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) 102_1006

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 two VUSAs;
- Noted two Security Self-Assessment (SSA);
- Approved one FUSA Director's Letter; and
- Noted one notification of a Second User System.

The SSC also discussed the following items:

Matters Arising

- The SSC noted an update from BEIS on an SSC query regarding Department for Digital, Culture, Media, and Sport (DCMS) Guidance on 'Secure by Design'. (**AMBER**)
- The SSC noted two BEIS consultations regarding a government response on Enduring Change of Supplier (ECoS) Separation; and regarding User Roles. (**AMBER**)
- The SSC noted updates regarding the SSC Risk Assessment; the Standalone Auxiliary Proportional Controller (SAPC) Commercial Product Assurance (CPA) Security Characteristics (SC) Workshop; and the User CIO re-procurement. (**RED**)

Agenda Items

7. **SCF Updates – CREST/CHECK Testing Proposals:** The SSC noted the proposed Security Controls Framework (SCF) updates and approved the SCF as amended. (**AMBER**)

8. **Manufacturers Notifying Vulnerabilities:** The SSC agreed on amendments to a proposed notification form for Manufacturers to notify the SSC of identified material security vulnerabilities

and agreed to alert Manufacturers to the CPA Build Standard Guidance once published by NCSC. (**AMBER**)

10. **SMETS1:** The SSC noted DCC updates regarding the different aspects of SMETS1 enrolment including the DCC's Active and Monthly Dormant Migration Process, CIO report updates, HAN Control Assurance, MOC MDS Cohort; Fast Track PPCT; and the DMCT additions to the EPCL. (**RED**)

12. **Anomaly Detection:** The DCC presented the most recent version of the Anomaly Detection report and noted feedback from SSC Members. (**RED**)

13. **SOC2 Update**: The DCC presented their update on the 2018 SOC2 Report and noted feedback from SSC Members. (**RED**)

14. **DCC Request – Network Evolution:** The DCC presented its request relating to Network Evolution and noted feedback from Members. (**RED**)

15. **MP113 Solution:** SECAS presented an update on SEC MP113 'Unintended Data Disclosure when using SR8.2' and presented several proposed solutions. SSC Members provided feedback on the potential resolution for SECAS to investigate.

16. **Q2 Work Package:** The SSC noted the Q2 Work Package of administrative expenditure and agreed to recommend the Q2 Work Package to the SECCo Board. (**AMBER**)

17. **DCC Request - ACB:** The DCC noted that further work would be done on proposals relating to replacing Access Control Brokers (ACB) Certificates and noted feedback from Members. (**RED**)

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

Next Meeting: Wednesday 24 June 2020