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) 118_2402

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 Security Self-Assessment (SSA);
- Approved three Full User Security Assessment (FUSA) Remediation Plans and Director's Letters;
- Approved one FUSA Director's Letter;
- Approved one Verification User Security Assessment (VUSA) Remediation Plan and Director's Letter;
- Approved one Security Self-Assessment Remediation Plan; and
- Noted one notification of a Second User System.

The SSC also discussed the following items:

Matters Arising

- The SSC noted an update regarding the User ID of a Supplier. **(RED)**
- The SSC noted an update regarding a SEC Obligation on the SSC. **(RED)**
- The SSC noted an update regarding the outcome of a User Security Assessment for a Small Supplier. **(RED)**
- The SSC noted an update regarding Supplier of Last Resort (SoLR). **(RED)**
- The SSC were advised of an Ops Group presentation by the DCC that was of interest. **(RED)**
- The SSC noted a recent National Cyber Security Centre (NCSC) Cyber Security Information Sharing Partnership (CiSP) presentation given regarding cyber security and encouraged attendance in future presentations. **(GREEN)**
- The SSC noted an update regarding Use Cases for triage / Device refurbishment. **(AMBER)**

- The SSC noted an update regarding the BEIS Smart Meter Cyber Incident Exercise. **(AMBER)**

Agenda Items

8. **SCF Updates:** The SSC Chair presented proposed updates to the Security Controls Framework (SCF) and Agreed Interpretations (AIs), and the SSC approved the amendment presented. **(AMBER)**

10. **CPA Monitoring:** The SSC was presented with an update on the early expiry of Commercial Product Assurance (CPA) Certificates and noted the latest Prepayment Meters (PPM) Report. **(RED)**

11. **CPA Industry Days:** The SSC Chair presented proposals based upon feedback received at the CPA Industry Days that took place throughout November 2020, and the SSC provided input on the outstanding actions. **(AMBER)**

12. **SMETS1 Update:** The SSC noted DCC updates regarding the different aspects of SMETS1 enrolment, including the Final Operating Capability (FOC) Live Service Criteria (LSC); FOC CHECK Assurance and CIO Report; Initial Operating Capability (IOC)/Middle Operating Capability (MOC) MDS remediations; the Active and Monthly Dormant Migration Process; CIO report updates; Home Area Network (HAN) Control Assurance; and MOC Secure remediations. **(RED)**

13. **SMETS1 HAN Assurance Report:** The DCC provided an update on the SMETS1 Home Area Network (HAN) Assurance Report. **(RED)**

14. **TSP Re-Procurement:** The DCC presented an update on Trusted Service Provider (TSP) Re-Procurement and agreed to return with further updates. **(RED)**

15. **CSS Risk Treatment Plan:** The DCC presented the DCC's Central Switching Service (CSS) Risk Treatment Plan (RTP) and noted feedback by the SSC. **(RED)**

16. **Post-Commissioning Report:** The DCC presented the Post-Commissioning Report for January 2021 and advised of future improvements to the Post-Commissioning Report. **(RED)**

17. **Anomaly Detection Report:** The DCC presented the latest Anomaly Detection Report and noted suggestions by the SSC regarding reporting. **(RED)**

18. **MP104 'Security Improvements':** SECAS presented an update on MP104 'Security Improvements' and noted suggestions by the SSC. **(GREEN)**

19. **New Draft Proposals and Modification Proposals Update:** Updates were given on new Draft Proposals and Modification Proposals:

- DP151 ‘Amending Payment Terms for User CIO Invoices’
- DP152 ‘Consumption on Smart Polyphase Electricity Meters’
- DP154 ‘CH Returns SLA Amendment’
- DP155 ‘Communications Hub Re-Flash’

Updates were given on Draft Proposals and Modification Proposals as previously requested by SSC due to the potential impacts on security:

- MP104 ‘Security Improvements’
- MP105 ‘Sending SR11.2 to Devices in Suspended State’
- MP107 ‘SMETS1 Validation of SRV 6.15.1’
- MP109 ‘ADT and Exit Quarantine file delivery mechanism’
- MP128 ‘Gas Network Operators SMKI Requirements’
- MP144 ‘Charging of Random Sample Privacy Assessments’

20. **Quarterly Standards Review:** The SECAS Security Expert presented the latest Quarterly Standards Review. **(AMBER)**

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

Next Meeting: Wednesday 10 March 2021