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) 163_0802

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 one Full User Security Assessment (FUSA), one Verification User Security Assessment (VUSA) and one Security Self-Assessment (SSA).

The SSC also discussed the following items:

Matters Arising

- The SSC noted an update regarding an in-person meeting in March.
- The SSC noted a Shared Resource Provider notification. **(RED)**
- The SSC noted an update on two material changes. **(RED)**
- The SSC noted an update on a Panel discussion. **(RED)**
- The SSC noted an update on actions taken from the User Security Assessments Feedback Workshop. **(RED)**
- The SSC noted an update on the Joint Industry Cyber Security Incident Management Plan (JICSIMP). **(RED)**
- The SSC noted that, following a Change Board meeting on 1 February 20-23, MP172 'Reduced CPA & CPL requirements for innovation and Device field trials' was voted to pass as supporting SEC objectives a) and e).
- The SSC noted a request from an Other SEC Party. **(RED)**

Agenda Items

4. **DCC CIO Assessment:** The SSC noted an update on the DCC CIO Assessments. **(RED)**
6. **CPA Monitoring:** The SSC was presented with an update on withdrawn Certificates and the expiry of Commercial Product Assurance (CPA) Certificates.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 an update on Pending figures and the Prepayment Report along with Supplier Remediation Plans submitted as required by SEC Appendix Z, particularly noting Suppliers who have not submitted Remediation Plans. **(RED)**

7. **CPA-Related Issues:** The SSC Chair presented an update on CPA-related issues, including, discussion of the agenda for the SSC CPA Issue Resolution Sub-Group (SCIRS) meeting on 13 February 2023. **(AMBER)**
8. **ECoS Risk Assessment:** The DCC presented the Enduring Change of Supplier (ECoS) Risk Assessment, and the SSC noted the update. **(RED)**
9. **DCC Gateway Risk Review:** The SSC noted an update on the DCC Gateway Risk Review. **(RED)**
10. **DCC CIO Procurement:** The SSC noted an update on the DCC CIO Procurement. **(RED)**
11. **Network Evolution DSP:** This SSC noted an update on the Network Evolution Data Service Provider (DSP). **(AMBER)**
12. **Alt HAN Options:** The SSC noted an update on the Silabs Communication Hubs Risk Assessment. **(RED)**
13. **Lookback Report:** SECAS provided the SSC with a lookback report against the Q3 (October – December) 2022 Work Package, and the SSC noted the report. **(AMBER)**

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

Next Meeting: Wednesday 22 February 2023.