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.

Headlines of the Security Sub-Committee (SSC) 95_2602

At every meeting, the SSC review the outcome for Users' Security Assessments and sets an Assurance status for Full User Security Assessments (FUSAs) or a Compliance status for Verification User Security Assessments (VUSAs). The SSC also reviews outstanding actions, monitors the risks to the Commercial Product Assurance (CPA) certification of Devices, considers available updates from the DCC on Anomaly Detection and any reported changes in Shared Resource Providers by Users and reported Security Incidents and Vulnerabilities.

The SSC reviewed the following which are classified as **RED** and therefore recorded in the Confidential Meeting Minutes:

- Considered the assurance status for one initial FUSA;
- Set a compliance status for four VUSAs;
- Noted one Security Self-Assessment (SSA); and
- Approved three Director's Letters.

The SSC also discussed the following items:

Matters Arising

- The SSC Chair informed Members of progress made in regard to Security Assessments by two separate Users. (**RED**).
- The SSC Chair sought advice from Members relating to facilitating compliance with SEC Section G3.20. (**RED**).
- The SSC Chair confirmed that a letter from Ofgem was issued on Thursday 20 February 2020, reminding Operators of Essential Services (OES) of their obligations under the Network Information Systems (NIS) Directive, where applicable.
- SECAS encouraged Members to give consent to participate in the annual SECAS Customer Satisfaction Survey and asked Members to raise awareness within their organisation, contacts and respective trade bodies by 5pm on Friday 6 March 2020.

Agenda Items

11. **SECMP0007:** SECAS presented an update regarding the SEC Modification SECMP0007 'Firmware updates to IHDs and PPMIDs' and sought SSC advice on a proposed solution to allow for the modification to progress smoothly. The SSC agreed that HCALCs should have

the same Anomaly Detection Threshold (ADT) rules as ESME and GSME, and agreed to commission a risk assessment on the SECMP0007 proposed solution upon receipt of the DCC's Impact Assessment. SECAS also presented updates on Draft Proposals DP112 'Setting the Privacy Assessment Assurance Status', DP113 'Unintended Data Disclosure when using SR8.2', DP115 'Changes to the NCSC Good Practice Guides', DP116 'Service Request Forecasting', and DP117 'Bulk CH returns'.

12. **SMETS1:** The DCC presented updates regarding the different aspects of SMETS1 enrolment, including the DCC's remediation plan; CIO report updates; negative testing and HAN Control Assurance; Certificate issues; and the Live Services Criteria. (**RED**).

13. **OTA and DCC Disaster Recovery:** The SSC considered a request for advice from the DCC relating to Over The Air (OTA) firmware upgrades and DCC Disaster Recovery. (**RED**).

14. **Proposals for Enhanced Separation between ECoS and DSP:** The SSC considered a request for advice from BEIS for Enhanced Separation between the Enduring Change of Supplier (ECoS) role and the DCC's Data Service Provider (DSP). (**AMBER**).

17. **Post Commissioning Report:** The DCC presented the Post Commissioning Report in the latest format and noted feedback from Members. (**RED**).

18. **Use Case – Factory Reset:** The SSC Chair presented a proposal for Use Case Guidance relating to Factory Reset and invited comments from SSC Members. (**AMBER**).

For further information regarding the Security Sub-Committee, please visit here.

Next Meeting: Wednesday 11 March 2020