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) 75_1004

10 April 2019 10:00 – 16:00

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

SSC_75_1004 – Meeting Headlines

Matters Arising

Updates were noted on the following Matters Arising;

- The SSC were informed that two papers were drafted and circulated to Panel members on Friday 5 April 2019 in relation to User Security Assessments highlighting any non-compliances during the Assessment stages. It was confirmed that no Events of Default had been recommended, excluding one which was currently under discussion with the SSC. A second paper was also circulated to Panel members highlighting the process for Security Characteristic (SC) Modifications.

- The SSC **NOTED** the update in relation to a Smart Metering Information Exchange (SMIE) meeting and a subsequent proposal for Chairmanship of the meetings. (**AMBER**)

- The SSC were provided with an update in relation to mitigating Security risks from internet-connected devices on which the Gemserv team had previously presented to the SSC. The SSC Chair confirmed a research paper was being drafted and would seek to focus on the core vulnerabilities and mitigating risks as agreed during a teleconference with Gemserv Representatives. (**AMBER**)

Items for Decision/Discussion

2. Previous Meeting Minutes and Actions Outstanding

The SSC noted that no comments were received for the Draft Minutes, however one set of comments was received from a Large Supplier Representative for the Confidential Minutes from the SSC meeting held on Wednesday, 27 March 2019. The SSC **APPROVED** the Draft Minutes and Confidential Minutes as modified.

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

3. Verification User Security Assessment – Small Supplier 'Z' (RED)

The SSC considered Small Supplier 'Z'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 'Z'.

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

The SSC considered Small Supplier 'AN'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 'AN'.

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

The SSC considered Small Supplier 'AM'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 'AM'.

6. Director's Letter – Small Supplier 'BP' (RED)

The SSC considered Small Supplier 'BP'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 'BP'.

7. Director's Letter – Large Supplier 'J' (RED)

The SSC considered Large Supplier 'J'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 Large Supplier 'J'.

8. Outstanding Actica Work (RED)

CPA Gap Analysis SEC VS CPA Assurance

The SSC were provided with an update in relation to the additional work commissioned from Actica in May 2018. Actica previously conducted a partial risk analysis of DCC Release 2, however, the SSC had since requested that work should include Dual Band Comms Hubs. Actica also provided a Gap Analysis to compare security assurance provided in the SEC versus assurance provided via the CPA

Scheme in order to identify whether additional CPA or SEC requirements are needed. The SSC **NOTED** the contents regarding the security matters relating to Dual Band Comms Hubs and the CPA Analysis which had been split between a Gap Analysis and Residual Risks.

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

9. Security Controls Framework (GREEN)

An update was provided to the SSC specifically, proposed changes to the guidance for what constitutes a SMETS1 'Appropriate Standard' for inclusion in the Agreed Interpretations, additional steps as part of the DCC On-Boarding Process and amendments to the Assessment type and frequency for Supplier Parties and Other Users.

The SSC **NOTED** the update and **AGREED** the amendments made to the Security Controls Framework (SCF) and Agreed Interpretations (AIs). The Agenda Item has been marked as **GREEN** and therefore recorded in the Draft Minutes.

10. Timing of Third and Subsequent User Assessments (GREEN)

An update was provided in order to clarify the interpretations relating to the timing of the Third and Subsequent Security Assessments within the SCF. Assurance was provided by SECAS that Users will be assessed within a consistent timeframe and provide clarity on the Third Year Assessment scheduling.

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

11. SECMP0013 Meter Triage (GREEN)

The SSC were provided with an update in relation to the Business Requirements previously discussed for SECMP0013 'Smart meter device diagnostics and triage'. The TABASC Chair confirmed that a use case has been developed which has been sent to the National Cyber Security Centre (NCSC) for review. This will in turn be forwarded to the Technical Specification Issue Resolution Sub Group (TSIRS) to confirm the viability from a technical point of view before coming back to the SSC.

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

12. Network Information Systems Directive (NISD) (RED)

Gemserv Representatives provided an overview of the NISD, specifically focusing on the approach, findings and recommendations for the SSC. The five considerations detailed within the comparative

analysis were noted in addition to the methodology of the Cyber Assessment Framework (CAF) and how this compared to the SCF.

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

13. SOC2 Final Report (RED)

The DCC confirmed the SOC2 Final Report had now been received and was currently being reviewed in order to specifically map and break down the findings and management responses before bringing to the SSC at the next meeting on 24 April 2019.

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

14. SMETS1 Update (RED)

The SSC were provided with an update in relation to the Security Architecture V1.4 and XML Certificate Recovery. It was confirmed that the SSC comments on the SMETS1 Security Architecture V1.4 had been provided to DCC.

The SSC also **NOTED** the update regarding XML Certificate Recovery whereby the SSC previously requested the DCC to explain the applicability of SEC Appendix L SMKI Recovery Procedures to SMETS1. It was confirmed this update would also be presented to the SMKI PMA on 16 April 2019.

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

15. DCC Post Commissioning Report (RED)

The SSC were provided with an update in relation to the updated Post Commissioning Report which provides information on the number of relevant SMETS2 Devices where the Responsible Supplier or DCC has failed to complete its Post-Commissioning obligations in accordance with Section 5 of Appendix AC of the SEC.

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

16. CPA Matters

<u>Security Characteristics Timing of Implementation</u>

The SSC **NOTED** the update in relation to the Security Characteristics document V1.3 which is being finalised by the NCSC following comments from industry.

The SSC has consulted with the relevant trade bodies on an implementation date for V1.3 of the Security Characteristics and is awaiting a response.

CPA Conditions relating to a Communications Hub

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

ESME Optical Report

The SSC **NOTED** the update in relation to the ESME Optical Port. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

CPA Qualification

The SSC **NOTED** the update regarding the extension of a Device Manufacturer's CPA Certification. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

17. Rogue Devices being Joined/Un-Joined (AMBER)

Due to time constraints, this agenda item was deferred to the next SSC meeting scheduled for Wednesday 24 April 2019.

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;
- Shared Resource Notifications; and
- Security Incident and Vulnerabilities. **(RED)**

19. Any Other Business (AOB)

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

Next Meeting: 24 April 2019