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_62_0911_21**
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.

2. Operations Group

2.1 DCC reporting

Report	Delivery per SEC	Content	Observations
Performance Measurement Report August 18	On Time (SEC H13.4 – Monthly 25 working days following end of month).	Per SEC H13.1. & L8.6	One Major Incident lasting 2 hours is not reflected in the DSP measures. (Incident ending 294975 – impacting Installations due to DSP change. An increased number of incorrect variant Hubs installations noted.)
DCC Responsible Communications Hub Returns Report Q3 2018	(SEC F9.15 – Quarterly) The SEC does not prescribe when after end of quarter, the report is provided.	Report received indicating 324 return requests in the period.	Incomplete DCC processing means it is not possible to draw any conclusions or trends.
DCC Network Enhancement Report (Network Enhancement Plans - NEP) Q3 2018	(SEC F7.21 "within a reasonable period of time following each quarter that ends prior to 1 January 2021").	Q3 report received 29 October	Will be reviewed at Ops Group November meeting
Registration Data Provider (RDP) Incident Report September 2018	On Time (SEC Appendix AG 2.5.10 – Monthly - timing not specified).	Per SEC Appendix AG.	7 open Incidents reported unresolved. 4 of the remaining open Incidents are all now over 60 days old. DCC is following up with RDP.

Certificate Signing Request (CSR) Variance Report – September 2018	(SEC L8.9 – 10th Working Day following month end)	Per SEC L8.9(a), 712,178 requests were sent versus a forecast of 1,284,781	None
Service Request (SR) Variance Reporting – September 2018	(SEC H3.24 – 10th working day of month)	Report not yet received	n/a
Quarterly Problem Report Q3 2018	Per SEC Appendix AG, quarterly specific timing not specified within Appendix AG.	Clause 3.2 Appendix AG Report received 24 October	Will be reviewed at Ops Group November meeting

2.2 Ops Group Meeting Highlights

Temporary Planned Maintenance

The DCC reported successful progress with the currently approved Temporary Planned Maintenance (TPM).

The DCC has made a further request to the Ops Group for changes to the latest TPM schedule. The DCC explained that no material changes to time, duration or date of slots was being proposed, only to the content at a detailed level, of the November slots. The Ops Group are considering the request ex committee.

A DNO member noted that DNOs make use of alerts from Devices that are sent as they are about to go off line, indicating a loss of supply. This capability is particularly valuable during bad weather but is lost during DCC outages. The Member requested that the Ops Group consider asking the DCC to defer planned maintenance when extreme weather is forecast. The Ops Group acknowledged the use being made of the DCC service, but noted that in the short term, completing the TPM work must take priority for the benefit of all Users. The Ops Group requested that the DNO Member bring forward a business case. Two approaches could be investigated for the longer term: 1) scheduling flexibility by the DCC and 2) a technical solution for caching of alerts.

DNO Incidents

SECAS provided an overview of initial analysis from the DCC of volumes of incorrect SMKI Certificates on Devices. The DCC informed the Ops Group that of the 32,000 Devices examined, about 36% had not had their two DNO slots populated correctly. As a first step, it was agreed that the underlying cause of the issues for the data assembled by the DCC would be shared with individual Suppliers for them to check. Ops Group Supplier Members agreed to provide feedback to the DCC by 12 November 2018. The DCC will provide a further update at the next Ops Group, where further actions will be considered as necessary.

DCC Major Incidents

The Ops Group considered 2 Category 1 Incidents that took place in September 2018. The Ops Group highlighted a number of issues with both reports including the lack of identified root causes, but not wishing to unduly delay publication of the reports to SEC Parties, agreed that these should be published, with an accompanying note explaining a number of points that the DCC agreed to address by OPSG_14.

DCC Performance Measurement Report (PMR)

The Ops Group reviewed the PMR and expressed frustration that the report continues to show DCC adherence to SEC Service Levels when operational experience by DCC Users differs. The Ops Group noted that DSP availability in the report did not take into account the Major Incident experienced in the month. The DCC said it is investigating with the DSP. The Ops Group are concerned about a lack of transparency with the report between SEC service measures and DCC Service Provider contracts. The Ops Group noted that they are not able to systematically verify the PMR at this time. The DCC stated that it is commissioning an independent audit as part of preparations for the Ofgem Operational Performance Regime review. The Ops Group welcomed this but requested that SECAS formally log inconsistencies and report these to the Panel in future.

DCC Communications Hub Ordering

The DCC presented a proposed approach for providing Parties with early access to small volumes of new variants of Communication Hubs. The Ops Group agreed that the proposal should be given detailed consideration, and that this would best be done via a Modification.

3. Security Sub-Committee and SMKI PMA

3.1 Assurance Status Decisions

The Security Sub-Committee (SSC) set seven assurance statuses in October 2018. Details can be found in confidential Appendix A.

3.2 Director Letters

The SSC reviewed one Director's Letter in October 2018, which showed there were no non-compliances to prevent the User in question beginning to use DCC Live Systems. Details can be found in confidential Appendix A.

3.3 Verification Assessments

As part of their wider obligations, the SSC review the outcomes of Verification 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 notify the Panel.

During October 2018, the SSC reviewed one Verification Assessment. Details of the non-compliances can be found in the confidential Annex A of Appendix A.

3.4 Security Self-Assessments

The User is responsible for conducting the Security Self-Assessment (SSA) using internal resources and under their own timescales, and is responsible for producing a report to be presented to the User CIO for review within a pre-agreed timescale prior to the results being provided to the SSC for review. The SSC reviewed 2 SSAs and the details can be found in the confidential Appendix A.

3.5 SSC Highlights

SMETS1 Device Assurance Survey

Following the SMETS1 Device Assurance workshop that took place on 25 September 2018, the SSC issued the SMETS1 Device Assurance Survey to Supplier Parties. The survey aims to identify existing good industry practice. The findings will help the SSC to develop guidance to be included in the Security Controls Framework (SCF), in addition to ensuring proportionality and avoiding unnecessary duplication of assurance activities by multiple Suppliers. Responses were required by 26 October and are now being reviewed by PA Consulting.

ADT Workshop

The SSC met with representatives from the TABASC, the Ops Group and the DCC Operations team, following on from the initial workshop in May 2018. The purpose of the initial workshop was to ensure that the DCC and User Anomaly Detection Threshold (ADT) volumes and values act as an effective means of detecting any Compromise to any relevant part of the DCC Total System or User Systems, whilst also ensuring the smooth operation of Smart Metering Systems with supporting ADT guidance. The group addressed all outstanding actions from the initial workshop, which additionally gave rise to new ones.

SSC Risk Register – ISO27005

With the quarterly review of the SSC Risk Register taking place, the SSC have identified that it would be beneficial to have the Risk Register align with the ISO27005 Standard. SECAS have begun undertaking the necessary work.

3.6 SMKI PMA Highlights

SMKI Recovery

As requested by the SMKI PMA, the DCC have agreed to undertake proving of SMKI Recovery in the live environment. The DCC presented the SMKI PMA with the risks associated with the Recovery exercise and agreed to update the group further once the exercise has begun.

Obtaining Device Certificates via SPOTI

The SMKI PMA discussed an issue that was raised at the September 2018 Panel meeting which relates to obtaining Device Certificates via the SMKI Portal via the Internet (SPOTI), and the need for Device Manufacturers or other non-Supplier Parties such as Meter Asset Providers (MAPs), Meter Operators (MOPs) or Shared Resource Providers (SRPs) to put Certificates on Devices.
The SMKI PMA noted that any access to SPOTI to obtain Device Certificates would require completion of SMKI and Repository Entry Process Tests (SREPT). Additionally, the group considered options that may meet the business needs described by the stakeholders.
The group agreed that a risk assessment will need to be undertaken to understand the security risks associated with making Device Certificates available to Parties that are not regulated under the SEC.

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

4.1 TABASC Highlights

SMETS Version & TS Applicability Tables Update

The Technical Specification (TS) Applicability Tables set out which versions of SMETS and CHTS a Device must comply with, either for installation or on-going maintenance of a given Device. This has been updated by BEIS for Release 2 and is being revised again for the implementation of SECMP0006 'Specifying the number of digits for device display', which specifies the number of digits on a Device's display. The TABASC agreed that the end dates for installation and maintenance of SMETS2 v3.0 meters should be the point at which v3.1 becomes available, subject to confirmation that v3.0 Devices are not being developed.

BEIS led Smart Flexibility Call for Evidence 'A Smart, Flexible Energy System'

BEIS presented on the development of the smart systems and flexibility plan, where the TABASC were invited to provide feedback related to the Technical and Business Architecture aspects.

SEC Quarterly Work Package & Industry Oversight

SECAS presented the actual spend for the TABASC in Quarter 2 and the budget for Quarter 3. The TABASC advised on other project budgets that need to be taken into account and raised the need to provide oversight and input on industry developments at each TABASC meeting.

4.2 TAG Highlights

The TAG has not met since 10 October 2018, when the Release 2.0 Live Service Criteria and supporting evidence was considered to form a recommendation to the Panel for consideration on 19 October 2018. The TAG will meet again on 6 November 2018 to primarily discuss the outstanding Severity 2 defect (70771) and updates to the SMETS1 Services items such as Migration Testing, System Capacity Testing and User Testing updates.

5. Recommendations

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

Hollie McGovern

SECAS Team

2 November 2018

Attachments:

Appendix A – Security Assurance Status Update (**RED**)