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

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

SSC_70_2301 – SSC Meeting Headlines

1. Matters Arising

Updates were noted on the following Matters Arising;

- SSC Members were informed there was a change in the DCC Chief Information Security Officer (CISO) whereby, Marc Avery would be leaving at the end of March 2019 with the interim (Rob Newby) in place for a handover.

- The SSC **NOTED** the update in relation to the ITT update for 'Mitigating Security risks from internet-connected devices' (**AMBER**)

- The SSC **NOTED** feedback had been received from the first Ofgem Central Switching Service (CSS) Transitional Security Governance Group (TSGG) whereby, it was agreed that anomaly detection was required for the CSS. (**AMBER**)

- The SSC were informed that Small Supplier 'BA' notified SECAS around the change in their Shared Resource Provider. (**RED**)

- The SSC **NOTED** the conclusion of the BEIS consultation on SMETS1 for CPA/CPL published on 20 January 2019 and is now laid before parliament.

- The SSC were informed that a joint SSC/ SEC Mod Working Group was scheduled for Tuesday 26 February to explore alternative options for 'SECMOD 0038 'Sending Commands via PPMIDS'.

- The SSC **NOTED** that the NCSC CPA Industry Day had been confirmed for 28 February 2019 which is being held externally.

2. Minutes and Actions Outstanding

The SCC noted that no comments were received for the Draft Minutes from the SSC meeting held on Wednesday, 9 January 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 – Small Supplier 'BP' (RED)

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

The SSC **AGREED** an Assurance status for Small Supplier 'BP'.

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

The SSC considered Small Supplier 'E'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 'E'.

5. Verification User Security Assessment – Large Supplier 'J' (RED)

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

6. Directors Letter – Small Supplier 'Z' (RED)

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

7. Directors Letter – Small Supplier 'BS' (RED)

The SSC considered Small Supplier 'BS'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 'BS'.

8. SEC Change Status Report

The SECAS Change Team provided an update to the SSC on 'SECMP0060 'Amend requirements to remove 'Pending' devices from SMI'.

The SSC **NOTED** the update and **AGREED** the term 'Pending' on devices should be configurable whilst increasing the period of time a device can remain 'pending' to 36 months but returning to 12 months as soon as practicable.

The SSC **NOTED** the proposed solution for SECMP0046 'Allow DNOs to control Electric Vehicles chargers connected to Smart Meter infrastructure'.

The SSC **AGREED** HAN Auxiliary Load Control Switch (HCALCS) is the most appropriate, secure solution to temporarily disconnect EV Charges from supply but the ability to issue these commands will require significant SEC changes which should be reviewed as part of the SEC Modification.

The SSC informed the Change Team that they were interested in the modification and would like to provide assistance in setting a secure process.

9. Large Supplier 'E' Remediation Plan (RED)

The SSC **NOTED** Large Supplier 'E's Remediation plan and **AGREED** an updated plan to be submitted in February 2019.

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

10. SSC Risk Assessment (RED)

The SSC were provided with an update around the use of SMKI Portal over the internet (SPOTI) and the risk assessment undertaken by the SMKI PMA.

The SSC **NOTED** the SPOTI risk assessment, its findings and the summary before agreeing to investigate the options to mitigate the SPOTI risks.

The SSC **AGREED** for an update to be provided at a future meeting.

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

11. SMETS1 Update (RED)

A SMETS1 update was provided to the SSC by the DCC.

The SSC acknowledged the SMETS1 Security Architecture Document v1.3 and associated risks which were shared with the SSC on 18 January 2019.

The SSC **AGREED** to review the SMETS1 Security Architecture Document v1.3 and provide comments to the DCC by Thursday 31 January 2019.

This agenda item is marked as **(RED)** and therefore recorded in the Confidential Minutes.

12. ADT Workshop Update (AMBER)

Following the Anomaly Detection Workshop (ADT) which was held on 16 October 2018, the SSC were provided with an update from the DCC.

The SSC **AGREED** to review the business requirements document being prepared by the DCC.

This agenda item is marked as **(AMBER)** and therefore recorded in the Confidential Minutes.

13. Conditional Certificate CPA Scenarios for EU Exit (RED)

An update was provided by the SSC Chair on the scenarios associated with the potential expiry of Conditional 'CPA' certificates.

The SSC **NOTED** the update and highlighted concerns on firmware that would fail to be upgraded by 7 February 2019.

This agenda item is marked as **(RED)** and therefore recorded in the Confidential Minutes.

14. Standing Agenda Items (RED)

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

- CPA monitoring of 'conditional' CPA Certificates;
- Anomaly Detection Update;
- Shared Resource Notifications; and
- Security Incident and Vulnerabilities.

15. Any Other Business (AOB) (RED)

Five additional items of business were raised under AOB and marked as **RED** and therefore recorded in the Confidential Minutes.

Next Meeting: 13 February 2019