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) 88_2310

At every meeting, the SSC review the outcome for Users' Security Assessments and sets an Assurance status for Full User Security Assessments (FUSAs) or a Compliance status for Verification User Security Assessments (VUSAs). 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 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 **RED** and therefore recorded in the Confidential Meeting Minutes:

- One Compliance Status for a VUSA;
- Approved one Director's Letter;
- Noted one Security Self-Assessment (SSA); and
- Noted Remediation Plan updates for User Security Assessments.

The SSC also discussed the following items:

Matters Arising

1. The SSC noted a Supplier's intention to operate meters in pre-payment mode. **(RED)**
2. The SSC noted that a Problem Statement DP091 'Updating Security Assurance Status' has been created which identifies that the wording of the Security Assessment assurance status terminology set out in SEC Sections G8.36 – G8.37 does not reflect the substantial remediation that is required for 'Provisionally approved' and 'Deferred'. It is proposed that the terminology is amended to 'Deferred' and 'Rejected' respectively. It has now been raised as a Draft Modification and will be discussed at the Change Sub-Committee on Tuesday 29 October 2019, with a recommendation it be presented to the SEC Panel on Friday 15th November 2019 for conversion to a full Modification Proposal.
3. The SSC Chair advised that he has responded to the BEIS consultation regarding SMETS1 Interoperability and has expressed an interest on behalf of the SSC. **(RED)**
4. The SSC agreed to discuss the criteria regarding CPA Assurance Maintenance for Device re-certification before publishing guidance. **(RED)**
5. The SSC agreed to take the CPA Use Case for Factory Reset to the Industry Working Group on Wednesday 6 November 2019.

Agenda Items

8. **Standards Guidance for Vulnerability Management in Agreed Interpretations:** The SSC Chair advised that members have until Friday 8 November 2019 to provide any comments on the proposed amendments to the Agreed Interpretations. (**AMBER**)
9. **Quarterly SSC Standards**: The SSC noted an update regarding new versions of industry standards which are referenced throughout Section G, such as ISO/IEC 27001:2013. It will now be published on the SECAS website.
10. **SMETS1:** The DCC presented updates regarding the different aspects of SMETS1 enrolment, including the DCC's remediation plan, CIO report, updated incident management actions, functional testing, SMETS1 Device Assurance Proposals and agreed to review a statement for the upcoming Live Services Criteria. (**RED**)
11. **DCC Anomaly Detection Attributes:** The DCC proposed suggested values for Anomaly Detection Attributes and the SSC agreed to review these prior to the next SSC meeting. (**RED**)
12. **DCC Elective Communication Services:** The DCC provided an update regarding the Elective Communication Services proposals. (**AMBER**)
13. **Supplier of Last Resort (SoLR) and Pre-Payment (PPM) Customers:** SECAS provided an update regarding the proposed solutions for protecting PPM customers during a SoLR event. (**AMBER**)
14. **CodeWorks – The Digital SEC**: SECAS gave a live demonstration of the new Digital SEC and advised SSC Members on the registration process.

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

Next Meeting: Wednesday 13 November 2019