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) 80_2606

26 June 2019 10:00 – 15:45

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

SSC_80_2606 – Meeting Headlines

Matters Arising

Updates were noted on the following Matters Arising;

- The SSC **NOTED** the update in relation the CPA Smart Metering Industry Day which took place on Tuesday 25 June 2019 in which, Supplier Representatives discussed the current requirement for 'resetting the Home Area Network (HAN)'. It was agreed that BEIS would analyse the feedback and provide an updated paper to the SSC and, agreed to consider further use cases submitted by Suppliers, Meter Manufacturers and others for Triage to establish solutions for implementation. **(GREEN)**

- The SSC **NOTED** an update in relation to NCSC's Smart Metering Information Exchange (SMIE) which is due to take place on Monday 1 July 2019 and will cover the work being commissioned in relation to Mitigating Security Risks from Internet-Connected Devices. **(GREEN)**

- The SSC **NOTED** an update in relation to Small Supplier 'H' regarding their submitted Remediation Plan Cover Letter. **(RED)**

- The SSC **NOTED** an update in relation to Small Supplier 'BP' regarding previous submission of their Director's Letter and Assurance Status set. **(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 Draft Minutes from the SSC meeting held on Wednesday 12 June 2019, and the SSC **APPROVED** the Draft Minutes and 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 – Small Supplier 'CN' (RED)

The SSC considered Small Supplier 'CN'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 Small Supplier 'CN'.

4. Verification User Security Assessment – Small Supplier 'N' (RED)

The SSC considered Small Supplier 'N'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 'N'.

5. Verification User Security Assessment – Small Supplier 'A' (RED)

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

The SSC **AGREED** to defer setting the Compliance Status for Small Supplier 'A' until the SSC meeting on Wednesday 10 July 2019.

6. Security Self-Assessment – Network Operator 'E' (RED)

The SSC considered Network Operator 'E's Security Self-Assessment. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **NOTED** the Self-Assessment for Network Operator 'E'.

7. Security Self-Assessment – Network Operator 'C' (RED)

The SSC considered Network Operator 'C's Security Self-Assessment. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **NOTED** the Self-Assessment for Network Operator 'C'.

8. Remediation Plans (RED)

Expected Remediation Plans were not made available therefore were deferred to the next SSC meeting on Wednesday 10 July 2019.

9. SMETS1 Appropriate Standards (AMBER)

The SSC Chair provided an update highlighting the sections of the Security Controls Framework (SCF) Part 2 which have been amended to clarify what the User CIO would be looking for in a User Security Assessment. In addition, clarification was provided that SMETS1 was included in SEC Obligations and this was reflected in a supporting paper distributed to SSC Members.

The SSC **NOTED** the update and **APPROVED** the publication of the SCF Part 2, pending modifications as requested by SSC Members.

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

10. CPA – Security Characteristics v1.3 (GREEN)

The SSC Members were provided with the latest draft of the CPA Security Characteristics v1.3 for approval in line with the timetable agreed by SSC at its meeting on Wednesday 24 April 2019.

The SSC:

- **NOTED** the update;
- **APPROVED** the CPA Security Characteristics v1.3;
- **APPROVED** the Implementation timescale of three months to enable the SC v1.3 to be a mandatory requirement for any Combined Business Questionnaires (CBQs) accepted by NCSC on or after Thursday 26 September 2019; and
- **APPROVED** the publication of the SSC decisions above to the SEC Website on Thursday 27 June 2019.

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

11. SMETS1 – Live Services Criteria (RED)

The SSC were provided with a three-part update, firstly seeking comments from the initial Risk Assessment that was raised at the previous SSC meeting on Wednesday 12 June 2019 which outlined the status of controls for Initial Operating Capability (IOC) and the design differences between CIO audits and the Residual Risks. The SSC then considered the recommendation to the

Panel for Live Services Criteria for the first entry of SMETS1 Devices onto the Eligible Products Combination List (EPCL).

The second update highlighted findings within the Security Testing Traceability Matrix, noting that the DCC Security have assessed whether each SMETS1 IOC Service Provider (SP) has implemented mandated security controls. The DCC also assessed whether an appropriate and proportionate level of security testing of these controls have been completed successfully.

The third update was regarding the DCC's Competent Independent Organisation (CIO) report in and the subsequent Management Response.

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

The SSC **NOTED** the update.

12. Triage Guidance – Resetting the HAN for Device Re-Use (AMBER)

There was a SSC paper that summarised the background and proposed solution and the SSC were asked to approve issuing guidance for energy Suppliers and Device manufacturers on re-setting the Home Area Network (HAN) for Devices where installation has been aborted for a variety of reasons and the Devices would otherwise be scrapped.

An agreed method has been developed in a series of Working Groups and has been refined by the BEIS led Technical Specification Issue Resolution Sub-Group (TSIRS) and has been approved by NCSC and BEIS.

Following the CPA Industry day on 25 June 2019, the SSC **AGREED** to defer the decision until the next SSC Meeting on Wednesday 10 July 2019 to take account of amendments by BEIS.

13. Standards Guidance (AMBER)

The SSC were presented with a paper which was produced in order to provide a guideline on vulnerability disclosure and handling based on ISO/IEC 29147:2018 and ISO/IEC (DIS) 30111:2018. This was in response to SSC's recommendation for a guidance document to be created based on updated versions of ISO/IEC 29147:2014 and ISO/IEC 30111:2013 to address the need for structured reporting, disclosure and handling of Material Security Vulnerabilities (MSVs).

The SSC **NOTED** the update and **AGREED** to defer the decision on the recommendations until the next SSC Meeting on Wednesday 10 July 2019, which have been marked as **AMBER** and therefore recorded in the Confidential Minutes.

14. SOC2 Report (RED)

The DCC confirmed the SOC2 Final Report has been reviewed to specifically map and analyse the findings. The SSC were presented with a further update in relation to the SOC2 Auditor which took place in 2018/19, along with the Post-Audit Remediation Progress and Material Findings and Conclusions.

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

15. Notification of a Second and Subsequent User System – Large Supplier 'E' (RED)

Following the implementation of SEC Modification 'SECMP0057: 'Users to notify SSC of a second or subsequent User System' on Thursday 28 February 2019, the SSC considers notifications to the SSC of Users intending to employ a second User System.

The SSC **NOTED** the Notification of a Second or Subsequent User System submitted by Large Supplier 'E'.

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

16. SEC Modification Proposals

The SSC were provided with an update in relation to the new Draft Proposals raised since March 2019 and the Draft Proposals that have converted to Modification Proposals in the last month.

The SSC **NOTED** the update and provided a view on the Draft Proposals that could be security-impacting.

17. CPA Monitoring (AMBER)

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 **AMBER** and therefore recorded in the Draft Minutes. The SSC **NOTED** the update in relation to certain meters upgrade statuses. The Agenda Item was marked as **AMBER** and therefore recorded in the Draft Minutes.

Withdrawn Certificates

The SSC **NOTED** the update in relation to Withdrawn CPA Certification Statuses and the Volumes of pre-v.49 Versions. The Agenda Item was marked as **AMBER** and therefore recorded in the Draft Minutes.

18. Standing Agenda Items (RED)

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

- Anomaly Detection Update **(RED)**;
- Shared Resource Notifications **(AMBER)**; and
- Security Incident and Vulnerabilities. **(RED)**

19. Any Other Business (AOB) (RED)

Two additional items of other business were raised and are classified **RED** therefore have been recorded in the Confidential Minutes.

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

Next Meeting: Wednesday 10 July 2019