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.

Headlines of the Security Sub-Committee (SSC) 94_1202

At every meeting, the SSC review the outcome for Users' Security Assessments and sets an Assurance status for Full User Security Assessments (FUSAs) or a Compliance status for Verification User Security Assessments (VUSAs). The SSC also reviews outstanding actions, monitors the risks to the Commercial Product Assurance (CPA) certification of Devices, considers available updates from the DCC on Anomaly Detection and any reported changes in Shared Resource Providers by Users and reported Security Incidents and Vulnerabilities.

The SSC reviewed the following which are classified as **RED** and therefore recorded in the Confidential Meeting Minutes:

- Set an assurance status for three initial FUSAs;
- Set a compliance status for two second or subsequent FUSAs;
- Set a compliance status for five VUSAs;
- Noted one Security Self-Assessment (SSA); and
- Approved two Director's Letters.

The SSC also discussed the following items:

Matters Arising

- The SSC Chair informed Members of the acquisition of Hudson Energy by Shell Energy and the SSC **AGREED** the arrangements for outstanding User Security Assessment observations.
- The SECAS Security Expert gave an overview relating to a Large Supplier who wishes to trial pilot installs of SMETS2 Devices in staff properties. (**RED**)
- The SSC Chair informed Members of developments regarding Use Case 004 (Factory Reset), which was originally raised by Meter Asset Providers (MAPs) but is also supported by Suppliers and manufacturers. The SSC Chair advised that draft guidance has been provided to National Cyber Security Centre (NCSC) and BEIS for comment and that a full agenda item would be raised for the next SSC Meeting on Wednesday 26 February 2020.
- The SSC Chair gave an update of progress made on current SSC projects, including the Security Architecture Document (SAD) review, Security Incident Management (SIM) exercise and the End-to-End Security Risk Assessment. (**RED**)
- Ofgem Representatives informed SSC Members of a letter to be sent to the wider industry advising of Ofgem's participation at SSC Meetings, and reminding Operations of Essential

Services (OES) of their obligations under the Network Information Systems (NIS) Directive, where applicable.

- The SSC Chair informed Members that the SMKI PMA SEC Modification DP115 'Changes to the NCSC Good Practice Guides' has been raised to replace the NCSC Good Practice Guide (GPG) which have now been discontinued.
- The SSC Chair informed Members that the next SSC Commercial Product Assurance (CPA) Industry day is proposed to take place on Tuesday 31 March 2020.

Agenda Items

15. **SMETS1:** The DCC presented updates regarding the different aspects of SMETS1 enrolment, including the DCC's remediation plan; CIO report updates; negative testing; HAN Control Assurance; Certificate issues; Penetration Testing of Systems Integration Testing (SIT) A and User Interface Testing (UIT) A; Live Service Criteria; and Engineering Pins. The SSC **AGREED** a recommendation to the SEC Panel for the Live Service Criteria. (**RED**).

17. **CPA Monitoring:** The SSC considered a request for advice from the NCSC relating to potential vulnerabilities identified in a Device undergoing CPA Certification. (RED).

18. **Anomaly Detection:** The DCC presented results from their investigation of Anomaly Detection. (**RED**)

For further information regarding the Security Sub-Committee, please visit here.

Next Meeting: Wednesday 26 February 2020