

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.

Security Sub-Committee (SSC) 78_2205

22 May 2019 10:00 – 16:00

Gemserv Office, 8 Fenchurch Place, London, EC3M 4AJ

SSC_78_2205 – Meeting Headlines

Matters Arising

Updates were noted on the following Matters Arising;

- The SSC **NOTED** an update in relation to a previous reported non-compliance with Small Supplier 'AP'. (**RED**)

Items for Decision/Discussion

2. Previous Meeting Minutes and Actions Outstanding

The SSC noted that no comments were received for the Draft Minutes and Confidential Minutes from the SSC meeting held on Wednesday 8 May 2019, and the SSC **APPROVED** the Draft Minutes and the Confidential Draft Minutes as written.

All outstanding actions were marked as complete or on target for completion, with several updates provided under separate meeting agenda items.

3. Full User Security Assessment – Other User 'N' (**RED**)

The SSC considered Other User 'N's Full User Security Assessment. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** the Assurance Status for Other User 'N'.

4. Full User Security Assessment – Shared Resource Provider 'D' (**RED**)

The SSC considered Shared Resource Provider 'D's Full User Security Assessment. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** the Assurance Status for Shared Resource Provider 'D'.

5. Verification User Security Assessment – Small Supplier ‘C’ (RED)

The SSC considered Small Supplier ‘C’s Verification User Security Assessment. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** the Compliance Status for Small Supplier ‘C’.

6. Verification User Security Assessment – Small Supplier ‘AD’ (RED)

The SSC considered Small Supplier ‘AD’s Verification User Security Assessment. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** the Compliance Status for Small Supplier ‘AD’.

7. Verification User Security Assessment – Small Supplier ‘AC’ (RED)

The SSC considered Small Supplier ‘AC’s Verification User Security Assessment. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** the Compliance Status for Small Supplier ‘AC’.

8. Director’s Letter – Small Supplier ‘CC’ (RED)

The SSC considered Small Supplier ‘CC’s Director’s Letter. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **APPROVED** Small Supplier ‘AC’s Director’s Letter.

9. Director’s Letter – Other User ‘L’ SRP (RED)

The SSC considered Other User ‘L’s Director’s Letter. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **APPROVED** Other User ‘L’s Director’s Letter.

10. SMETS1 Appropriate Standards (AMBER)

The SSC Chair noted that the paper circulated at the previous meeting was redacted and shared with members to facilitate the sharing amongst colleagues on a need to know basis.

The SSC:

- **CONSIDERED** the previous proposed recommendations and undertook to provide feedback regarding appetite for independent testing of SMETS1 Devices; and
- **AGREED** that further discussion should be held at the next SSC meeting on 12 June 2019 to consider the options for a testing approach.

The Agenda Item has been marked as **AMBER** and therefore recorded in the Confidential Minutes.

11. Post Commissioning report (AMBER)

The SSC Chair noted that the last Post Commissioning Report received was on 5 April 2019 for the period ending February 2019 and noted that the DCC had experienced problems in providing the data however, the SSC requested the next Post-Commissioning Report as soon as practically possible.

The SSC **NOTED** the update and **AGREED** that a further discussion should be held at the next SSC meeting on 12 June 2019 to discuss findings of the report in depth.

The Agenda Item has been marked as **AMBER** and therefore recorded in the Confidential Minutes.

12. SOC2 Final Report (RED)

The DCC confirmed the SOC2 Final Report has been reviewed to specifically map and analyse the findings. The DCC presented the breakdown of findings within the SOC2 Report via an excel collated spreadsheet. The SSC **AGREED** for a further update to be provided at the SSC meeting on Wednesday 26 June 2019.

The SSC **NOTED** the update. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

13. Mitigation of Type 1 and Type 2 Devices – Internet Connected Devices (AMBER)

The SSC were provided with an update on the progress of the SSC Project relating to the mitigation of Internet-Connected Device Risks. The SSC noted the plan on the page alongside a research paper which was previously circulated to SSC members via Egress.

The SSC **NOTED** the update and **AGREED** to review the papers previously circulated ready for discussion and approval at a future SSC meeting.

The Agenda Item has been marked as **AMBER** and therefore recorded in the Confidential Minutes.

14. Quarterly Work Package (RED)

SECAS presented the SSC Quarterly Work Package and clarified the activities and associated costs for the SECAS core team and project resource for the period of July – September 2019.

The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **NOTED** the update and **DEFERRED** a decision to recommend the work package for SECCo Board approval.

15. SEC and NIS / CAF Alignment (AMBER)

The SSC were provided with a proposal by the SSC Chair to align and make changes to the Agreed Interpretations and Security Controls Framework (SCF) Part 2 to demonstrate how the requirements of the Network Information Systems (NIS) Directive and its associated Cyber Assessment Framework (CAF) align with the SEC Security Requirements.

The SSC **NOTED** the update. The Agenda Item has been marked as **AMBER** and therefore recorded in the Confidential Minutes.

16. CPL Device Removal (AMBER)

The SSC were provided with an update on the scheduled removal of Devices with specific firmware versions from the CPL in which, the SSC **AGREED** their original 'minded to' position whilst reviewing the SEC obligations in SEC Appendix Z Section 6.2.

The SSC **NOTED** the update. The Agenda Item has been marked as **AMBER** and therefore recorded in the Confidential Minutes.

17. CPA Matters (RED)

Communications Hub CPA Conditions

The SSC **NOTED** the update in relation to a Communications Hub with Commercial Product Assurance (CPA) Conditional Certification. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

Optical Port for Triage

The SSC **NOTED** the update received from BEIS in relation to a Device having an Optical Port. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

18. Standing Agenda Items (RED)

The SSC were provided with updates on the following standing agenda items:

- CPA monitoring of 'Conditional' CPA Certificates (**RED**);
- Anomaly Detection Update (**RED**);
- Shared Resource Notifications (**GREEN**); and
- Security Incident and Vulnerabilities. (**RED**)

19. Any Other Business (AOB) (RED)

One confidential item of business was raised which has been recorded in the Confidential Minutes.

No additional items of business were raised, and the SSC Chair closed the meeting.

Next Meeting: 12 June 2019