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) 124_2605

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);
- Set the Compliance Status for one Security Self-Assessment (SSA);
- Approved one Security Self-Assessment Remediation Plan and Director's Letter; and
- Noted one Second User System notification.

The SSC also discussed the following items:

Matters Arising

- The SSC noted an update regarding a Shared Resource Provider (SRP). **(RED)**
- The SSC noted an update regarding off-the-shelf packages. **(AMBER)**
- The SSC noted a response from the Technical Specification Issue Resolution Subgroup (TSIRS) to an SSC request. **(RED)**

Agenda Items

7. **SCF Updates:** The User CIO Representative presented proposed updates to the Security Controls Framework (SCF) and the SSC considered further updates to the SCF. **(AMBER)**

9. **CPA Monitoring:** The SSC was presented with an update on the early expiry of Commercial Product Assurance (CPA) Certificates and Supplier issues updating to compliant Firmware Versions. The SSC was also presented with the latest Pre-Payment (PPM) Report. **(RED)**

10. **Anomaly Detection Report:** The DCC presented the latest Anomaly Detection Report and the SSC provided feedback to the DCC. **(RED)**

11. **Digital Signatures and IKI File Signing:** The SSC Chair and the TABASC Chair presented a proposed Draft Problem Statement regarding Digital Signatures and Infrastructure Key Infrastructure (IKI) File Signing and the SSC agreed to submit the proposed Draft Problem Statement to the SEC Panel. **(GREEN)**

12. **CPA Industry Days:** The SSC Chair presented an update on a response from NCSC explaining their concerns about a Use Case for Device Triage and the outcome of a meeting with NCSC on Tuesday 25 May 2021. The SSC noted the update and agreed that the NCSC concerns about the Use Case should be shared with attendees of the SSC Industry Days. **(AMBER)**

13. **SMETS1 Update:** The SSC noted DCC updates regarding the different aspects of SMETS1 enrolment including Initial Operating Capability (IOC)/Middle Operating Capability (MOC) Morrison Data Services (MDS) remediations; active and monthly dormant Migration process; CIO report updates; and Device Model Combination Testing (DMCT) Tranches for approval. **(RED)**

14. **Post-Commissioning Report:** The SSC noted the latest Post-Commissioning Report for April 2021 and provided feedback on the Post-Commissioning Report for the DCC. **(RED)**

15. **CSS Anomaly Detection Proposals:** The DCC presented its proposals for Anomaly Detection regarding the Central Switching Service (CSS) and the SSC provided recommendations to the DCC. **(RED)**

16. **BEIS Smart Meter Cyber Incident Exercise – Lessons:** BEIS and Contextis presented the lessons learned from the BEIS Smart Meter Cyber Incident Exercise and the SSC provided feedback. **(RED)**

17. **New Draft Proposals and Modification Proposals Update:** Updates were given on new Draft Proposals and Modification Proposals:
    - DP162 'SEC changes required to deliver MHHS'
    - DP164 'November 2021 SEC Release supporting changes'

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

    - MP104 'Security Improvements'
    - MP107 'SMETS1 Validation of SRV 6.15.1'
    - MP109 'ADT and Exit Quarantine file delivery mechanism'
    - MP113 'Unintended Data Disclosure when using SR8.2'
    - MP128 'Gas Network Operators SMKI Requirements'
    - MP144 'Charging of Random Sample Privacy Assessments'

18. **MP125 'Correcting Device Information ESME Variant, Device Model and Device Manufacturer':** SECAS presented an update on the business requirements for MP125 'Correcting Device Information ESME Variant, Device Model and Device Manufacturer' and queried whether the SSC would seek a risk assessment to be conducted after the Refinement Consultation or if the SSC would like the risk assessment to be started earlier. SSC Members provided feedback on potential issues for SECAS to investigate.

19. **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 9 June 2021