This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world, there is no limit on disclosure. Information may be shared without restriction subject to copyright.

Headlines of the Security Sub-Committee (SSC) 216_2805

The SSC reviews the outcome for Users' and DCC 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 the security implications of proposed changes 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 two Full User Security Assessments (FUSA), one Verification User Security Assessment (VUSA), one Security Self-Assessment (SSA), and approved one Remediation Plan and Director's Letter.

The SSC discussed the following items:

Matters Arising

- SSC Members were notified of a webinar hosted by Ofgem, on its decision on Governance of the Data Sharing Infrastructure.
- SSC Members were invited to attend a SEC Party Engagement Day on 1 July 2025, which will include interactive workshops, talks from industry experts and networking with industry colleagues.
- The SSC noted that the updated SSC Terms of Reference have been approved by the SEC Panel.

Agenda Items

1a. User SCF and Agreed Interpretations: SECAS presented three draft documents which had been updated in line with SSC feedback. The SSC **APPROVED** the User Security Controls Framework (SCF) and Agreed Interpretations for publication, subject to further feedback being implemented. **(RED)**

2. **DCC CIO Assessments, Forward Look and Remediations:** DCC CIO presented observations on three DCC Assessments and SSC set a compliance status. The DCC Forward Look and Remediations were presented, which the SSC **NOTED**. **(RED)**
4. **Anomaly Detection Report:** The DCC presented its six-month rolling anomaly detection report, including updated volume and rate observations from the previous month. The DCC requested to change an ADT Global Threshold to reflect the increased volume of Service Requests experienced, which the SCC **APPROVED**. **(RED)**
5. **Post-Commissioning Report:** The DCC presented the monthly post-commissioning report and gave an overview of PCO failures and Certificate rotation activity. This included an additional breakdown of data per region, which the SSC **NOTED**. **(RED)**
6. **FOC ANSO Re-procurement and HSM Approach – Back-up and Restore Process:** The DCC updated the SSC on the proposed approach for re-procuring the Hosting and Application, Network, Security and Operations (ANSO) Management Service for the SMETS1 Final Operating Capability (FOC) cohort. The proposed Back-up and Restore Process for transferring the HSM contents to a new Service Provider was outlined, and the SSC **AGREED** the proposals.
7. **Ephemeral Key Generation Options on VWP for VWAN:** The DCC presented two options for generating ephemeral keys for Virtual WAN Provider (VWP). The options were analysed and costs were presented, and the SSC **NOTED** there were no security objections for the DCC to proceed with either option. **(AMBER)**
8. **Use Case 005 (Workshop):** The SSC Chair and the DCC gave an overview of the background to Use Case 005, and led a workshop for SSC members. The SSC discussed and provided feedback on the documentation requirements, and requested a further update once the document was refined..
9. **CPA Risk Review:** There were no updates to the CPA Risk Review. **(RED)**
10. **CPA Matters**: The SSC Chair presented an update on CPA Matters including an overview of the SCIRS feedback from its meeting on 19 May 2025, and updated guidance on Device Security Assurance, which the SSC **APPROVED** subject to requested edits. **(RED)**
11. **CPA Scheme Update:** The SSC Chair presented Part 1 of the updated CPA Policies and Procedures, which had been reviewed by the SSC at its meeting on 9 April 2025, and then by SCIRS on 19 May 2025. The document has been updated in line with Committee feedback and discussions with the CPA Scheme Operator, and the SSC **APPROVED** the updated version. **(AMBER)**
12. **FSM Programme Update:** The DCC updated the SSC on the Future Service Management (FSM) go-live timeline, security considerations, and plans for stakeholder engagement. The SSC **NOTED** the update. **(AMBER)**
13. **Future Connectivity North:** The DCC updated the SSC on the progress of the Future Connectivity North (FCN) programme, which had been reviewed by stakeholders including

Sub-Committees and working groups. There had been consultation with DESNZ, and industry consultations on changes to SEC Subsidiary Documents. Next steps for the extension and scaling of the programme were explained, which the SSC **NOTED** and had no security objections. **(AMBER-STRICT)**

14. **ECS Report:** The DCC presented the April 2025 activity report for Elective Communications Services (ECS), which the SSC **NOTED**. **(RED)**
15. **Modifications Update:** SECAS presented an update on the ongoing modification proposals, and one new Modification Proposal which the SSC noted interest in **(CLEAR)**:

    MP291 'DNO Alerts to Suppliers' – Currently, Suppliers utilise Data, Events and Alerts received from Smart Metering Systems (SMS) on consumers' premises to determine whether the meter has been tampered with or to evaluate the meter for energy theft. Suppliers have obligations under the Standard Licensing Conditions (SLC) and the Retail Energy Code (REC), and are also required to act on Anomalous Events and Alerts under SEC Section G13.5 – G13.6.

    The Proposer would like Suppliers to have visibility of a number of Alerts that would provide the level of granularity needed to make the modelling mechanisms as accurate as possible. In turn, this would allow for more investigations into meter tampering / Energy theft to be carried out.

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

Next Meeting: Wednesday 11 June 2025