

SEC Modification Proposal, SECMP0265, MSACC0005

**Implementing ADT Changes in Response to a
Security Incident**

**Second Preliminary Impact Assessment (PIA),
Future DSP Platform**

Version:	2.2
Date:	28th July 2025
Author:	DCC
Classification:	DCC PUBLIC

Contents

1	Executive Summary	3
2	Document History	4
2.1	Associated Documents.....	4
2.2	Document Information	4
3	Context and Requirements.....	5
3.1	Current Arrangements	5
3.2	What is the Issue and Potential Solution?	5
3.3	Impact of the Issue.....	6
3.4	Business Requirements	6
4	Description of Solution.....	8
4.1	Impacts on Future DSP	8
4.2	Impacts on Future Service Management.....	9
5	Impact on DCC Systems, Processes, and People.....	10
5.1	Security Impact	10
5.2	Technical Specifications	10
5.3	Infrastructure Impact	10
5.4	Transition into Service.....	10
5.5	Service Impact.....	10
5.6	DCC Impacts.....	10
6	Implementation Timescales and Approach	11
6.1	Testing and Acceptance	11
6.1.1	Pre-Integration Testing	11
6.1.2	System Integration Testing	11
6.1.3	User Integration Testing	12
7	Costs and Charges	13
7.1	Design, Build and Testing Cost Impact	13
8	Clarifications, Risks, Assumptions, Issues, and Design Decisions	14
8.1	Required Clarifications	14
8.2	Risk	14
8.3	Assumptions	14
8.4	Issues.....	14
8.5	Design Decisions	15
	Appendix A: Glossary	16
	Appendix B: Low-Level Requirements for SECMP0265.....	17

1 Executive Summary

The Change Board are asked to approve the following:

- Cost to complete the Full Impact Assessment of **£29,117**.
- The timescales to complete the Full Impact Assessment of 40 Working Days.
- ROM costs for SECMP0265, up to the end of Pre-Integration Testing (PIT) of £160,000 to £240,000.
- The Future Data Service Provider (DSP) and Future Service Management (FSM) Service Providers are impacted by this Modification.

Problem Statement

The Security Sub-Committee (SSC) reviewed security compliance in both SEC Appendix AA and SEC Section H10 to assess if the controls are sufficient that could allow the DCC to secure its network and infrastructure in the event of system compromise. One hypothetical scenario is a situation where the energy supply to consumers is compromised by external threat actors and the existing User-set Anomaly Detection Threshold (ADT) files based checking might need to be centrally amended by the DCC to stop the attack.

It has been established that there is no capability to centrally amend the Service User ADT files by the DCC in the event of a system compromise and this would limit the readiness of the DCC to mitigate against, or respond to, the perceived threat.

Modification Benefits

Where urgent action is required to support recovery and / or multiple DCC Users are involved, the ability to centrally turn off and restart User-set ADT file checking in exceptional circumstances would help to expedite the recovery for DCC Users and minimise any impact for consumers.

2 Document History

Revision Date	Revision	Summary of Changes
17/07/2025	2.01	DSP2 Initial version, for DCC internal review
28/07/2025	2.2	Review completed, costs updated, with challenges to Service Providers provided

2.1 Associated Documents

This document is associated with the following documents:

Ref	Title and Originator's Reference	Source	Issue Date
1	MP265 - Modification Report v0.5	SECAS	07/07/2025
2.	MP265 - Business Requirements v0.2	SECAS	09/10/2024

References are shown in this format, [1].

2.2 Document Information

The Proposer for this Modification is Gordon Hextall of the Security Sub-Committee, although Martins Atoyebi of the DCC is acting as Technical Lead.

The first Preliminary Impact Assessment (PIA) for a solution on the existing DSP platform was requested of DCC on 8th November, 2024 and submitted on 28th November, 2024.

This second PIA relates to the implementation of this Modification on the Future DSP (also known as the DSP To Be or DSP2). It was requested on July 8th, 2025.

3 Context and Requirements

In this section, the context of the Modification, assumptions, and the requirements are stated.

The requirements have been provided by the Proposer and have been validated by SSC and TABASC.

3.1 Current Arrangements

The DCC Total System is used by multiple Service Providers and Service Users, covering many 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 a Service User has been temporarily suspended, DCC Users would need to turn off, or suspend, the User-set ADT checking to allow increased volumes of SRs to be processed without being quarantined.

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 or suspend ADT checking entirely when recovering from an incident. This could limit the readiness to recover in the event of such an incident.

3.2 What is the Issue and Potential Solution?

In exceptional circumstances, where urgent action is required to support recovery and / or multiple DCC Users are involved, the ability to centrally amend User-set ADTs and potentially even suspend ADT checking would help to expedite the recovery for DCC Users and minimise any impact for consumers. An improvement would be made in the current arrangements which would allow the DCC to potentially suspend ADT checking. This would be broadly consistent with current obligations in the Smart Energy Code (SEC) on the Security Sub-Committee, DCC ,and Users as noted following.

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) and G6.7 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 turning off and restarting ADT checking:

“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.

3.3 Impact of the Issue

If 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 DCC may suspend services to the impacted 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.

3.4 Business Requirements

The high-level business requirements are as follows.

Ref	Requirement	MOSCOW
1	For instances where DCC services have been suspended for impacted Service User(s) 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.	Must
2	For instances where DCC services have been suspended for impacted Service User(s) 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.	Must
3	For instances where DCC services have been suspended following a Security incident, the DCC –under authorisation of the SSC – shall turn off the ADT functionality for impacted Service Users for a limited period to be specified by the SSC.	Must
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 for impacted Service User(s) at a time specified by the SSC	Must

Further detail for each requirement follows.

Requirement 1: 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 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.

Requirement 2: 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 Service User(s), or someone on behalf of individual Service User(s), having to complete what could be dozens of CSV files.

Requirement 3: While in the recovery process following a Security incident, the Smart Metering Incident Response Team (SMIRT) would determine the affected Users that were affected by the incident.

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

Requirement 4: Following the completion of recovery from a Security incident, the DCC shall return the affected Service User(s) 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.

There should be no additional reporting requirements as a result of this Modification.

DCC have defined a series of Low-Level Requirements based on the requirements above. These will be used for development and testing of the functionality for this Modification. These Low-Level Requirements are included in Appendix B at the end of this document.

4 Description of Solution

This second Preliminary Impact Assessment has been completed based on the provision of screens and functionality in the Future Service Management (FSM) Service Now-based user interface and the Future DSP (DSP2).

This solution is based on the following design components:

1. Introduction of two new service calls from the FSM to DSP2 interface to allow DCC Service Management to turn off (suspend) and restart (reactivate) checking of Anomaly Detection Thresholds (ADTs) for specific, individual DCC Service Users (referred to as "Service User(s)" following).
2. Turn off ADT checking for specified Service User(s) on receipt of a request to do so from a valid DCC User.
3. Restart ADT checking for the specified Service User(s) on receipt of a request to do so from a valid DCC User.
4. Prevent the processing of any Business As Usual (BAU) ADT files for a Service User during any period where ADT checking has been turned off.
5. Implement a configurable maximum time period during which ADTs can be suspended for a specific Service User.
6. Automatically reinstate ADTs for a Service User once the specified maximum time period has elapsed.
7. Include information within logging and auditing when the turn off and reactivate functionality has been used including:
 - Service User details
 - start and end time of the ADT checking suspension period

4.1 Impacts on Future DSP

The Change is expected to have an impact upon the following workstreams:

Design Authority: impacts Microservice Component Specification Documents.

Application Development: impacts low level design and code to turn off and reactivate ADT thresholds for specified Service User(s) as follows:

- Include a configurable maximum time period that ADTs can be turned off
- Creation of an automated process to reactivate ADTs for a user once the maximum time period has been reached unless a separate FSM request has already restarted them

Testing: additional test scenarios will be required to prove the capability works as per requirements.

Migration from Existing DSP to DSP2: if implemented before the Migration of Devices to DSP2 is complete, the ADT checking will need to be turned off for on both DSPs for a

specified Service User because the DSP Total System will have two gateways for devices, and Service User Devices will most likely be held on both platforms. This would require implementation on both the current DSP, as detailed in the PIA for CR5524 previously, as well as the DSP2 platform in this PIA.

DSP Microservices: the Modification will impact on microservice designs; note currently the impacted microservices have not been designed.

Other Solution Impacts: Upon restarting the ADT checking, the ADT values for the selected Service User(s) will be returned to their previous values held before being ADT checking was turned off. Restarting will also reset the counter for each impacted ADT rule to ensure that the messages received during suspension do not impact subsequent ADT checking.

Although it is expected that ADT checking will be restarted by the DCC as soon as it is possible to do so, the DSP solution will provide a backstop position by setting a maximum time period for which ADTs checking can be turned off. This will be a global configuration value agreed with the DCC (and the SSC). ADT checking will be automatically restarted if the maximum time period is reached.

Note that whilst ADT checking is suspended for a given Service User ID, it will not be possible to upload a new ADT file for that Service User through the standard ADT upload process.

4.2 Impacts on Future Service Management

The FSM component based on ServiceNow will allow valid DCC Service Management Users to turn off and restart ADT checking. Changes to the existing FSM will include:

- Create a security group to provide RBAC access allow an entitled User to turn off or restart the ADT file checking.
- Configure a function for a User to request an update to a value through an API.
- Build proxy-APIs to perform an update between DSP and FSM. The FSM integration hub will create pass-through proxy APIs to expose these to FSM.
- Update transforms in ServiceNow to allow the data for the new field on the device table to be ingested via the ESI report and real time API.

5 Impact on DCC Systems, Processes, and People

This section describes the impact of SECMP0265 solution on DCC Services and Interfaces that impact Users and/or Parties.

5.1 Security Impact

Changes to the timing of message processing do not have a security impact. Further, there are no interface changes to the solution and no new infrastructure is being introduced in support of the solution. As such, there is no perceived need for penetration testing nor any Protective Monitoring changes. The security impact of this Modification should be limited to security assurance throughout the implementation phase. This assurance includes reviewing designs, test artefacts and providing consultancy to the implementation and test teams.

A more detailed assessment of Security impact will be carried out as part of the Full Impact Assessment.

5.2 Technical Specifications

No changes to any technical specifications required for this modification. This is not a design change.

5.3 Infrastructure Impact

There will be no change to the infrastructure design because of this Modification. Additional processing and storage might be required. However, they are not sufficiently large to warrant the procurement of additional compute power or storage.

This Modification does not impact the DSP resilience or Disaster Recovery implementation.

5.4 Transition into Service

It is assumed that the activities required for the Transition to Operations will be minimal.

5.5 Service Impact

No service impacts are anticipated.

5.6 DCC Impacts

The DCC Service Desk and Service Management teams will have to update existing, and potentially create new, processes to handle directions from the SSC to turn off, or restart the existing ADT-related processes and handle requests.

6 Implementation Timescales and Approach

This Modification will be implemented in a future SEC Release. Design, Build, and PIT is expected to take approximately **three** months to complete after the CAN is signed.

The current SECAS forecast for the implementation of this Modification is November 2026. Details of the implementation will be finalised in the FIA. However, the Modification cannot be implemented on DSP2 alone while the existing DSP platform is in use, and if designated for the DSP2 platform alone, must be implemented after Migration is complete.

Implementation of this change is assumed to follow a hybrid of agile and waterfall methodology. The release lifecycle duration will be confirmed as part of the FIA.

6.1 Testing and Acceptance

For each SEC System Release, there is a Post-PIT Change Request that provides the System Integration Testing (SIT) and UIT response for the SEC Release as a whole, covering the testing of individual changes in the scope of the release, as well as activities that are common to all changes in the scope (e.g. test plans, system regression testing, test management and governance). This is not included in this PIA.

6.1.1 Pre-Integration Testing

As part of PIT, the System Test Team will validate and verify new behaviour on DSP2 and FSM.

- New or updated tests will identify the areas within the DSP that will allow turning off, or the restart of ADT checking for Service User(s). Tests will be executed to turn off ADT checking and attempt an ADT file upload while suspended.
- Restarting will be run manually to test restart rules, which include restart rejections and timeouts.
- End to end suspension tests and regression testing of ADT while a feature switch is disabled.

6.1.2 System Integration Testing

The Modification will be delivered as part of a SEC System Release. The SIT scope of this Modification will comprise:

- verifying that a valid DCC User can turn off the ADT thresholds set by a DCC Service User via the new FSM user interface
- verifying that after turning off, the DCC Service User is able to successfully submit a volume of SRVs that exceed the thresholds set in the ADT file
- verifying that a valid DCC Service User is able to restart ADT checking set by a DCC Service User via the new FSM interface

As this Change is not device-related, the scope of testing will not require any dedicated Devices.

Note that SIT costs are not included in the PIA costs and effort calculations.

6.1.3 User Integration Testing

The User Integration Testing (UIT) team will check that the new FSM screens are available to verify that a DCC User is able to turn off the ADT checking set by a Service User via the new FSM user interface and verify that a DCC User is able to restart ADT file checking previously set by a Service User via the new FSM user interface.

To verify the new functionality listed above, new tests will be required. No Devices will be required to confirm.

7 Costs and Charges

The scope of supply under this PIA includes design, development (build), system testing, testing within the PIT environments.

The Rough Order of Magnitude cost (ROM) shown below describes indicative costs to implement the functional and non-functional requirements as assumed above. The price is not an offer open to acceptance. It should be noted that the change has not been subject to the same level of analysis that would be performed as part of a Full Impact Assessment and as such there may be elements missing from the solution or the solution may be subject to a material change. As a result, the final offer price may result in a variation.

7.1 Design, Build and Testing Cost Impact

The table below details the cost of delivering the changes and Services required by the Service Providers to implement this Modification. For a PIA, only the Design, Build and PIT indicative costs are supplied.

£	Design, Build and PIT
SECMP0265	£ 160,000 to 240,000

Although not included in this PIA, it is expected that there will be integration testing costs associated with this Modification. If the targeted SEC Release date includes another Modification or Change Request with regression testing, that cost will be shared equally between the two (or more) changes, and the cost of Integration Testing will come down.

Based on the existing requirements, the total fixed price cost for a Full Impact Assessment by the DSP and FSM is **£29,117** and would be expected to be completed in 40 Working Days.

8 Clarifications, Risks, Assumptions, Issues, and Design Decisions

In the following sections, Required Clarifications, and any Risks, Assumptions, Issues, and Design Issues have been identified.

DCC requests acceptance and mitigation plans be provided by the Business proposer and/or Working Group before moving to the FIA.

8.1 Required Clarifications

Ref.	Required Clarification	Status
MP265-RC1	Defining ADT management in this Modification on a per Service User basis does not give the granular control offered by specifying levels per SRV for either Warning or Quarantine values as defined below.	Requires Confirmation

8.2 Risk

Ref.	Risk	Mitigation
MP265-RR1	When DCC is directed to turn off ADT checking for a specific User(s), there will be no checking of ADTs for any SRV, and consequently an excessive number of single SRVs could be submitted at one time. There might be some impacts on the DCC Total System in this case.	Monitoring of the traffic to and from an impacted Service User by SSC and DCC Service Management will be a required part of managing an incident.

8.3 Assumptions

Ref.	Assumption	Status
MP265-DA1	ADT Threshold definitions include individual numbers against each service Reference Variant, defined as either Warning or Quarantine thresholds. As part of the Requirements Workshop (May 23, 2025), it was agreed that any suspension of ADT checking would be a blanket definition, i.e., all SRVs for the specified Service User(s), and would not specify levels per SRV for either Warning or Quarantine values.	Requires Confirmation
MP265-DA2	After ADT checking is restarted, the DSP shall use the previously agreed ADT settings for the specific Service User(s).	Accepted

8.4 Issues

None identified at this time.

8.5 Design Decisions

Ref.	Design Decision
MP265-DD1	An initial PIA was raised against the Legacy DSP system in November 2024. After review, SSC decided this Modification should not be implemented on the Legacy DSP.
MP265-DD2	As part of the Requirements Workshop, it was agreed that any suspension of ADT checking would be a blanket definition for that Service User, and would not specify levels per SRV for either Warning or Quarantine values. This is a far simpler path than having to recalculate levels for each SRV. The same would apply on restarting the ADT file checking.
MP265-DD3	When ADT checking is turned off, all elements of the ADT process such as the attribute checks for affected users and global settings are also turned off.

Appendix A: Glossary

The table below provides definitions of the terms used in this document.

Acronym	Definition
ADT	Anomaly Detection Threshold
API	Automated Programming Interface
BaU, BAU	Business As Usual
CAN	Contract Amendment Note
Comms Hub	Communications Hub
CR	DCC Change Request
CSV	Comma Separated Values
DCC	Data Communications Company
DSP	Data Service Provider
ESI	Enterprise Systems Interface (file format)
FIA	Full Impact Assessment
FSM	Future Service Management
PIA	Preliminary Impact Assessment
PIT	Pre-Integration Testing
RAID	Risks, Assumptions, Issues, and Dependencies
ROM	Rough Order of Magnitude (cost)
SEC	Smart Energy Code
SECAS	Smart Energy Code Administrator and Secretariat
SIT	Systems Integration Testing
SMIRT	Smart Metering Incident Response Team
SR	Service Request
SRV	Service Reference Variant
SSC	Security Sub-Committee
TABASC	Technical Architecture and Business Architecture Sub-Committee
UIT	User Integration Testing

Appendix B: Low-Level Requirements for SECMP0265

The following Low-Level Requirements have been defined for this Modification.

1. Develop APIs to enable the temporary turn off and subsequent reactivation of ADT checking for impacted Service User(s) to be managed via Future Service Management (FSM).
2. Prevent the processing of Service User ADT files if ADT checking for the corresponding Service User is currently turned off.
3. Implement a configurable maximum duration for which ADT checking can remain turned off for impacted Service User(s), serving as a safeguard.
4. Ensure that ADT settings checking is returned to previous settings for impacted Service User(s) once the maximum turn-off duration is reached.
5. Implement a user interface (within FSM) that enables suitably privileged DCC staff to turn off, or return to previous, ADT settings checking for a specified Service User(s).
6. Provide a corresponding screen (within FSM) to allow authorised DCC staff to reverse the changes i.e., restore the original ADT settings checking, for the specified Service Users.
7. Ensure that all ADT turn off and return to previous settings actions follow a two-step workflow, requiring submission by one DCC User and approval by a separate, suitably privileged DCC User.