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.

MP109 ‘ADT and Exit Quarantine file delivery mechanism’

Annex C

Legal text – version 1.2

About this document

This document contains the redlined changes to the SEC that would be required to deliver this Modification Proposal.

Appendix AA ‘Threshold Anomaly Detection Procedures’

These changes have been redlined against Appendix AA version 2.0.

Amend Clause 2.2 as follows:

2. DCC Anomaly Detection Threshold Guidance

2.2 DCC shall:

(a) provide guidance to support Users in setting appropriate ADT and Warning Thresholds;

(b) provide a template for the User to provide its ADT and Warning Thresholds in the format set out in clause 6.3 of this document; ~~and~~

(c) provide guidance to support Users in submitting ADT submissions to the DCC via the DCC’s secure delivery method of choice; and

(d~~c~~) provide the guidance and template referred to above via the Self Service Interface (SSI).

Amend Section 3.3 and 3.4 as follows:

3. Notification of Anomaly Detection Thresholds

User and DCC Responsibilities: ADT submissions

3.3. Where a User wishes to submit a Fast-Track Notification it shall, prior to doing so, contact the ~~Service Desk~~ DCC and provide a justification for why it is necessary for them to do so.

3.4 A User shall, in each User Role in relation to which it is required (or elects) to set ADTs, provide an Anomaly Detection Thresholds File to the DCC via the DCC’s secure delivery method of choice (as from time to time specified on the SSI)~~an email to the Service Desk~~. The User~~email~~ shall include in such submission:

(a) the SMSR reference number in the subject line of the submission~~email~~; and

(b) the Anomaly Detection Thresholds File (of the form set out in clause 6.3 of this document), Digitally Signed by a Private Key associated with a File Signing Certificate and provided to an Authorised Responsible Officer (ARO) in accordance with the SMKI RAPP.

Amend Section 4.3, 4.7 and 4.8 and as follows:

4. Exceeding Anomaly Detection or Warning Thresholds

User and DCC Responsibilities: User Warning Threshold

4.3. Each User shall investigate, and then update and assign the Incident to the ~~Service Desk~~DCC using the “Update Service Management Incident” Functional Component within the SSI.

4.7 Each User shall investigate and resolve the ADT exceeded event. Each User shall make a submission to the DCC (via its secure delivery method of choice, as from time to time specified on the SSI)~~provide an email to the Service Desk~~ indicating the action to be taken on each of the quarantined communications. The User ~~email~~ shall include in such submission:

(a) the Incident reference number in the title~~subject line~~ of the submission~~email~~; and

(b) a valid CSV file, updated with the required action for each communication (“Release” or “Delete”), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

4.8. Each User shall update the Incident using the “Update Service Management Incident” Functional Component within the SSI and assign to the ~~Service Desk~~DCC for further action. The DCC shall:

(a) Check Cryptographic Protection applied to the CSV file, Confirm Validity of the Certificate used to Check Cryptographic Protection for the CSV file; and

(b) check that the format of the data is correct.

Amend Clause 4.13 as follows:

User and DCC Responsibilities: DCC Set Anomaly Detection Threshold

4.13 Upon being advised of the action to be taken, the User shall raise a DCC Service Management Service Request (SMSR) via the SSI to obtain a reference number for use in its submission to DCC (which reference number will be generated by the SSI automatically). The User~~s~~ shall then send the DCC a~~submit an email and~~ Quarantined Communications Action File which specifies actions in respect of each quarantined communication (which actions must~~and shall~~, where relevant, correspond with the actions ~~as~~ advised by the DCC). The submission of ~~S~~such file~~email~~ shall be made via the DCC’s secure delivery method of choice (as from time to time specified on the SSI)~~submitted to the Service Desk~~, and shall include:

(a) the DSMS Incident reference number notified in the title~~subject line~~ of the submission~~email~~; and

(b) a valid CSV file, updated with the required action for each communication (“Release” or “Delete”), Digitally Signed with a Private Key issued to the ARO for the purposes of CSV file signing, as set out in clause 6.5 of this document.

Amend Clause 6.1 as follows:

6. Communication Formats

6.1 All data sent ~~by email~~to the DCC for use in the DCC Systems for the purposes of these Threshold Anomaly Detection Procedures shall be in the form of a Digitally Signed CSV file. The field separator shall be a comma "," and the record separator shall be a line feed character 0x0A. In the file descriptions set out in clause 6.3 to 6.5 of this document, the character "▲" indicates the record separator. Users may include, within such CSV files, consecutive comma separators to the left of a record separator to specify that a field has a null value. DCC shall interpret consecutive commas within a record to identify a null value.