This document is classified as **Clear** 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) 175_0908

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 Follow Up Assessment and one Security Self-Assessment (SSA).

The SSC also discussed the following items:

Matters Arising

- The SSC noted an update on a User Security Assessment Remediation Plan. **(RED)**
- The SSC noted an intent to notify a Material Change. **(RED)**
- The SSC noted a Party's intent to cease to be a SEC Party. **(RED)**
- The SSC noted that the amended Risk Assessment Iteration 9A will be brought to a future meeting **(GREEN)**
- The SSC noted that a DCC consultation on the "delivery plan for SMKI Service Continuity" has been released.
- The SSC noted that the NCSC announced on 8 August 2023 the launch of Cyber Incident response (CIR) Scheme level 2 from 15 August 2023. The NCSC recommends that any organisation within the UK uses an incident response company from the NCSC CIR scheme.

Agenda Items

4. **Remediation Plan Update:** The SSC noted an update on User Security Assessment Remediation Plans. **(RED)**
5. **DCC CIO Assessment:** The SSC noted an update on the DCC CIO Assessments. **(RED)**
6. **DCC CIO Assessment Scope:** The SSC noted an update on upcoming DCC CIO Assessments. **(RED)**

8. **CPA Monitoring:** The SSC was presented with an update on withdrawn Certificates and the expiry of Commercial Product Assurance (CPA) Certificates.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 Pre-Payment Meters. (**RED**)
9. **CPA-Related Issues:** The SSC Chair presented an update on CPA-related issues, including an update on the CPA Build Standard for Triage Tools and Triage System Interfaces. (**AMBER**)
10. **PKI-E High Level Requirements:** The SSC noted a DCC update on Public Key Infrastructure – Enduring (PKI-E) High Level Requirements. (**AMBER**)
11. **TCoS to ECoS Private Key Transfer:** The SSC noted a DCC update on Transitional Change of Supplier to Enduring Change of Supplier Private Key transfer. (**RED**)
12. **SMETS1 EPCL 31:** The SSC noted a DCC update on the Eligible Products Combination List (EPCL) Report 31 and **APPROVED** the Devices for inclusion on the EPCL. (**RED**)
13. **Modification Proposal - NCSC Qualifications – DCC Standards:** The SSC discussed a Modification Proposal for NCSC Qualifications and DCC Standards. (**RED**)
14. **Q1 Lookback Report:** SECAS provided the SSC with a lookback report against the Q1 (April – June) 2023 Work Package, and the SSC noted the report. (**RED**)
15. **MP231 'Firmware upgrade pathways':** The SSC discussed MP231 'Firmware upgrade pathways'. (**RED**)
16. **MP168 'CPL Security Improvements':** The SSC discussed MP168 'CPL Security Improvements'. (**RED**)
17. **JICSIMP Review:** The SSC was presented with an update on the Joint Industry Cyber Security Incident Management Plan (JICSIMP) review. (**RED**)

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

Next Meeting: Wednesday 23 August 2023.