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) 161_1101

At every meeting, the SSC review the outcome for Users' Security Assessments and set 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 User Security Assessments, the outcomes of which are classified as **RED** and therefore recorded in the Confidential Meeting Minutes:

- Set the Compliance Status for two Full User Security Assessments (FUSAs) and three Verification User Security Assessments (VUSAs).
- Approved one VUSA Remediation Plan and Director's Letter.

The SSC also discussed the following items:

Matters Arising

- The SSC noted an update on User Competent Independent Organisation (CIO) Assessments of De-Commissioned Services **(RED)**
- The SSC noted an update on a material change. **(RED)**
- The SSC noted an update on NCSC communications. **(RED)**
- The SSC noted an update on the review of the Security Architecture Document. **(RED)**
- The SSC noted an update on Enduring Change of Supplier (ECoS) Anomaly Detection Threshold (ADT) capability. **(AMBER)**

Agenda Items

7. **DCC CIO Assessment:** The SSC noted an update on the DCC CIO Assessments. **(RED)**
9. **CPA Monitoring:** The SSC was presented with an update on withdrawn Certificates and the expiry of Commercial Product Assurance (CPA) Certificates. The SSC was also presented with a Pre-Payment Report and an update on Pending figures. The SSC **AGREED** to defer the removal of the affected Devices, which was originally planned for January 27, subject to affected Suppliers providing a named Responsible Owner to be accountable for a Remediation Plan to ensure that affected Devices are upgraded, and to provide regular

reporting of progress to the SSC who will keep the removal from the CPL under review. **(RED)**

10. **CPA-Related Issues:** The SSC Chair presented an update on ongoing discussions with NCSC regarding CPA-related issues, including feedback from the SSC CPA Issue Resolution Sub-Group (SCIRS). **(AMBER)**
11. **BEIS Consultation: Changes to SEC/Licence:** The SSC noted an update on the BEIS Consultation on changes to the SEC/Licence. **(GREEN)**
12. **Communication Hubs Limitations (EM357):** The SSC was presented with an update on Communication Hubs limitations. **(RED)**
13. **Unit Inconsistency SMETS2 Meters:** The SSC noted an update on a unit inconsistency in SMETS2 Meters. **(RED)**
14. **DCC CIO Procurement Update:** The SSC noted an update on the DCC CIO procurement process. **(RED)**
15. **PKI Enduring Service – Business Needs:** The SSC noted an update on the Public Key Infrastructure (PKI) Enduring Service. **(RED)**
16. **Incident Management Update:** The SSC noted an update on outcomes and actions from the Incident Management Exercise held in December. **(RED)**
17. **Risk Assessment Review:** The SSC noted an update on the SSC Risk Register and provided feedback. **(RED)**

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

**Next Meeting: Wednesday 25 January 2023.**