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) 240_1006 – 10 June 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 Security Self-Assessment (SSA).

Matters Arising

The SSC noted updates on the following items:

- The SSC were provided with information on four material change requests. The SSC **NOTED** the proposal and provided the outcomes.
- The SSC Chair flagged that the Government has published the energy sector cyber security strategy: https://www.gov.uk/government/publications/energy-sector-cyber-security-strategy?utm_source=substack&utm_medium=email
  A roadmap for government, regulators and industry to strengthen cyber security and resilience across the Great British energy sector, supporting Clean Power 2030.
- The SSC were provided with information on the FSM post-go live security requirements members **NOTED** the update.
- The SSC were provided with an update on the RA11 Risk Assessment.

Agenda items:

2. **DCC CIO Forward Look (FOR INFORMATION):** The DCC provided information on the DCC CIO Forward Look. The SSC **NOTED** the update. **(RED)**

3. **Remediation Plan and Director's Letter Process (FOR DECISION) :** The SSC noted ongoing delays in the Remediation Plan (RP) process, with repeated assessment cycles delaying assurance outcomes indefinitely; to address this, a proposal was put forward to introduce a fixed timeframe with a maximum of three iterations, after which unresolved issues would be escalated to the SSC alongside targeted follow-up assessments. The SSC **AGREED** to introduce the limit of three RP submissions with subsequent escalation to the assessment process and that SECAS will communicate the measure timeously to all Users required to submit a RP. The SSC confirmed that an approach to investigate and address the Remediation Plan process in more detail would be addressed at the next SSC. **(RED)**

5. **CPA Matters (FOR DECISION):** The SSC Chair presented an update on the CPA Matters including interest from a company to be a CPA Test Lab, a risk review and summarised results of the CPL Survey. The SSC **NOTED** the update and provided feedback. **(RED)**

6. **Device Matters (non-CPA) (FOR DECISION):** The SSC Chair presented an update on issues with the FSM process for issuing IKI Certificates, noting SSC member reports of inconsistent DCC communications leading to a reversion to SharePoint, a recent IKI CRL availability issue, and related operational and submission challenges being addressed with DCC. The SSC **NOTED** the update and provided feedback. (**AMBER-STRICT**)

7. **Use Case 005 and Replay Risk (FOR DECISION):** The DCC presented an update on the risk assessment for Use Case 005, highlighting alignment with existing guidance to retain only Device Private Keys and ACB certificates during triage, confirming that risks are low and manageable with existing controls, and noting plans to update SEC guidance, implement the approach for DSP1, and support rollout through 4G Communication Hub Manufacturer updates. The SSC **NOTED** the update and **ACCEPTED** the risk described. **(RED)**

8. **FSM Service Now Notification (FOR DECISION):** The DCC presented information on a proposal to include incident severity within FSM email notifications, confirming that updates would be provided in plain text without hyperlinks to mitigate phishing risks, and that notifications would be limited to relevant recipients following feedback on security and distribution scope. The SSC **NOTED** the update and **AGREED** that there were no security objections to the proposal. **(GREEN)**

9. **CoS Re-procurement (FOR INFORMATION):** The DCC presented information on the COS procurement strategy, outlining plans to retain the existing environment, enable crypto agility to support post-quantum requirements, and introduce automated certificate rotation, with a low-risk walk-in takeover approach and no objections raised by the group. The SSC clarified that the correct regulatory term is ECoS and advised updating all documentation to ensure this aligns with the terminology in the SEC. The SSC **AGREED** there are no objections on security basis to the proposal. **(GREEN)**

10. **ISO 27701 Changes (FOR INFORMATION):** The SECAS Security Expert presented an update on ISO 27701 alignment with SEC Sections G and I, discussing potential amendments to the SEC and Guidance frameworks to ensure alignment with the new standards. The SECAS Security Expert confirmed that a proposal will be brought back to the SSC outlining potential SEC changes. The SSC **NOTED** the update. **(RED)**

11. **MP293 – Modification Report (FOR INFORMATION):** SECAS and the DCC Presented information on, MP293 'Provision of an DCC enhanced availability service to DCC users during DCC Service disruption/adverse weather' outlining an enhanced availability service to enable critical SRVs during DCC outages, particularly in exceptional scenarios, with a DSP1-focused solution that aims to mirror existing security controls, includes defined processing and assurance measures, and considers implementation timelines, migration impacts, and eventual decommissioning. The SSC **NOTED** the update and provided feedback. (**GREEN**)

12. **Standing Agenda Items (FOR INFORMATION):** The SSC Chair noted no Security Incidents and/or Vulnerabilities were reported since the last SSC Meeting. The SSC **NOTED** the updates. **(RED)**

13. **AOB (FOR INFORMATION):** There was one item of AOB. **(RED)**

Next Meeting: 24 June 2026