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.

SECMP0024 'Enduring Approach to Communication Hub Firmware Management'

Working Group Meeting 6 – 1 May 2019

Meeting summary

SECMP0024 business requirements

TABASC comments

The Working Group noted the comments of the Technical Architecture and Business Architecture Sub-Committee (TABASC) and how each will be accounted for.

The Data Communications Company (DCC) agreed that exception handling will need to be accounted for under the modification, but that this should occur later in the process after the DCC had carried out their Preliminary Assessment. The DCC also agreed that SLAs needed to be explored and put into the process, but that this would be done at the point of a DCC Impact Assessment, potentially via industry workshops. The Working Group agreed with this plan and were content with the timescales.

The DCC noted the comments from the TABASC who wanted more context in regard to a DCC operated web portal solution. Members were in agreement with SECAS that the detail around this solution would be given in the DCC Preliminary Assessment. The DCC did however note that the web portal solution option could utilise the functionality of the Self-Service Interface (SSI).

SSC comments

The DCC agreed with the Security Sub-Committee's (SSC) comment that, as part of any solution, the DCC needed to have the capability to deploy firmware updates to Communications Hubs in a shorter period than the default deployment/activation period of six months. SECAS confirmed the business requirements gave the DCC the capability to do this and the Working Group noted this.

The SSC have requested that the DCC carry out a risk assessment in parallel with the Preliminary Assessment, accounting for any possible exceptions that could occur during firmware deployment and activation scenarios. The SSC requested that the risk assessment include:

- any security risks and proposed mitigations arising from the solution itself; and
- any risks arising from failed firmware upgrades via the new solution (recognising that there is still the potential for upgrade failures due to a variety of circumstances and which could lead to stranding of assets etc).

The DCC asked for clarity as to whether the risk assessment should focus on the security of the DCC Systems or the security of the process, reiterating that the security of DCC Systems was secured as a matter of course. SECAS advised they would seek clarity from the SSC on what they wanted the risk assessment to examine.

Working Group comments

The Working Group had no further comments on the business requirements and agreed that, subject to SECAS and the DCC clarifying the requirements, they were now ready to be submitted for a DCC Preliminary Assessment.

Actions and next steps

- SECAS will work with the DCC and make amendments to the business requirements; and
- Subject to the Proposer's agreement, these will then be submitted to the DCC alongside a request for a Preliminary Assessment.