

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.



DP265

‘Implementing ADT changes in response to a Security Incident’

Modification Report

Version 0.3

10 September 2024

Corporate member of
Plain English Campaign
Committed to clearer
communication

592



About this document

This document is a draft Modification Report. It currently sets out the background, issue, and progression timetable for this modification, along with any relevant discussions, views, and conclusions. This document will be updated as this modification progresses.

Contents

1. Summary.....	3
2. Issue.....	3
3. Assessment of the proposal	5
Appendix 1: Progression timetable	6
Appendix 2: Glossary	7

Contact

If you have any questions on this modification, please contact:

Georgiana Severin

020 7770 6921

Georgiana.Severin@gemserv.com

1. Summary

This proposal has been raised by Gordon Hextall on behalf of the Security Sub-Committee (SSC).

The Data Communications Company (DCC) System is utilised by multiple Service Providers and Service Users, all with different activities. It is the DCC's responsibility to ensure adequate measures are in place to ensure security threats are mitigated.

The SSC considered several scenarios that could have an impact on the Supply of energy to consumers as part of a Major Security Incident exercise to test the ability to respond to a Compromise.

In recovering from a Compromise where Service Requests (SR) have been temporarily suspended, DCC Users would need to amend the User-set Anomaly Detection Thresholds (ADT) to allow increased volumes of SRs to be processed without being quarantined. Where urgent action is required to support recovery and / or multiple DCC Users are involved, the ability to centrally amend User-set ADTs in exceptional circumstances would help to expedite the recovery for DCC Users and minimise any impact for consumers.

2. Issue

What are the current arrangements?

DCC Security

The DCC has a responsibility under Smart Energy Code (SEC) Section H10 'Business Continuity' to protect the DCC System in the event of compromise to ensure business continuity. This section of the SEC allows the DCC to act by temporarily suspending Service Users in certain circumstances. This suspension can be done in whole or in part and it would cushion or avoid the potential impact of Compromise to the DCC System.

What are Anomaly Detection Thresholds?

Service Users currently provide the DCC with their own ADT files, and these should provide a granular level of control over the volume of SRs that a DCC User may be sending to the DCC.

ADTs will detail the SR forecast and expected pattern of demand for each SR. Service Users will liaise with the DCC when setting their forecast and pattern of demand, and this would normally align with DCC's own thresholds. This is in line with SEC Appendix AA 'Threshold Anomaly Detection Procedures'.

The SSC has an obligation to provide support to the DCC and its DCC Users *'in relation to the causes of security incidents and the management of vulnerabilities on their Systems'* as currently defined in SEC Section G7 'Security Sub-Committee'.

What is the issue?

The SSC has a responsibility under SEC Section G7.19 (b) (i) to conduct risk assessments *"at least once each year in order to identify any new or changed security risks to the End-to-End Smart*

Metering System.”. As part of this responsibility, the SSC carries out annual security incident exercises to review and assess the risks arising from a Compromise of the End-to-End Smart Metering System and to ensure the ability to respond to and recover from such a Compromise.

There is currently no capability to centrally amend the Service User ADT in the event of recovery from a system Compromise, which could limit the readiness to quickly recover from such an Incident.

The SSC noted that an improvement to the current User-set ADT arrangements could be made whereby the DCC could be directed by the SSC, with appropriate governance, to amend, in exceptional circumstances, the ADT levels of DCC Users. The exceptional circumstances would be where recovery requires a larger number of SRs to be processed than the ADT settings allow. The ADT settings therefore need to be temporarily amended to avoid SRs being quarantined to facilitate a recovery from a Compromise. This would be broadly consistent with existing SEC obligations on the SSC, DCC and DCC Users:

SEC Section G7.21 (b) requires that *“The Security Sub-Committee shall:*

(b) monitor the (actual and proposed) Anomaly Detection Thresholds of which it is notified by the DCC, consider the extent to which they act as an effective means of detecting any Compromise to any relevant part of the DCC Total System or of any User Systems, and provide its opinion on such matters to the DCC;”

SEC Section G6.10 (b) requires the DCC and DCC Users to have regard to SSC opinion:

“G6.10 The DCC and each User shall, in relation to each Anomaly Detection Threshold that it sets:
(a) keep the Anomaly Detection Threshold under review, having regard to the need to ensure that it continues to 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 and/or User Systems (as the case may be);
(b) for this purpose have regard to any opinion provided to it by the Security Sub- Committee from time to time as to the appropriate level of the Anomaly Detection Threshold;”

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.”

What is the impact this is having?

In the event that a Party is Compromised, and the Smart Metering Service is put at risk, the DCC may wish to take action to protect Services to other Users and may suspend a Service User.

Noting the allowance of SEC Section H10, there is currently no SEC compliant method by which DCC may override a DCC User provided ADT in efforts to recover Services after a Compromise.

Impact on consumers

The impact on consumers relates to mitigating against a risk of loss of key smart metering services as a result of an attack.

3. Assessment of the proposal

Areas for assessment

Amending User-set ADTs in Major Security Incidents

As part of the next steps of this Modification, the governance arrangements that will apply to the SSC decision-making will be clarified. This will include, but is not limited to, clarification of the quorum for decision-making and examples of the exceptional circumstances where User-set ADTs could need to be amended when the SSC meets as the Smart Metering Incident Response Team (SMIRT).

How will the ADTs be returned to their previous levels once a security incident is over?

Change Sub-Committee (CSC) members noted concerns around the reversal process following a Compromise. They wondered whether DCC Users would be required to provide new ADTs or whether the DCC would automatically revert to the original values before the Compromise occurred.

How ADTs are reverted to the original levels after recovering from a Compromise will be determined as part of the solution.

How will affected DCC Users be notified?

As part of the security incident management exercise, DCC Users should be notified of any Compromise. However, whether this communication comes from the DCC, or the SSC would depend on the nature of the security incident and how many DCC Users are affected.

Sub-Committee input

The Smart Energy Code Administrator and Secretariat (SECAS) will engage with the Chairs from the Operations Group (OPSG), the Technical Architecture and Business Architecture Sub-Committee (TABASC), the SSC, the Smart Metering Key Infrastructure Policy Management Authority (SMKI PMA) and Testing Advisory Group (TAG) to confirm what input is required from these forums. SECAS believes the following Sub-Committees will need to provide the following input to this modification:

Sub-Committee input	
Sub-Committee	Input sought
OPSG	None
SMKI PMA	None
SSC	Input on business requirements and solution development
TABASC	Input on business requirements and solution development
TAG	None

Views of the Change Sub-Committee

CSC members suggested that part of the solution should include communicating with DCC Users to improve the understanding of ADTs. While DCC Users may be setting reasonable ADT levels, it would be useful to be made aware when changes are needed.

CSC members queried whether part of the next steps would be taking the modification to be reviewed by TABASC, which may be needed if the developed solution requires a system change. SECAS noted that TABASC would be interested if the process involved system changes.

Appendix 1: Progression timetable

Timetable	
Event/Action	Date
Draft Proposal raised	13 Feb 2024
Presented to CSC for initial comment	20 Feb 2024
Modification discussed with Proposer	Feb-Mar 2024
Business Requirements discussed with DCC and the Proposer	Mar – Aug 2024
CSC converts Draft Proposal to Modification Proposal	17 Sep 2024
<i>Modification discussed with Working Group</i>	<i>Oct 2024</i>
<i>DCC Preliminary Assessment Requested</i>	<i>Oct 2024</i>
<i>DCC Preliminary Assessment Received</i>	<i>Nov 2024</i>
<i>Modification discussed with Working Group</i>	<i>Dec 2024</i>
<i>Modification discussed with TABASC</i>	<i>Dec 2024</i>
<i>Refinement Consultation</i>	<i>Dec 2024 - Jan 2025</i>
<i>Modification discussed with Working Group</i>	<i>Feb 2024</i>
<i>Impact Assessment costs approved by Change Board</i>	<i>Feb 2024</i>
<i>Impact Assessment Requested</i>	<i>Feb 2024</i>
<i>Impact Assessment Received</i>	<i>Apr 2024</i>
<i>Modification Report approved by CSC</i>	<i>May 2025</i>
<i>Modification Report Consultation</i>	<i>May - Jun 2025</i>
<i>Change Board Vote</i>	<i>Jun 2025</i>

Italics denote planned events that could be subject to change

Appendix 2: 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
CSC	Change Sub-Committee
DCC	Data Communications Company
OPSG	Operations Group
SEC	Smart Energy Code
SECAS	The Smart Energy Code Administrator and Secretariat
SMIRT	Smart Metering Incident Response Team
SMKI PMA	Smart Metering Key Infrastructure Policy Management Authority
SR	Service Request
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
TAG	Testing Advisory Group

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.

DP265 ‘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