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.

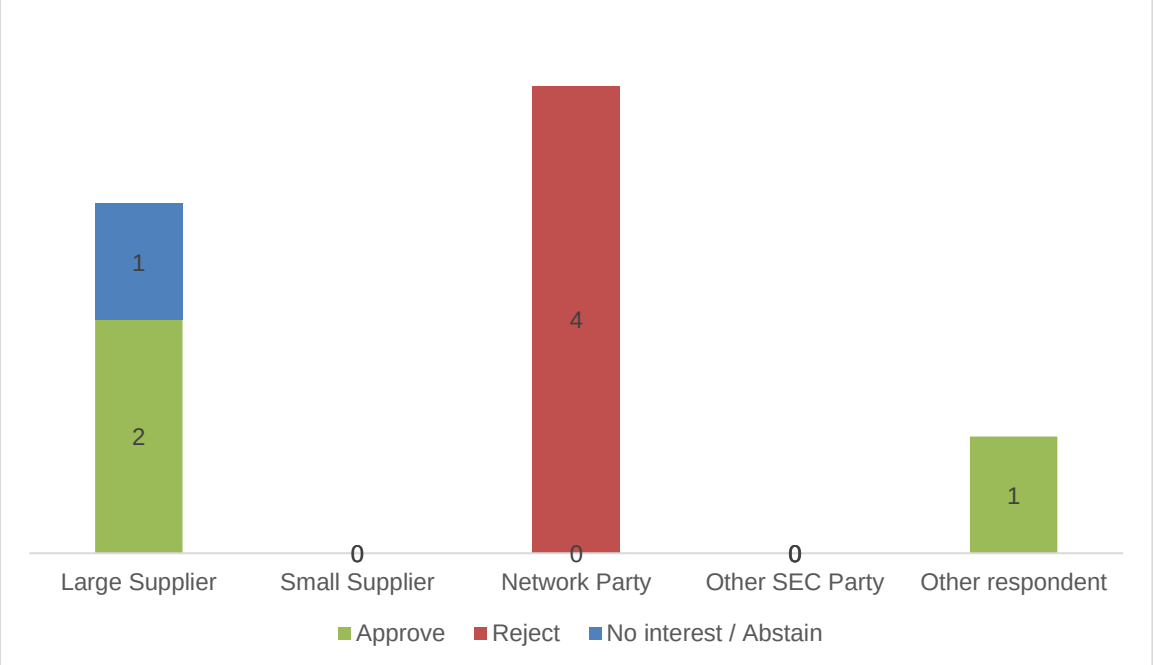
SECMP0062 'Northbound Application Traffic Management - Alert Storm Protection'

Modification Report Consultation responses

About this document

This document contains the full non-confidential collated responses received to the SECMP0062 Modification Report Consultation.

Summary of responses



Question 1: Do you believe that SECMP0062 should be approved?

Question 1			
Respondent	**Category**	**Response**	**Rationale**
Western Power Distribution	Electricity Network Party	Reject	Western Power does not believe that this modification as it stands better facilitates the SEC Objectives. The MRC states that the Proposer believes that it better facilitates SEC Objective (a) and (e). We cannot see any correlation to SEC Objective (e) 'to facilitate such innovation in the design and operation of Energy Networks (as defined in the DCC Licence) as will best contribute to the delivery of a secure and sustainable Supply of Energy.' We believe that the intent of this modification would be to better facilitate SEC Objective (f), to ensure the security of Data and Systems, however we do not believe that the solution proposed will do this. To help justify our response we have considered this modification against today's scenario. We are currently receiving over 1.3 million nuisance alerts (8014 and 8015) a day. If this solution was implemented it would not actually supress any of these due to their frequency. Also, if the solution did create incidents, as the Target Recipient we would be getting incidents assigned to us, however we have absolutely no control over these alerts and so would have to use resource to respond to incidents advising that there is nothing we can do to stop the issue.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			Finally in the WGC a recommendation was proposed that the Unauthorised Physical Access alerts (including 8F3F) be exempt. We believe that this is reasonable due to Health and Safety concerns, however if this was the case, the current issues that the DCC are experiencing would continue and the issue remain as none of the current nuisance alerts would be disregarded. In conclusion we do not believe that the proposed solution, as it currently stands, better facilitates any SEC Objective, nor resolves the issue outlined in the background of the Modification Report Consultation as it does not address the root causes of the high volumes of these alerts.
EDF Energy	Large Supplier	Approve	We believe that SECMP0062 better facilitates SEC Objective (a) as minimising the impact of 'alert storms' will ensure that the DCC systems do not become overloaded and continue to support communications with smart metering devices. It will also prevent DCC User systems from receiving unnecessary duplicate alerts, enabling actual problems to be more easily identified and rectified.
Electricity North West Limited	Electricity Network Party	Reject	We support the intent of the modification proposal, however, we challenge whether the proposed solution results in efficient operation as per Objective (a) or innovation in operation as per Objective (e). The key reasons for our rejection of this modification are as follows: a) The proposed solution would do nothing to filter the 8014/8015 Power Factor alerts (number two issue in terms of volume on the SECOPS list of nuisance alerts). The proposed DCC solution would only filter alerts happening at a rate of more than 2 per minute per device. 8014/8015 are spurious alerts being incorrectly generated by non-compliant SMETS2 meters when power consumption falls to or returns from

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			a very low threshold and as such we could receive one every 5 minutes or every half hour e.g. when a fridge compressor in an empty premise kicks on and off. To date we have received circa half a million of these alerts from just a few hundred devices. b) The modification does not identify or address root cause of alert storms which are in our belief primarily caused by non-compliant meter devices rather than by individual device behaviour. As part of this SEC modification DCC should look to provide MI/Analytics based reporting which will pro-actively identify the manufacturer/model/firmware combinations of meters that result in alert storms such that appropriate action can be taken by suppliers/manufacturers to resolve/remediate the root causes. c) Each individual meter affected by the proposal could result in hundreds, if not thousands, of incidents being raised in the DCC Incident Management System. Each time throttling is initiated for an individual device it will generate an incident in the DCC Incident Management System, this would have a clear knock on-impact in terms of DCC and User resource in order to update and resolve/close the incidents and therefore a likely increase in both DCC and User resource costs. There is no assessment by DCC of consequential cost and resource impacts required to manage the increased volumes of incidents. There is also no mention of how DCC would propose to use problem management to collate and resolve the numerous incidents (as per standard ITIL process) and address root cause. d) DCC are proposing that the incidents would be assigned to the intended alert recipient, not to the party responsible for the meter/configuration. As a DNO we can do little or nothing to prevent further alerts or to resolve issues with non-compliant

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			meter functionality, we have no commercial or contractual relationship with Suppliers or Manufacturers. e) DCC are proposing to build email functionality to send an email each time throttling is initiated for an individual device. Although DCC are proposing to allow Users to individually choose whether switch this functionality on or off this would clearly result in huge volumes of email traffic which would impact on DCC and User email infrastructure. There is no assessment by DCC of consequential infrastructure costs required to manage increased volumes of emails. f) DCC are proposing to amend DUIS functionality so that subsequent alerts which are not throttled would include metadata to indicate that alerts were previously throttled and to provide a counter of the number of throttled alerts in real-time. It is unclear what the business use case for this requirement is and what action could actually be taken in real-time to remediate any affected devices. A DCC reporting/MI system could provide the same information without requiring each User to make any amendments to their DUIS interface. g) DCC have not provided any modelling to show what the solution outputs would actually result in e.g. 10k meters each generating 10 alerts, throttled as 1 in 10 could theoretically result in 10k incidents and 10k emails dependent upon the timing/interval between the alerts being received by DCC.
SSEN	Electricity Network Party	Reject	SSEN support the overall requirement to supress alert storms to protect the DCC and user systems. From the previous consultation, SSEN still challenge whether the proposed changes will adequately deliver the required solution.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			Our concerns still surround the suppression logic. As we have not seen the worked example as described in the consultation, we are unable to understand the true impact on SSEN and our adapter. Looking to the initial proposed configuration parameters, in this consultation, this will still allow many alerts through to our adapter. We also have concerns around the proposed SSI Dashboard, reporting and email notification functionality. As previously stated we would want to be able to understand the number of alerts throttled without this having a negative impact on SSI, our internal systems and processes. The proposed solution does not allow for an appropriate mechanism to notify us, manage and report on throttling without internal processes created to handle this. It is also proposed to introduce DUIS schema changes to provide real time notification of alert throttling. SSEN are unclear as to why this would be required if the throttling is already handled by a new mechanism within the DCC.
Security Sub-Committee	Other Respondent	Approve – subject to security concerns being satisfactorily addressed.	The Consultation Report contains a statement: **"Sub-Committee views** The Security Sub-Committee (SSC) chairman was on the Working Group and attended one of the meetings when the business requirements were being formulated. The view provided on behalf of the SSC at the time was that this shouldn't hold any security risks provided the proposed solution adheres to the requirements put forward." This does not represent clearly enough the SSC view. The SSC view is firmly that security alerts should not be throttled or discarded. The notes from the Working Group 2 show: "An SSC member raised concern over the alert types being throttled in the Working Group meeting, citing security implications. The Working Group took note of these concerns and

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			highlighted in the drafted Business Requirements where this had been taken into account and would be consulted over with the rest of the Working Group." I request that the entry for the Sub-Committee views be amended to: **"Sub-Committee views** The Security Sub-Committee (SSC) chairman was on the Working Group and attended one of the meetings when the business requirements were being formulated. The view provided on behalf of the SSC was that security alerts should not be restricted. A solution could be supported where a list of exempted security-related Alerts that will not be subject to throttling or subject to a different level of throttling can be approved by the SSC and for SSC to receive regular reports**."**
Northern Powergrid	Electricity Network Party	Reject	We wholeheartedly support the intent of the modification proposal; however we are concerned that the proposed solution may only filter out some, but not all, nuisance alerts. Our concern is partly based upon: • The initial configuration parameters included in the Modification Proposal. If these parameters were to be adopted then, at a device level, three nuisance alerts every two minutes could be generated by rogue devices without then being discarded. • If our understanding is correct then, a rogue device could generate 2,160 nuisance alerts per day (3x30x24) without them being discarded. At this rate, across a population of say 1,000 meter sets this would see a User Party receiving over 2 million nuisance alerts per day. • The modification does not identify or address what we believe to be the root cause of nuisance alerts. We believe that the primary driver behind nuisance alerts is that device sets that haven't been tested with sufficient rigour before being deployed into the DCC's production environment. We note, for example, that no devices have

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			yet passed all SMDA tests. In this context we consider it likely that device sets will continue to be deployed in the DCC production environment that will generate significant volumes of nuisance alerts. • If the 'active notification being given to Users when the Alerts are being controlled' is undertaken on a per device basis, or is somehow based upon the number of nuisance alerts being discarded, then a very 'chatty' device set cohort could generate an enormous volume of incidents for Users or the DCC to manage, which could act as an unwelcome distraction from the day-to-day operation of their respective businesses. Our view therefore, is that any solution that is implemented should: • Through a SEC modification or similar industry change, mandate those parties responsible for bringing new device sets into the DCC production environment to undertake more rigorous testing of such device sets prior to their deployment, and provide an evidence based affirmation outlining why they believe such sets are fit for such deployment. If an alert 'filtering' / discarding solution is employed then it should: • Be capable of filtering out the 8014/8015 Power Factor alerts (the nuisance alerts that thus far have been the most problematic for DNOs and against which the DNOs will assess the suitability of any proposed solution). The initial configuration parameters of the proposed solution may not filter out the 8014/8015s that are currently causing problems for DNOs. • Generate an output for User Parties, perhaps via report or another form of management information, which provides an easy to consume view of device sets (manufacturer/model/firmware combinations) generating high volumes nuisance

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			alerts. In tandem with this a complementary report could also be provided that provides details of the remediation progress of responsible parties. With regards to alert 'filtering' and/or discarding, we are mindful that this proposal runs counter to the idea that the DCC is, at its heart, a message processing, execution and transmission organisation, and that it does not interfere with or otherwise manipulate message delivery. This view, that the DCC is primarily a message delivery service, is an idea that the DCC has itself emphasised in the past. If a message filtering precedent is therefore established via this, or any other SEC modification proposal, it is important that strong governance and oversight arrangements are put in place to ensure that filtering is only ever used where it is in the best interests of all relevant stakeholders, especially energy consumers.
Npower	Large Supplier	Approve	We support the proposers views and believe that this change to the SEC will reduce the likelihood of DCC overload due to alert storms.
Scottish Power	Large Supplier	Neutral	While we would welcome the beneficial effects of implementing SECMP0062, we are very concerned about projected costs that appear to us as excessive. Moreover, we note that the SECMP0062 solution would effectively deliver a level of functionality that Users were already given to expect of the DCC's basic design. Therefore, we are of the view that the costs to implement should already have been factored into the DCC's business plan and that there should be no question of these costs now being passed on separately to the DCC's Users. At high volumes, alert storms have a detrimental impact on User system performance and server capacity. They have been consistently highlighted as an issue, ever since the DCC UIT-A network was first brought down by a small number of alerting devices circa two years ago.

Question 1			
Respondent	**Category**	**Response**	**Rationale**
			While this traffic management solution does not address the root cause, it will at least help to buffer User systems from potentially large volumes of nuisance alerts and alerting behaviour until an enduring solution can be put in place. As such we agree that this modification broadly supports General SEC Objectives (a) and (f). However, we note that the solution only mitigates the problem of alert storms when such messages are at the point of delivery to the DSP. We would assume, then, that the volume of messages is likely to remain high for the CSP and, unless further measures were to be taken, could once again become problematic over time. Therefore, while we are very concerned about the costs of SECMP0062, these concerns are compounded by the risk that SECMP0062 may not represent an effective long term solution.

Question 2: Please provide any further comments you may have

Question 2		
Respondent	**Category**	**Comments**
Western Power Distribution	Electricity Network Party	
EDF Energy	Large Supplier	
Electricity North West Limited	Electricity Network Party	The main reason for rejecting the proposal is primarily it does nothing to mitigate a major issue which is currently affecting DCC and Users alike. An alternative solution could be for DCC to identify the manufacturer/model/firmware variants of meters which are causing alert storms and then agree with each individual Users as to whether they wish to either fully suppress particular type of alerts or let 1 in 'n' alerts through. e.g. they could ask DNO's do you want the 8014/8015 alerts from manufacturer/model/firmware = 'X' and we would decline because we know they originate from a non-compliant device.
SSEN	Electricity Network Party	SSEN as previously stated, are concerened that this implementation approach does not address the root cause of the alert storms issue. Based on the volumes and time periods proposed in this consultation, we agree this will supress some alerts. However, based on the current rate of Power Factor alerts we receive, it is estimated that we will still receive large volumes of alerts daily. Due to this we are unable to support this SEC Mod.
Security Sub-Committee	Other Respondent	
Northern Powergrid	Electricity Network Party	We have no further comments.

Question 2		
Respondent	**Category**	**Comments**
Npower	Large Supplier	An improvement to this proposal would have been to enable user specific configuration. By not having user specific configuration, controls can't be put in place that meet the specific needs of suppliers who may use differing configuration on the devices, or who may want to see differing levels of alert volumes.
Scottish Power	Large Supplier	We note that the 8f3e alerts from the GPF are only an issue for the Telefonica hubs. The defect on the EDMI hub where no 8f3e are generated by that hub will not be implemented due to loss of connection when the fix is in place. We think this lack of consistency in how the three hubs implement the 8f3e specification is something that needs to be addressed in the longer term; perhaps through a solution that manages the throughput of such alerts at the CH itself.