

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.

MP265 ‘Implementing ADT changes in response to a Security Incident’

Annex A

Business requirements – version 0.2

About this document

This document contains the business requirements that support the solution(s) for this Modification Proposal. It sets out the requirements along with any assumptions and considerations. The Data Communications Company (DCC) will use this information to provide an assessment of the requirements that help shape the complete solution.

1. Business requirements

This section contains the functional business requirements. Based on these requirements a full solution will be developed.

Business Requirements			
Ref.	Requirement	Responsible for delivery	MoSCoW
1	For instances where DCC services have been suspended following a Security incident, the Security Sub-Committee (SSC) – on behalf of affected DCC Users – shall authorise the DCC to make changes in User-set Anomaly Detection Thresholds (ADT) levels to prevent quarantining of critical messages for a specified period.	SSC	M
2	For instances where DCC services have been suspended following a Security incident, the DCC – under authorisation of the SSC – shall make changes in User-set ADT levels without recourse to individual Comma-Separated Values files, subject to Security controls, e.g. two-Party involvement.	DCC/SSC	M
3	For instances where DCC services have been suspended following a Security incident, the DCC – under authorisation of the SSC – shall suspend/amend User-set ADT settings for specified Service Reference Variants (SRV) for a limited period to be specified by the SSC.	DCC/SSC	M
4	For instances where DCC services have resumed following a Security incident suspension, the DCC – under authorisation of the SSC – shall return to the previous User-set ADT settings at a time specified by the SSC.	DCC/SSC	M

Key

- M = Must have
- S = Should have
- C = Could have
- W = Won't have

2. Considerations and assumptions

This section contains the considerations and assumptions for each business requirement.

2.1 General

The Proposer has identified that as part of Security incident recovery, there are currently no processes in place that would allow the DCC to amend User-set ADT files when recovering from an incident. This could limit the readiness to recover in the event of such an incident.

An improvement could therefore be made in the current User-set ADT arrangements which would allow the DCC to amend, in exceptional circumstances, the ADT levels of DCC Users. This would be broadly consistent with current obligations in the Smart Energy Code (SEC) on the Security Sub-Committee, DCC and Users.

SEC Section G6.7 provides for the SSC to advise the DCC on DCC-set ADTs global ADTs:

“G6.7 Where the DCC sets any Anomaly Detection Threshold in accordance with Section G6.6, it shall:

- (a) set that Anomaly Detection Threshold at a level designed to ensure that it will function, when used for the purposes of Threshold Anomaly Detection, as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems; and*
- (b) before doing so consult, and take into account the opinion of, the Security Sub- Committee as to the appropriate level of the Anomaly Detection Threshold.”*

This solution will be applied to instances of recovery following a major Security Incident. There should be no additional reporting requirements as a result of this modification.

2.2 Requirement 1: For instances where DCC services have been suspended following a Security incident, the SSC – on behalf of affected Users – shall authorise the DCC to make changes in User-set ADT levels to prevent quarantining of critical messages for a specified period.

In recovering from a major security incident, e.g. where DCC services have been suspended for a number of Users (maybe due to a common problem with a specific Device or system component), the recovery will require a backlog of SRVs to be sent to the DCC which are likely to exceed the User-set ADT levels for a temporary period.

In these circumstances, to facilitate a rapid recovery, the SSC shall authorize the DCC, on behalf of affected DCC Users, to make changes in User-set ADT levels to prevent critical messages from being quarantined for a specified period. The SSC shall provide effective governance and recording for the decision-making and direction to the DCC.

2.3 Requirement 2: For instances where DCC services have been suspended following a Security incident, the DCC – under authorisation of the SSC – shall make changes in User-set ADT levels without recourse to individual CSV files, subject to Security controls, e.g. two-Party involvement.

Amending User-set ADT levels is usually carried out by the DCC within 24 hours of receiving the file from the DCC User requiring amendments. In the event of a Security incident, the 24-hour lag may have an impact on the rapid recovery.

The aim is to enable rapid recovery by avoiding the need for individual DCC Users or someone on behalf of individual DCC Users having to complete what could be dozens of CSV files.

2.4 Requirement 3: For instances where DCC services have been suspended following a Security incident, the DCC – under authorisation of the SSC – shall suspend/amend User-set ADT settings for specified SRVs for a limited period to be specified by the SSC.

While in the recovery process following a Security incident, the Smart Metering Incident Response Team (SMIRT) would determine the affected Users and associated SRVs that were affected by the incident.

To avoid quarantining critical messages, User-set ADT settings for specified SRVs will be suspended or amended for a limited amount of time. This would allow critical messages to be processed as part of the recovery process.

2.5 Requirement 4: For instances where DCC services have resumed following a Security incident suspension, the DCC – under authorisation of the SSC – shall return to the previous User-set ADT settings at a time specified by the SSC.

Following the completion of recovery from a Security incident, the DCC shall return the affected DCC Users to the previous User-set ADT settings. The timing of when this should be implemented shall be dictated by the SSC.

The aim is the rapid recovery of the service following an incident. Returning the User-set ADT settings to their original figures would reduce the overall time after a recovery to re-instate ADT settings.

3. Glossary

This table lists all the acronyms used in this document and the full term they are an abbreviation for.

Glossary	
Acronym	Full term
ADT	Anomaly Detection Threshold
CSV	Comma-Separated Values
DCC	Data Communications Company
SEC	Smart Energy Code
SMIRT	Smart Metering Incident Response Team
SSC	Security Sub-Committee
SRV	Service Request Variant