This document is classified as **Clear** in accordance with the Panel Information Policy. Recipients can distribute this information to the world; there is no limit on disclosure. Information may be shared without restriction subject to copyright.

Headlines of the Security Sub-Committee (SSC) 232_1102 11 February 2026

The SSC reviews the outcome for Users' and DCC Security Assessments and sets an Assurance status for Initial Full User Security Assessments (FUSAs), or a Compliance status for Verification User Security Assessments (VUSAs) and subsequent FUSAs. 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 the security implications of proposed changes and Anomaly Detection and any reported changes in Shared Resource Providers by Users and reported Security Incidents and Vulnerabilities.

The SSC set the Compliance Status for one Initial Full User Security Assessments (IFUSA), one Full User Security Assessment (FUSA), and three Security Self Assessments (SSA). Members were also notified of a potential escalation involving a Full User Security Assessment Remediation Plan and agreed the next steps.

Matters Arising

- The SSC reviewed three material change notification and agreed the next stages.
- Members were notified of the approval of the VWAN Soft Launch.
- SECAS noted a proposed migration of Devices from Small Supplier 'CE' to Small Supplier 'AM' scheduled to take place in the coming weeks. It was confirmed that SECAS will contact Small Supplier 'CE' to establish more information and to advise on the decommissioning process if this is necessary.
- The SSC were informed that the Quantum consultants have been engaged to review the outcome of the DCC Post-Quantum Computing Proof of Concept and advise on next steps.
- Members noted the Ofgem announcement on 9 February 2026 regarding the appointment of DCC2 Ltd.
- Members were notified that initial preparation for Risk Assessment RA11 has commenced. The SSC Chair asked for volunteers to form a sub-group to meet regularly to review progress and address issues ahead of SSC presentations.

2a. DCC CIO Assessments: The DCC CIO presented members with the CIO assessments, members noted the assessments and **AGREED** to the outcomes **(RED)**

2b. DCC CIO Forward Look and Remediations: The DCC CIO provided information on the DCC CIO Forward Look. The SSC **NOTED** the update. **(RED)**

4. CPA Matters: The SSC Chair presented updates on CPA Matters. The SSC provided feedback and **AGREED** the outcomes. **(RED)**

The SSC **APPROVED** the updated Communication Hub Security Characteristics to include Communication Hubs with Virtual WAN capability (**GREEN**)

5. **JICSIMP v1.5 Contacts and Web Form Review:** The SSC were provided with the amendments to the Joint Industry Cyber Security Incident Management Plan (JICSIMP) following the Security Incident Management Exercise (SIME) Outcomes Report and Lessons Learned item at SSC meeting 231. The SSC **APPROVED** JICSIMP V1.5 subject to members feedback and updates required on the web documents **(RED)**
6. **Device Manager Re-procurement:** The DCC presented an outline of the Device Manager Re-procurement project noting the background and the approach. The DCC will return to the SSC in March 2026 seeking formal support that there are no changes needed to the DM requirements. Members noted the update and provided feedback. **(GREEN)**
7. **Public Key Infrastructure Enduring (PKI-E) Live Service Criteria Readiness Update:** The DCC shared the Live Service Criteria with the SSC ahead of the recommendation which will be presented at SSC Meeting 233. Members noted the update and provided feedback. **(GREEN)**
8. **MP313 'Remove the DCC requirement to delete CHs from the SMI':** SECAS presented an overview of MP313 noting the issue, impact and potential solution. SECAS flagged that the modification originated from discussions held at TABASC 119 in November 2025. Members provided feedback on the modification. **(GREEN)**
9. **Standing Agenda Items:** SECAS noted that there were no Security Incidents and Vulnerabilities reported since the last SSC Meeting. **(CLEAR)**
10. **AOB:** Members raised two items of AOB which the SSC **NOTED**. **(RED)**

Next Meeting: 25 February 2026