criteria may be sought. TAG considers that DIT has been beneficial in identifying issues and that the existing exit criteria are appropriate.

SMETS1

Following last month's agreement that the SIT exit criteria for IOC were met, the focus is now on migration testing and system capacity testing. Challenges affect each of these aspects of testing, with testing of each being underway prior to the closure of consultation on the approaches – therefore both are progressing at risk. There has been engagement on migration testing and the risk relates primarily to consultation responses identifying weaknesses in the currently-planned testing. There has been less engagement on system capacity testing and the concerns are more fundamental as it is currently unclear whether the testing is representative and whether it demonstrates that live system capability will be sufficient – further engagement is necessary.

BEIS has requested the support of the Panel and sub-committees in the IOC go live decision-making process and the proposed schedule has been shared. There will be a role for TAG in agreeing that additional Device Model Combinations are approved – the responsibility and process is being agreed.

November 19 Release

Engagement with TAG regarding the November 19 Release has commenced. We consider that a formal consultation on the Testing Approach Document is necessary; the TAG will contribute to this consultation.

5. Recommendations

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

Rebecca Jones

SECAS Team

2 May 2019

Attachments:

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