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

28 November 2018, 10:00 – 16:00, Gemserv Office, 8 Fenchurch Place, London, EC3M 4AJ

SSC_67_2811 – SSC Meeting Headlines

1. Matters Arising

Updates were noted on the following Matters Arising;

- Extra Energy & Spark Energy ceased trading; **(GREEN)**
  The DCC Representative provided an update on the Supplier of Last Resort (SoLR) activities for Extra Energy and Spark Energy.

- Duty to notify & to be notified on churn;
  The SSC were asked to review SEC obligations *G3.18 to G3.20* to notify and to be notified of material security vulnerabilities where suppliers are inheriting a SMETS2 meter and can still operate SMETS2 meters inherited on churn as long as they are taking reasonable steps to agree a contract with a MAP or meter manufacturer to meet the obligations in G3.20. The SSC agreed to clarify this in the Security Controls Framework (SCF) and via the December SECAS Newsletter.

- The BEIS Representative provided an update on Certified Product Assurance (CPA) developments including; **(GREEN)**
  - the key outputs of the Certified Product Assurance (CPA) Industry Day which took place on 11 October 2018;
  - a requirement for a Supplier to sponsor a meter manufacturer to undertake diagnostics against the proposed CPA Security Characteristics changes that may be used for wider industry; and
  - the BEIS SMETS1 consultation published on 5 November 2018 closes on 3 December 2018 and the SEC Designation will be in March 2019.

- SSC Members reviewed the forward plan for scheduled Security Assessments.

2. Minutes and Actions Outstanding

The SCC noted that no comments were received for the Draft Minutes from the SSC meeting held on Wednesday, 14 November 2018. 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 'BV' (RED)

The SSC considered Small Supplier 'BV'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 'BV'.

4. Verification User Security Assessment - Small Supplier 'D' (RED)

The SSC considered the Small Supplier 'D'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 'D'.

5. Security Controls Framework – Security Self-Assessment Updates (GREEN)

The SSC considered the role of the User CIO as part of Security Self-Assessments and agreed that revised questions should be included in the Self-Assessment declaration form to cover the following risk areas:

- Vulnerability management
- Personnel screening
- Security training
- Anomaly detection thresholds
- Duty to notify and to be notified

The SSC will consider the revised questions at the next SSC meeting on 12 December for inclusion in the Security Controls Framework (SCF).

6. Security Self-Assessment – Large Supplier 'A' (RED)

The Self-Assessment for Large Supplier 'A' was considered by the SSC. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **NOTED** the Self-Assessment for Large Supplier 'A'.

7. Large Supplier 'E' – Remediation Plan (RED)

Progress against the Remediation Plan for Large Supplier 'E' was considered by the SSC. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **NOTED** the contents and **AGREED** the date for the next progress update to be provided.

8. Hypothetical Notification of a Second User System' (RED)

Pending the progress of SEC Modification SECMP0057 'Notification of a second or subsequent User System', the SSC considered the process of notification to the SSC and audit of the User should a User decide to employ any new and/or additional User Systems.

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

The SSC **AGREED** to include guidance regarding notifying a second or subsequent User System in the Security Controls Framework (SCF) for consideration by the SSC at the 12 December meeting.

9. Directors Letter - Small Supplier 'U' (RED)

The SSC considered the Directors Letter provided by Small Supplier 'U'. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **APPROVED** the Directors Letter for Small Supplier 'U'.

10. Directors Letter – Small Supplier 'I' (RED)

The SSC considered the Directors Letter provided by Small Supplier 'I'. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **APPROVED** the Directors Letter for Small Supplier 'I'.

11. Query - Small Supplier 'AI' (RED)

The SSC considered a query from Small Supplier 'AI'. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** there were no security implications arising from the query.

12. SMETS1 Update and BEIS Consultation on SMETS1 (RED)

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

- SMETS1 Consultation
    - LC13 consultation:
        - Issued to SEC parties for consultation on 1 Nov with capability release dates:
        - DCC held a conference call on 13 Nov to provide stakeholders an opportunity to ask questions to inform their final responses.
        - Consultation closed 23 Nov 2018 and responses now being assessed.

- LC13 Plan
    - A revised LC13 project plan was presented
- SMETS1 Ongoing
    - An update was provided on SMETS1 enrolment and adoption for meters
- SMETS1 manufacturer image
    - All firmware to include a manufacturer image
- SMETS1 cryptography key usage
    - Usage of cryptographic keys in the SMETS1 total system.

SMKI certificate segregation

The SSC **AGREED** that Users should have the facility to segregate SMKI Private Keys for SMETS1 as a necessary User-defined control to mitigate risk to supplier device portfolios.

Security Architecture

The DCC presented the key changes to the Security Architecture document.

The SSC **NOTED** the information provided and **AGREED** to review the Appendices slides post meeting.

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

13. ADT Workshop Update (AMBER)

Following the Anomaly Detection Workshop (ADT) which was held on 16 October 2018, the SSC were presented with initial updates at the 14 November 2018 SSC meeting from the DCC to the outstanding actions captured at the workshop and the previous workshop held on 30 May 2018.

Detailed updates have since been provided and were presented by the DCC to the SSC.

The SSC **NOTED** the updates provided to the actions and **AGREED** next steps.

14. SSC Risk Assessment Completion and Likelihoods Definition (AMBER)

The SSC reviewed the amendments made to the SSC Risk Assessment since 25 September 2018.

The SSC discussed the probability percentages assigned to the Likelihood Definitions used in the SSC Risk Assessment and considered the requested examples provided by the Service Provider.

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

15. SEC Modifications Update

SECMP0059

At the SSC meeting on 14 November, the SSC considered legal text for SECMP0059 'Amendments to SEC Security Assessments for Non-Domestic Suppliers and Other Users'. The SSC agreed that

revised legal text for G8.41 c) should be drafted to recognise a clear weighting between domestic and non-domestic meters in terms of a risk profile to trigger a FUSA.

The revised legal drafting has been submitted to the Modification Working Group for review.

The SSC **NOTED** the text and **AGREED** the revised legal text for SECMP0059 G8.41 c) reflected the SSC view.

16. Standing Agenda Items (RED)

The SSC were provided with updates on the following standing agenda items marked as **RED** and therefore recorded in the Confidential Minutes:

- Reporting on 'Conditional' CPA certificates;
- Anomaly Detection Update;
- Shared Resource Notifications; and
- Security Incident and Vulnerabilities.

The SSC **NOTED** the updates.

17. Any Other Business (AOB) (RED)

Three items were raised under AOB and marked as **RED** and therefore recorded in the Confidential Minutes.

Next Meeting: 12 December 2018