This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

Headlines of the Security Sub-Committee (SSC) 176_2308

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 three Full User Security Assessments (FUSAs).

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 update on an Event of Default. **(RED)**
- The SSC noted an update on a material change. **(RED)**
- The SSC noted that SMKI PMA has raised a SEC Modification to amend the DCCKI Certificate Policy to support the process set out in SEC Section G2.22F to G,2.22I. **(GREEN)**
- The SSC noted that the SSC Chair gave a quarterly update to the SEC Panel on 22 August 2023. **(GREEN)**
- The SSC noted an update on Threat Assessment capabilities. **(RED)**
- The SSC noted that an update on SSC elections. **(GREEN)**

Agenda Items

5. **Remediation Plan Update:** The SSC noted an update on User Security Assessment Remediation Plans. **(RED)**
6. **User CIO SCF:** The SSC was provided with the latest updates to the User CIO Security Controls Framework (SCF) and approved it for publication. **(RED)**
7. **DCC CIO Assessment:** The SSC noted a verbal update on the DCC CIO Assessments. **(RED)**

8. **DCC CIO Forward Look:** The SSC noted an update on upcoming DCC CIO Assessments. **(RED)**
10. **CPA Monitoring:** The SSC was presented with an update on withdrawn Certificates and the expiry of Commercial Product Assurance (CPA) Certificates.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)**
11. **CPA-Related Issues:** The SSC Chair presented an update on CPA-related issues. **(AMBER)**
12. **Post Commissioning Report:** The DCC presented the latest Post Commissioning Report. **(RED)**
13. **Anomaly Detection Report:** The DCC presented the latest Anomaly Detection Report. **(RED)**
14. **SEC Modifications Update:** SECAS presented an update on the progress of Modifications the SSC had previously expressed an interest in and new Modifications that may be of interest to the SSC. The SSC noted the update and provided feedback. **(GREEN)**
15. **Testing Automation Framework:** The SSC noted an update on the Testing Automation Framework (TAF). **(RED)**
16. **Incident Management:** The DCC presented an update on outstanding actions from the Incident Management exercise in December 2022. **(RED)**
17. **Silabs:** This SSC noted an update on Silabs. **(RED)**
18. **PKI-E:** The SSC noted a DCC update on Public Key Infrastructure – Enduring (PKI-E). **(RED)**
19. **JICSIMP Scenarios:** The SSC was presented with an update on the Joint Industry Cyber Security Incident Management Plan (JICSIMP) Scenarios **(RED)**

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

Next Meeting: Wednesday 13 September 2023.