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) 106_1208

At every meeting, the SSC review the outcome for Users' Security Assessments and sets an Assurance status for Initial Full User Security Assessments (FUSAs) or a Compliance status for Verification User Security Assessments (VUSAs) and subsequent FUSAs. 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 SMETS1 enrolment and 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:

- Set a compliance status for one VUSA;
- Noted one Security Self-Assessment (SSA);
- Approved one VUSA Remediation Plan and Director's Letter;
- Approved one FUSA Remediation Plan and Director's Letter; and
- Noted a progress update on one FUSA Remediation Plan and Director's Letter.

The SSC also discussed the following items:

Matters Arising

- The SSC noted an update regarding the User CIO contract. (**RED**)
- The SSC noted an update on a Small Supplier's change of Shared Resource Provider (SRP). (**RED**)
- The SSC noted an update on SECMP0007 'Firmware updates to IHDs and PPMIDs', and agreed on a solution for Anomaly Detection Threshold (ADT) rules for Prepayment Interface Devices (PPMIDs), advising that ADT rules for PPMIDs should be set at the Supplier's discretion, with guidance on the risk being provided through the DCC's guidance on ADT.
- The SSC noted a CPL entry with an incorrect hash value and agreed a proposed solution. (**RED**)
- The SSC agreed to a request by the proposer of SECMP094 'Supporting prepayment customers in no SM WAN scenarios', to attend the SSC for a discussion on the aforementioned SEC Modification. The SSC also agreed to a request for a formal response as to why the SSC agreed that the proposed solutions for SECMP0037 'Pairing Local

PPMIDs' and SECMP0038 'Sending Commands via PPMIDs' were not considered secure as explained in the draft minutes of the SSC meeting on Wednesday 8 February 2017.

- The SSC noted an update on the Commercial Product Assurance (CPA) Security Characteristics (SC) Threat Mapping. (**RED**)
- The SSC noted the British Standards Institution (BSI) Consultation on PAS 1878 which has been published and is available for review and comment here.
- The SSC noted an invitation to a Cyber Security Event by Ernst & Young (EY). (**GREEN**)
- The SSC noted a SECAS survey of the SEC Panel and Sub-Committees regarding remote working arrangements. (**GREEN**)

Agenda Items

6. **SEC Section G3.20:** SECAS presented proposals for SEC Section G3.20 and received feedback from SSC Members. (**AMBER**)

8. **Market Wide Half Hourly Settlements:** Gemserv presented proposals for Market Wide Half Hourly Settlements and noted feedback from Members. (**AMBER**)

9. **SOC2 Update**: The DCC presented its update on the 2019 SOC2 Report and noted feedback from SSC Members. (**RED**)

10. **SMETS1:** The SSC noted DCC updates regarding the different aspects of SMETS1 enrolment including the DCC's Initial Operating Capability (IOC)/Middle Operating Capability (MOC) MDS Remediations; Active and Monthly Dormant Migration Process, CIO report updates, Home Area Network (HAN) Control Assurance, MOC Morrison Data Services (MDS) Cohort, and MOC Secure Remediations. (**RED**)

12. **DCC Network Evolution:** The DCC presented an update relating to Network Evolution and noted feedback from Members. (**RED**)

13. **SSC Risk Assessment:** The SSC Consultants presented an update relating to the SSC Risk Assessment and noted feedback from Members. (**RED**)

14. **Anomaly Detection Report:** The DCC presented the most recent version of the Anomaly Detection Report in the latest format and noted feedback from Members. (**RED**)

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

Next Meeting: Wednesday 26 August 2020