

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) 76\_2404

24 April 2019 10:00 – 16:00

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

### SSC\_76\_2404 – Meeting Headlines

#### Matters Arising

Updates were noted on the following Matters Arising;

- The SSC **NOTED** that the Agreed Interpretations V1.7 were published on 15 April 2019 and that the SMKI PMA had suggested to amend the Use of SPOTI to make the appropriate wording clearer regarding the use of SMKI Testing Certificates.
- The SSC **NOTED** that the Security Controls Framework (SCF) V1.16 has not yet been published due to ongoing changes. (**AMBER**)
- The SSC **NOTED** the update regarding Initial Operating Capability (IOC) Live Service Criteria whereby, a letter from BEIS was circulated to Members to explain the requirement for SEC Panel approval supported by sub-committees which will require advice from SSC to the SEC Panel from the SSC meeting on 22 May 2019. (**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 Minutes from the SSC meeting held on Wednesday 10 April 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 ‘CG’ (**RED**)

The SSC considered Small Supplier ‘CG’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 'CG'.

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

The SSC considered Small Supplier 'AL'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 'AL'.

**5. Verification User Security Assessment – Small Supplier 'T' (RED)**

The SSC considered Small Supplier 'T's Verification User Security Assessment. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

The SSC **AGREED** to defer the decision to the next SSC Meeting on Wednesday 8 May 2019 for Small Supplier 'T'.

**6. Verification User Security Assessment – Large Supplier 'L' (RED)**

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

The SSC **AGREED** to defer the decision to the next SSC Meeting on Wednesday 8 May 2019 for Large Supplier 'L'.

**7. Director's Letter – Small Supplier 'BO' (RED)**

The SSC considered Small Supplier 'BO'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 'BO'.

**8. Remediation Plan – Small Supplier 'E' (RED)**

The SSC **NOTED** Small Supplier 'E's Remediation Plan.

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

**9. Other User 'L' – Shared Resource Provider (RED)**

The SSC were provided with an update in order to make a decision as to whether a Party acting in the role of Shared Resource Provider to Export Suppliers only, can commence with Live Operations.

The SSC **NOTED** the update and **AGREED** the proposed recommendations which have been marked as **RED** and therefore recorded in the Confidential Minutes.

**10. SMETS1 Appropriate Standards (AMBER)**

An update was provided to SSC members on the development of guidance for Users from the User CIO concerning how to prepare for User Security Assessments and how to interpret the SEC obligations in respect of the application of an 'Appropriate Standard' of security to be applied to SMETS1 Smart Metering Systems.

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

## 11. SOC2 Final Report (**RED**)

The DCC confirmed the SOC2 Final Report had been received and was still being reviewed in order to specifically map and analyse the findings. A further update will be brought to the SSC meeting on 22 May 2019.

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

## 12. SSC Risk Register (**RED**)

The SSC were provided with an update on the current Risk Register and discussed the residual risks relating to each risk ID before deciding whether or not to close specific risk IDs.

Subsequent actions were classified as **RED** and have therefore been recorded in the Confidential Minutes.

The SSC **NOTED** the update and **AGREED** to close several risk IDs.

## 13. Rogue Devices being Joined/Un-Joined (**AMBER**)

An update was provided in relation to a previous request raised by the SSC to consider the issues posed by the joining and unjoining of rogue Devices. As such, the SSC **NOTED** the update and **CONSIDERED** the agreements and next steps proposed.

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

## 14. Feedback Review (**GREEN**)

The SSC were provided with an update on actions derived from feedback sought by SECAS in February 2019 at SEC Sub-Committee meetings which identified areas for improvement as well as areas that are working well which could be shared across Committees.

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

## 15. Change Items

An update was provided in relation to [SECMP0024 'Enduring Approach to Communication Hub Firmware Management'](#) which is currently undergoing the refinement process. Following feedback from the Proposer, the Working Group and the DCC, the business requirements have been established and solution design specifications for the proposed solution are being prepared for a DCC Preliminary Assessment.

The SSC **NOTED** the update and **CONSIDERED** the business requirements and solution design specification before providing advice on next steps.

## 16. CPA Matters (RED)

### Security Characteristics Timing of Implementation

The SSC **NOTED** the update in relation to the Security Characteristics document V1.3, whereby the SSC had consulted with the relevant trade bodies on an implementation date for V1.3 of the Security Characteristics.

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

### 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 **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.

### Optical Port for Triage

The SSC **NOTED** the update from NCSC in relation to a Device with an Optical Port. The Agenda Item was marked as **RED** and therefore recorded in the Confidential Minutes.

## 17. 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**)

**18. Any Other Business (AOB)**

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

**Next Meeting: 8 May 2019**