

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) 101_2705

At every meeting, the SSC review the outcome for Users' Security Assessments and sets 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 which are classified as **RED** and therefore recorded in the Confidential Meeting Minutes:

- Set an assurance status for two initial FUSAs;
- Set a compliance status for one second or subsequent FUSA;
- Set an assurance status for one Follow-Up Assessment; and
- Noted one Security Self-Assessment (SSA).

The SSC also discussed the following items:

Matters Arising

- A manufacturer requested SSC assistance in dealing with a query from a Commercial Product Assurance (CPA) Test Lab. (**RED**)
- BEIS hosted a session on Incident Planning on Monday 18 May 2020, and reviewed lessons learned from the SSC Joint Industry Cyber Security Incident Management Plan (JICSIMP).
- Agenda item 16 – MP113 Solution – had been replaced by an agenda item on [SEC MP105 'Sending SR11.2 to Devices in a Suspended State'](#).
- A change has been made to the scope of an SSC risk assessment due to news of a cyber-attack on an energy code administrator. (**AMBER**)
- The SSC was informed of the escalation of a risk by the SMKI PMA to the SEC Panel. (**RED**)
- Two SSC Members volunteered to represent the SSC on the SMKI PMA and the TABASC Sub-Committees, respectively. (**AMBER**)
- The SSC was informed of project updates regarding the CPA Security Characteristics (SC) Threat Mapping project; a new CPA SC for Standalone Auxiliary Proportional Controller (SAPC); and the User CIO re-procurement process. (**RED**)

- Middle Operating Capability (MOC) has been rescheduled, which necessitates a rescheduling of the SSC recommendation of the Live Service Criteria. (AMBER)
- DCC has requested SSC engagement regarding the Network Evolution Project at the SSC Meetings on Wednesday 10 and 24 June 2020. (GREEN)

Agenda Items

- 9. SCF Updates:** SECAS presented the SSC with proposed Security Controls Framework (SCF) updates and the SSC approved the SCF as amended. (AMBER)
- 10. SMETS1:** The SSC noted DCC updates regarding the different aspects of SMETS1 enrolment including the DCC's Active and Monthly Dormant Migration Process, Remediation Plan, CIO report updates, HAN Control Assurance, and the MOC MDS Cohort. (RED)
- 12. Post-Commissioning Report:** The DCC presented the April Post Commissioning Report in the latest format and noted feedback from Members. (RED)
- 14. DCC Request - ACB:** The DCC presented its request relating to replacing Access Control Brokers (ACB) Certificates and noted feedback from Members. (RED)
- 15. HSM Security Incident:** The DCC Data Service Provider (DSP) presented its report on a Hardware Security Module (HSM) Security Incident and noted comments from Members. (RED)
- 16. MP105:** SECAS presented an update on [SEC MP105 'Sending SR11.2 to Devices in a Suspended State'](#) and advised that the target for implementation is either the June or November 2021 SEC release. SSC Members provided feedback on the potential resolution for SECAS to investigate.
- 17. New Draft Proposals and Modifications Proposals Updates:** Updates were given on Draft Proposals and Modification Proposals including:
 - [DP128 'Gas Network Operators SMKI Requirements'](#)
 - [DP126 'Smart meter consumer data access and control'](#)
 - [MP123 'IVP realignment of SMETS2 v2.0 and v3.1'](#)
 - [MP117 'Bulk CH Returns'](#)
 - [MP113 'Unintended Data Disclosure when using SR8.2'](#)
 - [DP094 'Supporting prepayment customers in no SM WAN scenarios'](#)
- 18. SAD Approval:** The SSC was presented with the latest draft of the Security Architecture Document (SAD), and voted to approve the latest draft of the SAD as written. (AMBER)

19. **Q4 Lookback Report:** The SSC noted the Q4 lookback report of administrative expenditure.
(**AMBER**)

For further information regarding the Security Sub-Committee, please visit [here](#).

Next Meeting: Wednesday 10 June 2020