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) 90_2711

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:

- 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 Chair informed Members that guidance relating to the Use Case 'To identify installed SMKI Certificates' has been circulated for Industry comment by Friday 6 December 2019. The Industry Working Group agreed the guidance could now include the Public Certificate number behind a menu . It was noted that the SSC Chair is attending a meeting with NCSC and BEIS on Tuesday 4 December 2019 to finalise the security controls required at triage facilities. A further update will be provided at the next SSC meeting on Wednesday 11 December 2019.
2. The SSC Chair gave an update on the stages compromising the Security Architecture Document (SAD) review, and SSC Members have been asked for their availability to attend the Security Incident Management exercise in February 2020. (**AMBER**)
3. The SSC discussed a query from a User regarding the security implications from Office of Meter Accuracy Testing (OFMAT) testing. (**AMBER**)
4. The SSC Chair (GH) provided an update regarding a journalist seeking to identify smart metering security issues and has offered SSC input. (**RED**)
5. Under the confidential action 'SSC Conf 88/11', a BEIS Representative highlighted that funding has now been allocated for SMETS1 Device Assurance testing. (**RED**)

Agenda Items

4. **User CIO Re-Procurement Exercise:** In line with SEC G7.20(h), SSC Members provided feedback on the current User Competent Independent Organisation (CIO) service provider in light of the upcoming User CIO re-procurement exercise. (**RED**)
8. **ADT End User Submission and Quarantine Management:** The SSC approved the DCC's request to change the way in which users submit ADT values. (**RED**)
9. **SMETS1:** The DCC presented updates regarding the different aspects of SMETS1 enrolment, including the DCC's remediation plan; CIO report updates; functional testing; SMETS1 alert storms; the depth and breadth testing documents for Final Operating Capability (FOC); the risks of XML signing enforcement; Device Assurance proposals; SMETS1 Certificate issues; and the Joint Industry Cyber Security Incident Management Plan (JICSIMP) Scenario Workshop feedback. (**RED**)
10. **Post Commissioning Report:** The DCC presented the Post Commissioning Reports in the latest format and noted feedback from Members. (**RED**)
11. **Alternative SOC2 Approach:** The DCC presented the proposals for an alternative approach to SOC2. (**RED**)

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

Next Meeting: Wednesday 11 December 2019