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) Meeting Headlines

27 February 2019, 10:00 – 16:00, Gemserv Office, 8 Fenchurch Place, London, EC3M 4AJ

SSC_72_2702 – SSC Meeting Headlines

1. Matters Arising

Updates were noted on the following Matters Arising;

- The SSC **NOTED** the consultancy assignment for 'Mitigating Security Risks from Internet-Connected Devices. **(RED)**

- An update was provided whereby the Working Group met on 26 February 2019 in order to discuss and review the risks for SECMP0037 'Pairing Local PPMIDS' and SECMP0038 'Sending Commands via PPMIDS'. The outcome of the meeting advised for the SSC to review the Working Group's Risk Assessment at a future SSC meeting.

- The SSC **NOTED** the request from the SEC Panel to consider a Supplier of Last Resort (SoLR) Scenario. **(RED)**

- An update was provided regarding changes to the SEC taking place on 28 February 2019 in order to implement SECMP0057 'Users to notify SSC of a Second or Subsequent User System' and SECMP0059 'Amendments to SEC Security Assessments for Non-Domestic Suppliers and Other Users'.

- The SSC **NOTED** the update in relation to the SEC changes currently due to take place on 11 March 2019 to transition responsibility to the SSC for CPA and Security Characteristics maintenance.

- The SSC **NOTED that** comments on the SMETS1 Device Assurance Guidance paper produced by PA Consulting are due by close of play today 27 February 2019.

2. 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, 13 February 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 ‘L’ (RED)

The SSC considered Other User ‘L’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 ‘L’.

4. Verification User Security Assessment – Small Supplier ‘AA’ (RED)

The SSC considered Small Supplier ‘AA’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 ‘AA’.

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

The SSC considered Small Supplier ‘AE’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 ‘AE’.

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

The SSC considered Small Supplier ‘B’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 ‘B’.

7. Security Self-Assessment – Other User ‘I’ (RED)

The SSC considered Other User ‘I’’s Security Self-Assessment. The agenda item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **NOTED** the Self-Assessment and the User CIO report for Other User ‘I’.

8. Directors Letter – Small Supplier ‘N’ (RED)

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

The SSC **APPROVED** the Director’s Letter for Small Supplier ‘N’.

9. Notification of a Second or Subsequent User System – Large Supplier ‘B’ (RED)

The SSC considered the formal notification received by Large Supplier ‘B’ intending to employ a second user system.

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

The SSC **NOTED** the report of a second user system.

10. Self-Assessment Changes for Security Controls Framework (SCF) (GREEN)

The SSC were provided with an update regarding the Self-Assessment changes to the Security Controls Framework which have been endorsed by the User CIO, this work has already been completed and implemented in the latest version (version 1.2) of the Validation Workbook.

The SSC **NOTED** the update.

11. 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 April – June 2019.

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

The SSC **NOTED** the update and **RECOMMENDED** the work package for SECCo Board approval.

12. SMETS1 Update (AMBER)

The DCC provided an update previously presented to the SMKI PMA which consisted of an overview of, and background to, the SMETS2 approach for the segmentation of SMKI certificates. Two options were proposed by the DCC noting that the one that is in the current design for IOC will be complicated for Suppliers to implement. SSC members were asked to consider the business impact of both options and the outcome will be considered at SSC on 13 March.

The DCC presented four options to check separation of XML and SMKI keys for SMETS1 with the advantages and disadvantages for each, and the DCC's proposed conclusion.

The DCC also provided an update on proposed changes to Section G, specifically G2.44 and G2.45 whilst noting the current issues with the wording and the proposed alterations for each Section.

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

The SSC **NOTED** the update.

13. SMETS1 Draft CIO Report (RED)

PA Consulting provided an update on the SMETS1 Draft CIO Report which noted that four stages of the CIO assessment have been completed and clarified the risk assessments undertaken, the Data Service Provider systems report, the DCO controls report and the S1SP systems report whilst also highlighting the fundamental key findings within the reports.

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

The SSC **NOTED** the update.

14. SOC2 Draft Report (RED)

The SSC were provided with an update on the Report Status within the SOC2 Draft Report, specifically highlighting content regarding management assertions, a description of the system, information provided by the Service Auditor and other information provided by Service organisations.

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

The SSC **NOTED** the update.

15. DCC Go Live On-Boarding Process – Pre-Live Preparation (AMBER)

The SSC were informed of the background and current process within the DCC Go Live On-Boarding Process whilst outlining a proposed improved and more efficient solution in relation to the DCC Go-Live On-Boarding Process. It was advised that Utiligroup have been working with their customers to support them through the DCC On-Boarding process for SEC Parties to become a DCC User and that, they currently await a two-step approval notification from the SECAS Security Team to confirm the assurance status that has been set.

The potential process improvements were highlighted whilst the SSC considered the risk to the overall programme and implementation approach of Pre-Live Preparation.

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

The SSC **NOTED** the update.

16. CPA Conditional Certificates – Risk Based Decision (AMBER)

The SSC were provided with an update on a previous action which was raised to provide an options paper for the SSC on communications and handling of an SSC decision on whether Devices that have not been remediated should be removed from the CPL.

The SSC Chair provided a proposed 'minded to' position for SSC to consider prior to SSC becoming responsible for CPA matters in an update to the SEC scheduled to be implemented on 11 March 2019.

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

The SSC **NOTED** the update.

17. CPA Certificates and Bulk Ordering Devices (AMBER)

The SSC considered the need to make a risk-based decision on whether to remove devices that have not been remediated by 25th June from the CPL. The National Cyber Security Centre (NCSC) were asked to assist the SSC decision-making by articulating and calibrating Security risks arising from MISRA violations.

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

The SSC **NOTED** the update.

18. Issues arising from the Use of SPOTI (RED)

The SSC provided clarification regarding issues arising from the Use of SMKI Portal via The Internet (SPOTI) which was previously presented to the SMKI PMA on 19 February 2019.

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

The SSC **NOTED** the update and **AGREED** to seek NCSC advice and legal advice on changes to the SEC.

19. 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;
- Shared Resource Notifications; and
- Security Incident and Vulnerabilities.

20. Any Other Business (AOB) (RED)

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

Next Meeting: 13 March 2019