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) 89_1311

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 **RED** and therefore recorded in the Confidential Meeting Minutes:

- Two Compliance Statuses for VUSAs;
- Approved one Director's Letter;
- Noted two Security Self-Assessments (SSAs); and
- Noted Remediation Plan updates for User Security Assessments.

The SSC also discussed the following items:

Matters Arising

1. The SSC discussed whether there should be additional SEC requirements for Users of Shared Resources to ensure security across multiple User Systems. **(AMBER)**
2. The SSC noted the following SEC Modification Updates:
    - The SMKI PMA Modification MP074 'Clarity on Obtaining SMKI Device Certificates' is due to be implemented in the SEC November Release.
    - A new problem statement was published on Tuesday 12 November 2019 DP094 'Supporting prepayment customers in no SM WAN scenarios' which may present security issues in which SSC may have an interest.
    - The SSC has provided input on SECMP0007 'Firmware Updates for IHDs and PPMIDs', which requires the DCC to clarify whether SRV11.1 can differentiate between firmware upgrades to ESME & GMSE separately from IHDs and PPMIDs, ADT to be performed and a limit of 30 days in the future for firmware upgrades to be activated.
    - SSC Supplier Members were encouraged to respond to the SECMP0046 'Allow DNOs to control Electric Vehicle chargers connected to Smart Meter Infrastructure' consultation by 5pm on Friday 15 November 2019.

3. The SSC agreed to approve the immediate drafting of guidance for SSC and industry review for:
   - The Use Case 'To identify installed SMKI Certificates' which was previously agreed at the Industry Working Group could now include the Public Certificate number behind a menu; and
   - The Use Case 'to reset the HAN' in cases where Commissioning has not completed, subject to the National Cyber Security Centre (NCSC) agreeing on the security controls that need to apply to the Triage site.

   The SSC also agreed to approve the actions to progress an impact analysis for:
   - The Use Case 'Factory Reset';
   - The Use Case 'Replace DNO Certificates'.
4. The SSC discussed two upcoming projects, including the Security Architecture Document (SAD) review and a Security Incident Management exercise. **(AMBER)**
5. The SSC Chair advised Members that the NCSC has not yet responded to the Gemserv report on 'Mitigating Risks for Internet-Connected Devices', and the SSC agreed this as an agenda item at the SSC meeting on Wednesday 11 December 2019 in order to create a high-level strategy of actions required. **(GREEN)**

Agenda Items

10. **SMETS1:** The DCC presented updates regarding the different aspects of SMETS1 enrolment, including the DCC's remediation plan; CIO report updates; SMETS1 alert storms; functional testing; the applicability of SEC obligation G2.11 in a MOC cohort; the depth and breadth testing documents for Final Operating Capability (FOC); the statement for the upcoming Live Services Criteria; and SMETS1 Certificate issues. (**RED**)
11. **Central Switching Service (CSS) Update:** The DCC provided an update on the risk assessment of the security architecture of the CSS. (**RED**)
12. **Improving DCC's Testing and Incident Response Plans:** The DCC provided an overview of the plans to improve its testing and incident response management. (**AMBER**)
13. **Anomaly Detection Threshold (ADT) Update:** The SSC Members agreed on ADT values for the DCC November Release. **(RED)**
14. **Supplier of Last Resort (SoLR) and Pre-Payment (PPM) Customers:** SECAS provided an update regarding the proposed solutions for protecting PPM customers during a SoLR event. (**AMBER**)

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

Next Meeting: Wednesday 27 November 2019