Data Communications Company

DCC Performance Measurement Report

Performance Measurement Period:

March 2021

Version:	**V1.0**
Date:	**10/05/2021**
Security Classification:	**DCC Controlled – Panel, Ofgem, BEIS and SEC Parties Only**

Table of Contents

Control Sheet **6**
1 Introduction **7**
1.1 Purpose **7**
1.2 Content **7**
1.3 Scope **8**
1.4 Confidential Information **8**
2 Executive Summary **9**
3 Code Performance Measures **16**
3.1 Service Levels Attained **16**
3.1.1 CPM1 – PM2 Volumes Data **21**
3.1.2 Service Level below Minimum – CPM1 ..... **22**
3.1.3 Category 1 and 2 Incident Resolution – CPM4 ..... **25**
3.1.4 Category 3, 4 and 5 Incident Resolution - CPM5 ..... **26**
3.1.5 CPM4 and CPM5 – Incidents Re-Opened after Closure **26**
3.1.6 Incident Resolution Information – CPM 4 & 5 ..... **26**
3.2 Performance Level Exemptions **30**
3.2.1 CPM4/5 - Incidents which the DCC is responsible for resolving and are resolved in accordance with the Incident Management Policy within the Target Resolution Time. **30**
4 Reported List of Service Provider Performance Measures DSP **32**
4.1 Service Levels Attained **32**
4.1.1 Service Level Below Target Service Level **33**
4.2 Performance Measurement Exceptions **33**
5 Reported List of Service Provider Performance Measures CSP North **34**
5.1 Service Levels Attained **34**
5.2 Performance Measurement Exceptions **36**
5.2.1 In Period Exceptions **36**
5.2.1.1 PM1.4 SMWAN Connectivity Level **36**
5.2.2 Total Estate Exceptions **37**
6 Reported List of Service Provider Performance Measures CSP Central **38**
6.1 Service Levels Attained **38**
6.1.1 Service Level Below Target Service Level **40**
6.2 Performance Measurement Exceptions **40**
6.2.1 In Period Exceptions **40**

6.2.1.1 PM1.1 First Time SMWAN Connectivity 40
6.2.1.2 PM11 Accuracy of Coverage Database 41
6.2.2 Total Estate Exceptions 42
6.2.2.1 PM1.3 SMWAN Connectivity Level 42
7 Reported List of Service Provider Performance Measures CSP South 43
7.1 Service Levels Attained 43
7.2 Performance Measurement Exceptions 45
7.2.1 In Period Exceptions 45
7.2.1.1 PM1.1 First Time SMWAN Connectivity 45
7.2.1.2 PM11 Accuracy of Coverage Database 46
7.2.2 Total Estate Exceptions 47
7.2.2.1 PM1.3 SMWAN Connectivity Level 47
8 Reported List of Service Provider Performance Measures S1SP SIE 48
8.1 Service Levels Attained 48
8.2 Performance Measurement Exceptions 48
9 Reported List of Service Provider Performance Measures S1SP Capgemini 49
9.1 Service Levels Attained 49
9.1.1 Service Level Below Target Service Level 49
9.2 Performance Measurement Exceptions 50
10 Reported List of Service Provider Performance Measures S1SP Vodafone. 51
10.1 Service Levels Attained 51
10.1.1 Service Level Below Minimum Service Level 51
10.2 Performance Measurement Exceptions 51
11 Reported List of Service Provider Performance Measures S1SP Critical Software 52
11.1 Service Levels Attained 52
11.2 Performance Measurement Exceptions 52
12 Reported List of Service Provider Performance Measures S1SP Morrison Data Services (MDS) 53
12.1 Service Levels Attained 53
12.2 Performance Measurement Exceptions 53
13 Reported List of Service Provider Performance Measures S1SP Secure 54
13.1 Service Levels Attained 54
13.2 Performance Measurement Exceptions 54
14 Service Credits 55
15 DCC's Internal Costs and/or External Cost 56

16 Appendices 57
16.1 Appendix A – Open Problem & Incidents relating to Prior Periods 57
16.1.1 PBI000000116812 57
16.1.2 PBI000000117240 58
16.1.3 PBI000000120410 59
16.1.4 PBI000000121400 59
16.1.5 PBI000000121900 60
16.1.6 PBI000000121704 60
16.1.7 PBI000000121926 61
16.1.8 PBI000000121821 61
16.1.9 PBI000000122005 62
16.1.10 PBI000000122516 62
16.1.11 PBI000000122229 63
16.1.12 PBI000000122418 64
16.1.13 PBI000000122422 64
16.1.14 PBI000000122520 65
16.1.15 PBI000000122415 65
16.1.16 PBI000000122237 66
16.2 Appendix B – Performance Measure Exception Definitions 67
16.2.1 CSPN 67
16.2.2 CSPC & CSPS 67
16.3 **Appendix C - Incident Reports Glossary** 69

Control Sheet

Table below details all enduring changes made to the report this month.

Page/ Section	Change

1 Introduction

1.1 Purpose

The Smart Energy Code (SEC) sets out the operational Service Levels which DCC needs to meet when providing services to DCC Users. This report provides details of the Service Levels achieved in respect of the Code Performance Measures set out in Sections H13.1 and L8.6 of the SEC and such Service Provider Performance Measures as are specified in the Reported List of Service Provider Performance Measures document[1].

Service Levels are reported following the end of each calendar month and this report is provided within 25 working days following the end of each calendar month.

This report is provided to the Panel, SEC Parties, the Authority and (on request) the Secretary of State.

1.2 Content

A Target Service Level and Minimum Service Level apply to each of the Code Performance Measures and to the Service Provider Performance Measures in the Reported List of Service Provider Performance Measures[2]. This report sets out the Service Levels achieved in respect of each Performance Measure[3].

Where the Service Level achieved for a Performance Measure is less than the Target and/ or Minimum Service Level, the report provides the reasons for this. Where the Service Level achieved is less than the Minimum Service Level the report also outlines the mitigating actions DCC is taking to prevent re-occurrence.

Where the Service Level achieved is less than the Target Service Level, Service Points are accrued by the DCC Service Provider. Service Points are then converted into Service Credits (monetary amount). Any Service Credits due from the DCC Service Provider are treated as a reduction in their charges and may be reflected in a reduction in DCC's Internal Costs and/ or External Costs. The method for calculating Service Points and Service Credits is detailed in the DCC Service Provider contracts in Schedule 2.2.

[1] The Reported List of Service Provider Performance Measures document was provided 18th December 2015 to Parties, the Panel and the Authority by the Secretary of State and identifies itself as being produced for the purposes of Section H13; it can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures.
[2] The Target and Minimum Service Levels are defined in Sections H13.1 and L8.6 of the SEC and in the Reported List of Service Provider Performance Measures document.
[3] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

1.3 Scope

This document reports on the performance of the DCC Service against the Performance Measures for March 2021.

1.4 Confidential Information

This report is classified as DCC Controlled in accordance with the confidentiality provisions under Section M of the SEC. Where the Service Level achieved is below the Target / Minimum Service Level and the reasons for this or the mitigating actions being taken by DCC are classified as DCC Confidential, this shall be reported in an annex to this report which shall be available on request.

2 Executive Summary

The historical February 2021 performance for CSPC and CSPS CH PM1.1 Percentage of Communications Hubs delivered on time has been changed to reflect recalculated performance amendments made in 202102_DCCPerformanceMeasurementReport_V2.0 issued on 10/05/2021.

Code Performance Measure (CPM) Summary

CPM1 measures Percentage of On-Demand Service Responses delivered within the applicable Target Response Time, the Service Level achieved is 92.75% and is below the Minimum Service Level, further details provided in Section 3.1.2.

The Service Levels achieved for CPM2, CPM3, CPM4, CPM5, CPM6, CPM7 and CPM8 are all above the Target Service Level.

Service Provider Performance Measures Summary

DSP PM2.7 Percentage Service availability - Externally exposed test services (08.00 to 20.00 UTC Monday to Saturday) , reported Service Level is 98.56% and is below the Target Service Level.
Further Details are provided in Section 4.1.1

CSPC PM CH1.3 Percentage of Communications Hubs determined not to be faulty following attempted installation, reported Service Level is 99.896% and is below the Target Service Level.
Further Details are provided in Section 6.1.2

S1SP-CapGemini PM2.1 Percentage Service availability – DCO Service (Production Environment) Service Level is 99.84% and is below the Target Service Level.
Further Details are provided in Section 9.1.1

S1CSP - Vodafone Monthly IoT Core availability (Voice/Data/SMS) reported Service Level was 99.85% and is below the Minimum Service Level. Further Details are provided in Section 10.1.1

Where the Performance Measure is reportable, all other Service Provider Performance Measures are above the Target Service Level.

Any Service Credits accrued for this measurement period are detailed in Section 14 of the report.

Key Incidents

Included Incidents

Incident Reference	INC000000697994
Problem Reference	PBI000000122516
Category	1
Service(s) Impacted	I&C, FW management, Read Requests, Certificate Rotations (21,773 SRV's and 164 Install and Commissions DCC TOC Data)
Service impacted date/time	25/02/2021 12:47
Service restored date/time	25/02/2021 13:50
Incident raised date/time	25/02/2021 13:05
Incident resolved date/time	25/02/2021 14:43
Actual Impact Duration	1hrs 3 Minutes
Incident Duration	1hrs 38 Minutes
Impacted Region	CSP North
Was the Incident prioritised correctly?	Incident initially came in as a Category 2 but was escalated to a Category 1 when it was confirmed total loss
Resolved within SLA	**Yes**

Summary of Incident

At 12:47 CSP North started to see a degradation in service within their infrastructure which when attempting to deliver traffic Northbound to the DSP. At 12:58 they experienced a total outage until 13:50.

All Northbound responses to all SRV's were failing during this period. Impacts to I&C, FW management, Read Requests, Certificate Rotations. All Southbound traffic (from DSP to CSP was received and processed correctly. Due to the short period of the outage, any SRV's with a DSP retry of longer than 15 minutes will be automatically picked up by the retry mechanism.
Additional conversation with DSP indicates impact to I&C may be an additional 45 minutes on the install from 1pm

Customer Impact

4 Service Users reported Install and Commission issues after the Major Incident was raised.

Actions Completed to Recover Service

Item	Description	Owner
1	CRL (Cert Revocation List) expired at 12:02 which held existing connections but did not allow new connections, when new CRL was applied at 12:25 which didn't activate until 13:50 when full service was restored. It was identified this was caused by multi browser issue when applying the new CRL. Monitoring has been put in place to confirm that CRL's are in situ and active once replaced.	DSP

Incident Reference	INC000000698821
Problem Reference	PBI000000122229
Category	2
Service(s) Impacted	Single DNO User
Service impacted date/time	27/02/2021 17:20
Service restored date/time	27/02/2021 21:46
Incident raised date/time	27/02/2021 17:17
Incident resolved date/time	28/02/2021 11:27
Actual Impact Duration	4hrs 26mins
Incident Duration	18hrs 10mins
Impacted Region	All
Was the Incident prioritised correctly?	Initially a Category 3 became Category 2 when all traffic stopped
Resolved within SLA	**Yes**

Summary of Incident		
Single DNO identified issues with receiving traffic from the DSP. Single DNO highlighted that they had moved to DUIS 4, DSP were unaware of this change. DSP investigated this issue and found that the MGN (Management Gateway North) had not been configured correctly to support DUIS 4. Once the configuration was updated at the DSP the traffic was seen to flow. All alerts/responses were queued and resent when the connection was restored.		
Customer Impact		
This would have impacted the single DNO's ability to receive traffic including AD1 alerts. AD1 alerts are classed as critical to DNOs.		
Actions Completed to Recover Service		
Item	Description	Owner
1	DSP reconfigured MGN (Management Gateway North) to DUIS 4 traffic. Incorrect IP address and port found. The DSP were receiving traffic, and this was being passed to devices. Root Cause was established during the course of the Major Incident; When the Service User upgraded their adaptor to DUIS 4, DSP were unaware of this change, and the DSP infrastructure was not configured to support DUIS 4.	DSP

Incident Reference	INC000000702177
Problem Reference	PBI000000122418
Category	2
Service(s) Impacted	Degradation to Install and Commission
Service impacted date/time	10/03/2021 08:20
Service restored date/time	10/03/2021 10:51 Impact mitigated
Incident raised date/time	10/03/2021 09:16
Incident resolved date/time	10/03/2021 19:07
Actual Impact Duration	2hrs 31 minutes
Incident Duration	9hrs 51 minutes
Impacted Region	CSP North
Was the Incident prioritised correctly?	Original ticket came in as a Category 3 but was escalated to a Category 2 due to the degradation seen by industry, DCC TOC and Arqiva on the I&C activity.
Resolved within SLA	**Yes**
Summary of Incident	
At 09:16 Multiple Service Users reported issues with Install and Commission and an increase in E20 alerts being received in the CSP North region for SMETS2, this was initially logged as a Category 3. Category 2 was declared at 10:09 with Investigating comms being distributed to the DCC Service Centre at 10:12. DCC Major Incident bridge was stood up at 10:15 with Arqiva to discuss the initial investigations. At this point Arqiva confirmed they can see an issue but need more time to set up an internal bridge with their 3rd/4th line and their Vendor. At 10:51 impact was mitigated following a failover from Route Manager 1 to Route Manager 2, even though this failover occurred, and Service Levels returned to with tolerance Arqiva continued to investigate as performance was slightly below baseline levels when running on Route Manager 1.	
Customer Impact	
Multiple Service Users reported failures in the North when trying to Install and Commission. Although some I&C's were still happening the majority were delayed/failing. Arqiva to confirm their stance on the CH activity following their internal triage/review – Difficult to confirm as the messages would have been dropped (Hardware reset to resolve) – DCC TOC to confirm numbers impacted between (08:20 started to see an impact) 09:00 and 10:51. Root Cause was confirmed as a configuration issue which was further compounded by a lack of memory. Memory has been increased to mitigate future impact.	

Actions Completed to Recover Service		
Item	Description	Owner
1	Failed over to Route Manager 2	CSP North

Incident Reference	INC000000702810
Problem Reference	PBI000000122418
Category	2
Service(s) Impacted	Degradation to Install and Commission
Service impacted date/time	11/03/2021 08:33
Service restored date/time	11/03/2021 09:30
Incident raised date/time	11/03/2021 09:40
Incident resolved date/time	11/03/2021 16:42
Actual Impact Duration	57 minutes
Incident Duration	7hrs 2 minutes
Impacted Region	CSP North
Was the Incident prioritised correctly?	Yes
Resolved within SLA	**Yes**

Summary of Incident
At 09:10 CSP North requested a call back from the DCC Incident Management team as they had observed a significant increase in E20 alerts being received in the CSP North region for SMETS2. DCC TOC had also identified an issue with low installs at the same time Arqiva confirmed they could see the same issue as INC000000702177 the previous day, and that Route Manager 1 had come back into service. The affected server was removed from service at 09:07. At 09:30 E20 errors subsided and impact was mitigated. With Service Levels returned to with tolerance Arqiva continued to investigate as performance was slightly below baseline levels when running on Route Manager 1.
Customer Impact
Multiple Service Users reported failures in the North when trying to Install and Commission. Although some I&C's were still happening the majority were delayed/failing. Root Cause was confirmed as a configuration issue which was further compounded by a lack of memory. Memory has been increased to mitigate future impact.

Actions Completed to Recover Service		
Item	Description	Owner
1	Failed over to Route Manager 2	CSP North

Incident Reference	INC000000707890
Problem Reference	PBI000000122422
Category	1
Service(s) Impacted	All SMETS 1 SRs
Service impacted date/time	23/03/2021 13:52
Service restored date/time	23/03/2021 15:01
Incident raised date/time	23/03/2021 14:34
Incident resolved date/time	24/03/2021 08:54
Actual Impact Duration	1 Hour 9 Mins
Incident Duration	18 Hours 20 Mins
Impacted Region	All
Was the Incident prioritised correctly?	Yes
Resolved within SLA	**Yes**

Summary of Incident
At 13:52 there was a database server cluster failure within in DCO's infrastructure resulting in a loss of capability to deliver any SMETS1 traffic (100% failure) this would have meant that SMETS1 migrations would not be able to be completed. However, no migrations were planned for the day. A DNO notified the DCC Service Centre at 14:29 and ticket was raised in remedy. DCC TOC and DSP also notified DCC Major Incident Management of the outage observed. DCO restarted their database cluster, which completed at 15:01 restoring service. The root cause could not be determined, therefore DCO engaged their vendor who are currently performing root cause analysis.
Customer Impact
For the duration of the outage Service Users would not have been able to successfully send or receive any traffic across the SMETS1 Estate. SMETS1 Migrations would not have been able to be undertaken. Due to the root cause being unknown the High Impact Release window due on the night of 23/03/2021 had to be postponed. Root Cause investigations have identified that this was an application failure within DCO's vendors hosting platform.

Actions Completed to Recover Service		
Item	Description	Owner
1	Restart of the Database cluster (all 4 elements)	DCO
2	Re enable of replication services	DCO

Excluded Incidents

Non DCC Service Impacting

Incident Reference	INC000000701200
Problem Reference	PBI000000122520
Category	2
Service(s) Impacted	DCC Internal: Global Protect authorisation (Multi-Factor Authentication [MFA])
Service impacted date/time	07/03/2021 15:27
Service restored date/time	08/03/2021 10:45
Incident raised date/time	07/03/2021 15:50
Incident resolved date/time	08/03/2021 13:45
Actual Impact Duration	19 hours 13 minutes
Incident Duration	21 hours 35 minutes
Impacted Region	DCC Internal
Was the Incident prioritised correctly?	Yes . Multiple users were unable to access key services.
Resolved within SLA	**Yes**

Summary of Incident
On 07/03/2021 some DCC users received authentication errors when their laptops attempted to access the DCC VPN. DCC TOC escalated the issue directly to the DCC On-Call Incident Manager (IM) at 15:30, who tested the connectivity and then engaged DCC Service Centre (SC). At this point some users were still able to access key services (including Remedy), but there were multiple reports of users having access issues and a Category 2 incident was raised. DCC Incident Management were unable to find a DCC escalation point for this issue and attempted to escalate directly to the Director of EIT (voicemail left), before escalating to the Capita on-call Major Incident Manager (MIM) in case there was any form of ancillary support. The Capita on-call MIM advised that there was no escalation path for issues of this type, but they would pass the call on to their technical teams in case they managed to uncover anything. At 8am on 08/03/2021 the DCC EIT Director confirmed acknowledgement of the issue and after a brief investigation confirmed the issue to be with the Multi-Factor Authentication (MFA) service, which is managed by Capita.

After liaising with Capita, the MFA configurations for the affected users were bypassed and service was restored. At 10:45 users confirmed they were able to access services via VPN and the incident was set to Resolved.
Customer Impact
Approximately 200 users were unable to access services requiring DCC VPN access, including: • Remedy • SSMI • Database Services (DCC TOC)

Actions Completed to Recover Service		
Item	Description	Owner
1	DCC/Capita amended conditional access policy (DCC017) so that they did not need to be on a trusted site to verify the MFA credentials.	Capita IT

Non DCC Service Impacting

Incident Reference	INC000000701348
Problem Reference	PBI000000122415
Category	2
Service(s) Impacted	DCC Internal: Internet-based services access
Service impacted date/time	08/03/2021 10:45 (Capita start time 10:52)
Service restored date/time	08/03/2021 15:15
Incident raised date/time	08/03/2021 13:08
Incident resolved date/time	09/03/2021 15:06
Actual Impact Duration	4 hours 30 mins
Incident Duration	25 hours 58 minutes
Impacted Region	DCC Internal
Was the Incident prioritised correctly?	Yes – Multiple users were unable to access key services.
Resolved within SLA	**Yes**

Summary of Incident
Following on from the resolution of Category 2 incident INC000000701200, a number of users responded to the resolution comms, stating that they were still unable to access key services. A review of the affected services indicated that, while access to VPN-based services was possible, access to any internet-based service or websites was not possible. Capita IT Services were engaged and confirmed that there was a multi-client major incident in process under Capita reference INC000007225905 [P1]. Service was restored following a reboot of a Capita Area Border Router (ABR) device and confirmed by DCC Incident Management at 15:15.
Customer Impact
Multiple DCC users were unable to access any external internet-based services, including: • Okta • Clarity • Workday No impact to DCC Service Users or SEC Parties

Actions Completed to Recover Service		
Item	Description	Owner
1	Partial service restored following action to bypass the affected nodes	Capita IT
2	Capita IT rebooted ABR device	Capita IT

Non DCC Service Impacting

Incident Reference	INC000000708834
Problem Reference	PBI000000122237
Category	1
Service(s) Impacted	Web-based services, such as Remedy, SharePoint and SSMI. Avaya (telephony service) unavailable. Degraded access to Microsoft Applications (Outlook, Teams)
Service impacted date/time	25/03/2021 11:15
Service restored date/time	25/03/2021 12:34
Incident raised date/time	25/03/2021 13:40
Incident resolved date/time	25/03/2021 16:13
Actual Impact Duration	1 hour 19 minutes
Incident Duration	4 hours 58 minutes
Impacted Region	N/A
Was the Incident prioritised correctly?	**Yes** . Multiple business-critical services were unavailable.
Resolved within SLA	**Yes**

Summary of Incident

A Capita-wide network issue arose, impacting all Azure-destined traffic in the primary Telehouse North (THN) datacentre. This impacted multiple key services for DCC, including the primary CRM solution (Remedy), telephony systems (Avaya) and other web-based services.

Capita Networks Services (CNS) failed service over to the Secondary Telecity Power (TCP) datacentre at 12:34 and service was restored.

Customer Impact

DCC Staff were unable to access business-critical applications, including Remedy, SSMI and SharePoint. Access to Microsoft Applications, including Outlook and Teams was also impacted, with users reporting intermittent service degradation for the duration of the incident.
An associated ticket (INC000000708773) was raised by the DCC SMETS1 Requesting Party, Secure, who reported FTP Client Errors on Test and Prod Environments.

Actions Completed to Recover Service

Item	Description	Owner
1	Service was routed via TCP at 12:34 – Service Restoration	Capita IT
2	THN was reloaded at 16:45 25/03 and service failed back to THN at 17:30 – Incident Resolution	Capita IT

3 Code Performance Measures

3.1 Service Levels Attained

This section reports the Service Levels achieved in March 2021 against the targets specified in Sections H13.1 and L8.6 of the SEC.

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
CPM1	**Percentage of On-Demand Service Responses delivered within the applicable Target Response Time.**			**93.95%**	**92.75%**	**99.00%**	**96.00%**
	PM1.1	Percentage of DSP Service Request Times within relevant TRT	DSP	99.91%	99.83%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP SIE	99.98%	99.36%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP Capgemini	100.00%	99.98%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP Secure	99.81%	99.31%	99.00%	96.00%
	PM1.1	Percentage S1SP Countersigned Service Request Times within relevant Target Response Time	S1SP DXC	N/A	No Events	99.00%	96.00%
	PM1.4	Percentage of DCC Service Request Times within relevant TRT	DSP	99.98%	99.98%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPN	35.88%	23.74%	99.00%	96.00%
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPC	99.02%	99.17%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM2	Percentage of Category 1 Firmware Payloads completed within the relevant TRT	CSPS	99.18%	99.28%	99.00%	96.00%
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPN	100.00%	100.00%	85.00%	80.00%
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPC	99.86%	99.80%	96.00%	90.00%
	PM4.3	Round Trip Time 4 Test HAN Interface Command Time: percentage delivered within 25 seconds	CSPS	99.84%	99.81%	96.00%	90.00%
CPM2	**Percentage of Future-Dated Service Responses delivered within the applicable Target Response Time**.			**99.92%**	**99.91%**	**99.00%**	**96.00%**
	PM1.2	Percentage of DSP Service Response Times within relevant TRT	DSP	100.00%	99.98%	99.00%	96.00%
	PM1.3	Percentage of DSP Service Request Scheduling Times within relevant Target Response Time (as set out in Part C of this Appendix 1)	DSP	100.00%	100.00%	99.00%	96.00%
	PM3.1	Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPN	99.21%	99.19%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM3.1	Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPC	99.97%	99.98%	99.00%	96.00%
	PM3.1	Percentage of Category 2 HAN Interface Commands delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPS	99.96%	99.96%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPN	100.00%	100.00%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPC	100.00%	100.00%	99.00%	96.00%
	PM4.1	Round Trip Time 2 Test HAN Interface Command Time: percentage delivered within 22 hours	CSPS	100.00%	100.00%	99.00%	96.00%
	PM4.2	Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours	CSPN	100.00%	100.00%	99.00%	96.00%
	PM4.2	Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours	CSPC	99.99%	99.95%	99.00%	96.00%
	PM4.2	Round Trip Time 3 Test HAN Interface Command Time: percentage delivered within 2 hours	CSPS	99.99%	99.95%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
CPM3	**Percentage of Alerts delivered within the applicable Target Response Time.**			**99.71%**	**99.57%**	**99.00%**	**96.00%**
	PM1.5	Percentage of DSP Alert Response Times within relevant Target Response Time (as set out in Part C of this Appendix 1)	DSP	99.93%	99.93%	99.00%	96.00%
	PM1.5	Percentage of S1SP SMETS1 Alert Response Times within relevant Target Response Time	S1SP SIE	100.00%	99.77%	99.00%	96.00%
	PM1.5	Percentage of S1SP SMETS1 Alert Response Times within relevant Target Response Time	S1SP Secure	99.78%	99.62%	99.00%	96.00%
	PM1.5	Percentage of S1SP SMETS1 Alert Response Times within relevant Target Response Time	S1SP DXC	N/A	No Events	99.00%	96.00%
	PM3.2	Percentage of Category 3 Alerts delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPN	99.54%	99.22%	99.00%	96.00%
	PM3.2	Percentage of Category 3 Alerts delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPC	99.50%	99.52%	99.00%	96.00%
	PM3.2	Percentage of Category 3 Alerts delivered to the DCC WAN Gateway Interface within the relevant Target Response Time	CSPS	99.50%	99.37%	99.00%	96.00%
CPM4	**Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 1 or 2 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.**			**No Events**	**100.00%**	**100.00%**	**85.00%**

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
CPM5	**Percentage of Incidents which the DCC is responsible for resolving and which fall within Incident Category 3, 4 or 5 that are resolved in accordance with the Incident Management Policy within the Target Resolution Time.**			**90.11%**	**90.12%**	**90.00%**	**80.00%**
CPM6	**Percentage Availability – Self Service Interface**			**100.00%**	**99.95%**	**99.50%**	**98.00%**
	PM2.4	Percentage Service availability – Self Service Interface (Production Services)	DSP	100.00%	99.95%	99.50%	98.00%
CPM7	**Percentage of Certificates delivered within the applicable Target Response Time for the SMKI Services.**			**100.00%**	**100.00%**	**99.00%**	**96.00%**
	PM1.1	Batch requests for device certificates maximum 375,000 for RA system received 07:00-18:00 available by 06:59 next day	TSP	100.00%	100.00%	100.00%	95.00%
	PM1.4	Single certificate requests via RA System 100% within 30 seconds	TSP	100.00%	100.00%	100.00%	99.00%
	PM1.7	Single certificate request via system to system interface in Core Service Hours (maximum 12 certificate requests/second) 100% within 15 seconds	TSP	100.00%	100.00%	100.00%	99.00%
CPM8	**Percentage of documents stored on the SMKI repository delivered within the applicable Target Response Time for the SMKI Repository Service.**			**100.00%**	**100.00%**	**99.00%**	**96.00%**
	PM13	Percentage of documents stored on the SMKI Repository delivered within the applicable Target Response Time for the SMKI Repository Service.	DSP	100.00%	100.00%	99.00%	96.00%

Code Performance Measure Number	Performance Measure			Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	PM1.8	Processed certificate or binding is made available to PKI repository within 10 seconds	TSP	100.00%	100.00%	100.00%	99.00%

Table 1 - DCC Code Performance Measures

3.1.1 CPM1 – PM2 Volumes Data

	CSPN	CSPC	CSPS
Total number of Communications Hubs with Firmware Payload delivered successfully in Measurement Period	56,774	571,383	515,774
Total Number of Connected Communications Hubs identified in Service Requests to have Firmware Payload delivered within Measurement Period	239,128	576,139	519,490
Reported Percentage Performance	**23.74%**	**99.17%**	**99.28%**

Table 2 - DCC Code Performance Measures

3.1.2 Service Level below Minimum – CPM1

Percentage of On-Demand Service Responses delivered within the applicable Target Resolution Time

The Service Level reported for CPM1 is 92.75% and is below the Minimum Service Level.

CSPN PM2 reported Service Level was 23.74% and is below Minimum Service Level.

This Performance Measure has been failing since April 2018. Despite a number of CSPN lead action plans no improvement to service has been seen and performance against SLA is worse now that it was 12 months ago.

DCC are now taking a different approach to addressing this short fall in performance by engaging the Service Users, identifying the business issues this is causing and developing a Service Improvement Plan to significantly improve performance in 2021. The Service Users have told DCC that they want a service that is predictable, works first time and minimises the need for rework. A 'Fire and Forget' service.

The DCC and CSPN have developed two forward approaches:

- Tactical improvement plan.
- Enduring architecture uplift plan.

To note the delivery of the two plans will not deliver a PM2 service of 99% until summer 2022.

Tactical improvement plan

This plan contains 6 distinct actions to address business impact through to the end of summer 2021 in a staged release and is aimed at significantly improving performance as follows:

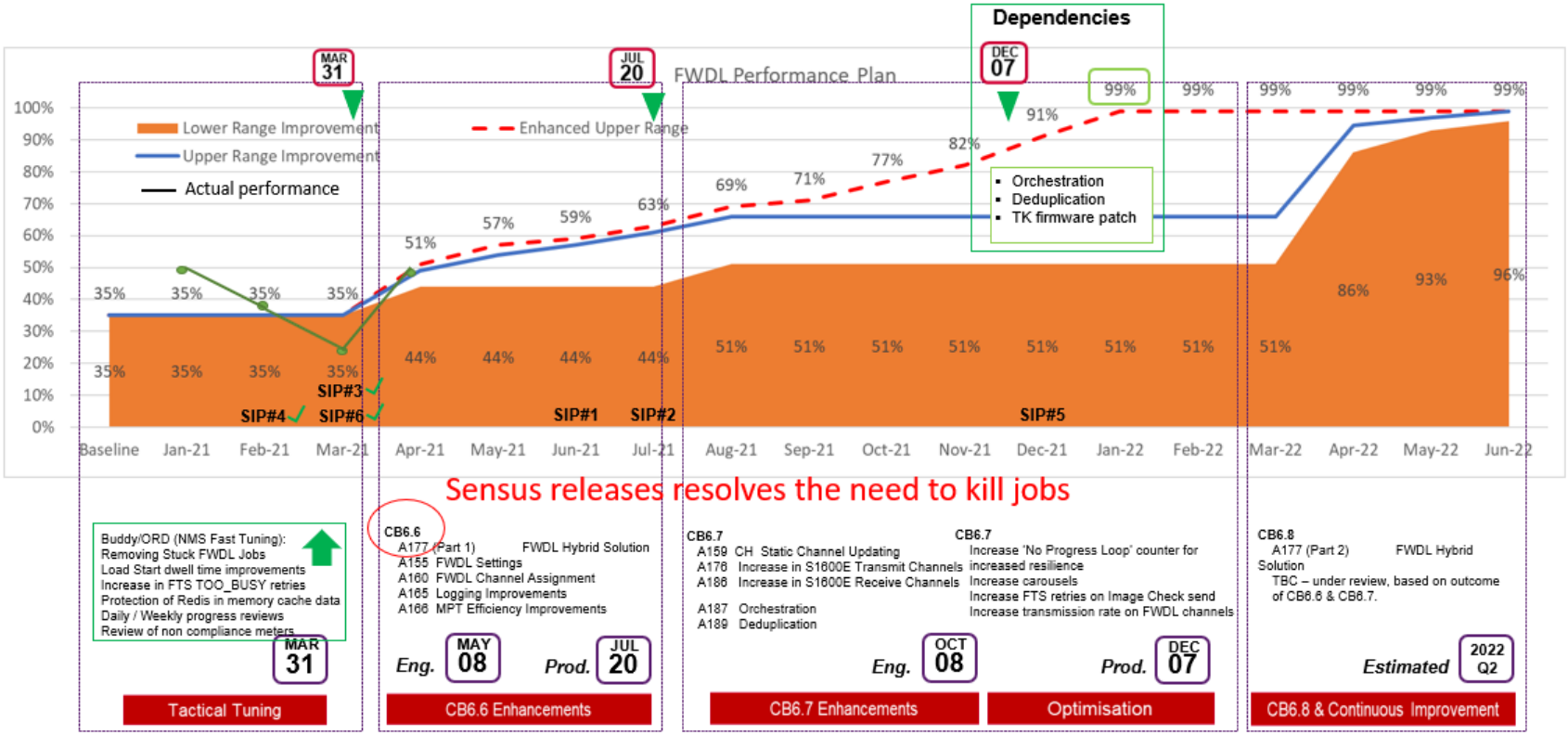
- Action 1 – Terminate jobs at 10 days not 5 (1 day DSP + 4 days CSP N)
- Action 2a – Increased Channels from 3 to 4 in November 2020. Completed. Now looking at Action 2b to which will increase Channels to 6
- Action 3 – Admin rate channels – Arqiva change with Sensus to utilise resource more efficiently
- Action 4 – Firmware passes – Reducing re-broadcasts from 5 to 2
- Action 5 – CSP N Meter OTA Batching solution
- Action 6 – Removal of stuck jobs in image check state ***New initiative***

Enduring Improvement Plan

The DCC and Arqiva have now developed the enduring plan with the aim to then deliver the PM2 performance at 99%. This plan has now been backed off by Sensus, Arriva's solutions partner, and will be delivered now by the end of this calendar year, 2021. The graph below shows the forward plan to deliver PM2 and the progress through 2021 against the plan. The Red dotted line is now the backed off and signed up plan to deliver against and the current performance will be plotted against it and shared with Industry.

FWDL Performance Plan – Target Enduring Plan

Timescales backed off and agreed with Sensus to deliver this year



Progress to Date

In November CSPN increased channel capacity by 33% by adding a 4th channel to its infrastructure. An uplift in SLA Performance was seen in December to 50%.

It was felt through modelling that the single biggest impact to performance would be to introduce a batching solution into the CSPN network solution, but a proof of concept trial was required, this was done in January with the support of industry. The trial came back to show an 86% success rates in those jobs that were batched. DCC, DSP and CSPN have now developed a batching solution that was presented to TABASC in March for assessment and sign-off was given, with a target for implementation in late 2021.

However, it must be noted that to create the environment for the batching trial we had to terminate a number of jobs and this action led to a drop in performance to 43% from the gains we had seen in December.

CSPN noted during the enhanced network monitoring through this period that there were a number of bad Communication Hubs that were getting stuck in the system. This was leading to many jobs becoming stuck behind these jobs and all of them would fail at the 5-day SLA limit. CSPN have developed a manual solution to selectively terminate these individual jobs thus freeing the many jobs queueing behind them. It was felt by these actions we would give many more jobs the chance to succeed within the 5-day SLA.

This was presented to SECOPS at beginning of March 2021 and was endorsed as an action to implement immediately and this has now happened.

In addition, CSPN have developed two configuration actions that will allow them to make more efficient use of the channels dealing with firmware downloads and remove a lot of noise from the network. SECOPS also endorsed the implementation of these two actions in the 3rd and 4th week of March.

It is believed these three actions will deliver a performance improvement from between 15% to 25%. We will not implement any further actions in April to baseline and monitor performance.

Action 1 has been put on hold to trial after we have proved the cumulative impact of actions 2a,6,3 and 4.

Action 2b continues to be developed for implementation later in 2021.

March Update

Tactical actions 3,4 and 6 were launched successfully in March. However, two major outages hit performance hard in March (INC000000702177 & INC000000702810, details in Section 2 Executive Summary). On both occasions these outages resulted in the system cache being dumped and all firmware jobs in those caches failed. This had a dramatic impact on performance, finishing the month on 23.48% which is extremely poor. We have identified the cache issue and process has now been changed so that this cannot happen going forward.

In addition to this, the implementation of daily monitoring and terminating stuck jobs, identifying issues has led to a full understanding of why this performance was achieved.

As a result of this, we have had a number of conversations with customers regarding the way their systems submit jobs, we have implemented terminating jobs twice daily 7 days a week and we are seeing the trend for April tracking performance against the enduring plan above.

Average duration times have come down in April and the results of the implemented actions are having a positive effect :

	March Average Duration (Hrs)	April* Average Duration (Hrs)
Meter	31	22
CH	110	39

Table 3 – CSPN PM2 FW Durations

* April Average Duration is as at 20/04/2021

We can see that the average for Meter FWDL requests in March is 31 hours, compared to 110 hours for a CH FWDL request.
CH image size is not quite double that of the average meter FW image.

The ongoing work on non-compliant installations, decommissioning of no-longer installed hubs, dealing with connectivity related issues and the implementation of action 6 (terminating stuck jobs) will increase performance in future months

3.1.3 Category 1 and 2 Incident Resolution – CPM4

For clarity please note, to ensure operations boards are furnished with the most recent information, data provided to them utilises the "Start Date". The PMR utilises the "Closed Date" as the formal service level performance on Incident Resolution can only be calculated on closure. This can result in discrepancies between operational reporting and contractual reporting in instances where Incidents are Opened in one month and Closed in another.

Incident Volumes – Closed in Measurement Period

CPM4 measures Incident resolution performance for Category 1 and 2 Incidents that were Closed in the Measurement Period. The table below illustrates how many of the Incidents were closed in the Measurement Period and of those, how many failed to meet the Service Level Requirements defined in the SEC.

Category	Total Incident Count	Within SLA	Failed SLA	% Within SLA
Category 1	2	2	0	100.00%
Category 2	3	3	0	100.00%
Total	**5**	**5**	**0**	**100.00%**

Table 4 - CPM4 Incident Count

For Information only: Prior to any Performance Measurement Exclusions Applied

Category	Total Incident Count	Within SLA	Failed SLA	% Within SLA
Category 1	3	3	0	100.00%
Category 2	5	5	0	100.00%
Total	**8**	**8**	**0**	**100.00%**

Table 5 – CPM4 Pre-PMEL Incident Count

3.1.4 Category 3, 4 and 5 Incident Resolution - CPM5

Incident Volumes – Closed in Measurement Period

CPM5 measures Incident resolution performance for Category 3, 4 and 5 Incidents that were Closed in the Measurement Period. The table below illustrates how many of the Incidents were closed in the Measurement Period and of those, how many failed to meet the Service Level Requirements defined in the SEC.

Category	Total Incident Count	Within SLA	Failed SLA	% Within SLA
Severity 3	111	108	3	**97.30%**
Severity 4	131	124	7	**94.66%**
Severity 5	649	571	78	**87.98%**
Total	**891**	**803**	**88**	**90.12%**

Table 6 - CPM5 Incident Count

3.1.5 CPM4 and CPM5 – Incidents Re-Opened after Closure

Where an incident that has been closed and their Service Level reported on in a previous period, and re-opened and Closed in this reporting period, the Service Level reported may be subject to change. The new Service Level will be documented below:

No Incidents Closed in this period have been re-opened and reported in a previous period.

3.1.6 Incident Resolution Information – CPM 4 & 5

For information only

Incident Volumes - Raised at any point in time and in a Resolved Status at the point of extract. (Point of Extract: 1st of the Month following the reporting period)

Category	Total Incident Count	Within SLA	Failed SLA	% Within SLA
Category 1	0	0	0	N/A
Category 2	1	1	0	100.00%
Total	**1**	**1**	**0**	**100.00%**

Table 7 - Incidents Relating to CPM4

Category	Total Incident Count	Within SLA	Failed SLA	% Within SLA
Severity 3	14	13	1	**92.86%**
Severity 4	13	11	2	**84.62%**
Severity 5	145	125	20	**86.21%**
Total	**172**	**149**	**23**	**86.63%**

Table 8 - Incidents Relating to CPM5

Incident Volumes assigned to Service Users – Tickets not Closed (Raised at any point in time - Point of Extract: 1st of the Month following the reporting period)

Category	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Total Incidents
2018 July					1	1
2018 August					12	12
2018 September					33	33
2018 October					47	47
2018 November					76	76
2018 December					120	120
2019 January					180	180
2019 February					182	182
2019 March					229	229
2019 April					212	212
2019 May					202	202
2019 June				1	329	330
2019 July				4	381	385
2019 August					468	468
2019 September					488	488
2019 October				1	785	786
2019 November				1	402	403
2019 December					586	586
2020 January				4	570	574
2020 February				3	818	821
2020 March				10	755	765
2020 April				3	244	247
2020 May				4	264	268
2020 June				2	435	437
2020 July				3	605	608
2020 August				5	789	794
2020 September				3	1,387	1,390

Category	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Total Incidents
2020 October			1	3	1,383	1,387
2020 November				21	1,401	1,422
2020 December			2	26	1,133	1,161
2021 January			1	22	1,643	1,666
2021 February				9	1,701	1,710
2021 March			23	12	2,442	2,477
Total			**27**	**137**	**20,303**	**20,467**

Table 9 - Aged Incidents Assigned to Service Users

Analysis of these aged incidents show that the top 3 issues are: -

Incorrect Communications Hub Variant Installed – 10,572
CSPs unable to communicate with a Communication Hub – 3,915
Service Users unable to communicate with a Communication Hub – 3,899

Enhanced attention to “Aged” Incidents has continued to see a decrease in the total. Further to simply resolving these “Aged” Incidents, if a resolution is not possible, actions are being taken to reclassify the specific action required from Service Users to resolve. This additional data quality will provide us with greater insight of what the DCC can influence in these Incidents. Many of these require a site visit to resolve, which is difficult within this current climate.

Specific attention has been placed on the Incidents raised prior to 2020. After seven consecutive months of large number of Incident reductions, the open Incidents from this period has plateaued. Fewer than 5,000 Incidents raised within that period. ~4000 of these appear to require a Site Visit to resolve the issue.

After extensive analysis on the “Incorrect Communications Hub Variant Installed” Incidents that have been raised, we agreed that we will only raise ‘Incorrect Variant’ Incidents for Gateway hubs. Meaning there is a dependency on the device being a Mesh CH to ensure the connecting properties can connect to the network. All of these require a site visit to resolve, which again, is difficult within this current climate.

A high volume of Incidents have been resolved; we are now able to focus on those that remain. These are varied in root causes, but ultimately are due to Non-Responsive Communication Hubs. Over time, we will identify the root causes in further detail as our investigation continue. Currently there is an even split between those raised by the CSPs and those raised by Service Users (predominately Network Operators).

Incident Volumes assigned to Service Providers or DCC Resolver Teams – Tickets not Closed (Raised at any point in time - Point of Extract: 1st of the Month following the reporting period)

Category	Cat 1	Cat 2	Cat 3	Cat 4	Cat 5	Total Incidents
2018 August					1	**1**
2018 September					1	**1**
2018 November					1	**1**
2018 December					11	**11**
2019 January					4	**4**
2019 February				1	4	**5**
2019 March					7	**7**
2019 April					18	**18**
2019 May					18	**18**
2019 June					14	**14**
2019 July					27	**27**
2019 August					70	**70**
2019 September					35	**35**
2019 October			1	1	115	**117**
2019 November				1	48	**49**
2019 December					28	**28**
2020 January				1	44	**45**
2020 February					54	**54**
2020 March					61	**61**
2020 April					59	**59**
2020 May					52	**52**
2020 June				2	67	**69**
2020 July				3	89	**92**
2020 August				1	82	**83**
2020 September				2	191	**193**
2020 October				2	165	**167**
2020 November			1		170	**171**
2020 December				5	189	**194**
2021 January			4	5	319	**328**
2021 February			6	6	293	**305**
2021 March			8	20	744	**772**
Total			**20**	**50**	**2,981**	**3,051**

Table 10 - Aged Incidents Assigned to Service Providers or DCC

DCC Incident Management have a process whereby the aged incidents are split into Service User and Service Provider. These are worked through daily to bring the number of aged incidents down. The majority of the actions in the previous section are also being applied to the Aged Incidents assigned to DCC and Service Providers.

The top types of Incidents that are assigned internally are:

- Unresponsive Devices – 1,565
- CSP Event Monitoring – 732
- Reboots - 349

We also saw a reduction of ~22% of Incidents over 90 days old. We will continue to focus on these Incidents, ensuring that lessons are learned from the Incidents that take much longer to resolve.

Similarly, to the Incidents assigned to Service Users, the majority of the Incidents are due to our inability to communicate with the Communication Hub. With the support of our Technical Operations Centre and Problem Management team, we are investigating the root causes of these issues. Whilst some are due to CHIPSM non-compliance, certificate management issues or meter defects, effectively restoring service to these devices remotely remains a challenge.

3.2 Performance Level Exemptions

In accordance with the Performance Measurement Methodology document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below.

No Service Providers requested exemptions this period.

3.2.1 CPM4/5 - Incidents which the DCC is responsible for resolving and are resolved in accordance with the Incident Management Policy within the Target Resolution Time.

Exception Type	Total Incidents
Incident Resolution Not DCC Responsibility - ADT Unsolicited SRV's	842
Incident Resolution Not DCC Responsibility	615
User Request - CH Reboot Request	351
Not DCC Resolution - 8.14.1 Not Received	67
Non DCC Service Impacting	54
Incident Resolution Not DCC Responsibility - PCO	24
User Request	1
Non DCC Resolution Total	1,954
Exclusion Type	**Total Incidents**
Alert / Event Monitoring (For Information only)	3,345
Cancelled	490
Duplicate	487

Exception Type	Total Incidents
SMETS1 Migration Related	22
Prod Proving	2
DCC Resolution Total	4,346
Grand Total	**6,300**

Table 11 - PMEL Exclusions Detail

Further Information on the above exclusions:

Incident Resolution Not DCC Responsibility:

These are predominately Incidents that were caused by CHIPSM non-compliance and required corrective action from Energy Suppliers, including but not limited to; Incorrect Credentials mentioned in Section 3.1.6

Incident Resolution Not DCC Responsibility - ADT Unsolicited SRV's:

Due to Anomaly Detection Threshold configuration, we received a high frequency of Incidents when a device acted erroneously. If said device acted in this way for a prolonged period, it would continuously generate Incidents. Many of these were due to the same event. Since this issue arose, DCC have spent significant time and engaged multiple internal resources to address the root cause. Developing new process and amending configuration items that now enable our Technical Operations Centre to perform precise trending analysis.

Incident Resolution Not DCC Responsibility – PCO:

These are Incidents raised against Energy Suppliers when they failed to fulfil their SEC-Mandated Post Commissioning Obligations and cause the device to be non-responsive to the DCC or any other Service User who attempts to communicated with it. Most notably, Network Operators.

User Request - CH Reboot Request:

Incident Management has been frequently used as a mechanism to reboot a Communication Hub. As these have fault declaration or triage performed prior to the Incident submission, these are effectively request fulfilment activities. Due to the urgency of these requests, Incident Management remains the preferred submission channel.

Cancelled:

Since their creation, both "Incorrect Credentials" raised by the Service Centre and "Incorrect Variant" Incidents have had their validity re-evaluated. These are deemed no longer required and have subsequently been cancelled. The majority of these exclusion would be categorised as one of these two Incident types.

Alert / Event Monitoring (For Information only):

This type of exclusion covers all proactively raised Incidents.

Duplicate:

Previously additional Incidents were needed to be created that could manage interactions between multiple Service Users. The second Incident that was created by the DCC Service Centre will be classified as a "Duplicate." Many of the aforementioned Anomaly Detection Incidents fall into this category.

4 Reported List of Service Provider Performance Measures DSP

4.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service availability – DCC Data Service	Monthly	100.00%	100.00%	99.95%	99.00%
	2.2	Service availability – DCC User Interface	Monthly	100.00%	100.00%	99.95%	99.00%
	2.3	Service availability – DCC Service Management	Monthly	100.00%	100.00%	99.50%	98.00%
	2.4	Service availability – Self Service Interface	Monthly	100.00%	99.95%	99.50%	98.00%
	2.5	Service availability – Average Interface (DCC Internal availability	Monthly	100.00%	100.00%	95.00%	90.00%
	2.7	Service availability - Test services	Monthly	100.00%	98.56%	99.00%	98.00%
Application Management	3	Category 1 or 2 Incidents directly related to a change release within 30 days of release*	Monthly	0	0	0	5
Anomaly Detection	11	Anomalous Service Requests	Monthly	No Events	No Events	99.00%	96.00%
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level Aug20 – Oct20	Latest Qtr. Service Level Nov20 – Jan21	Target Service Level	Minimum Service Level
Service Management	7	Notification of Planned Maintenance events**	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 12 - DSP Reportable Performance Measures

*DCC are reviewing the contractual definition of this DSP Performance Measure

**Measurement Period is a Calendar Quarter – current reported Quarter is Nov 2020 – Jan 2021. Previous Quarter is Aug 2020 – Oct 2020

4.1.1 Service Level Below Target Service Level

DSP PM2.7 reported Service Level was 98.56% and is below the Target Service Level.

This Service Level was impacted by an outage of 558 minutes to the UIT-B environment on 2 March 2021, caused by the accidental decommissioning of a network route by a 3rd party supplier (INC000000699464). The outage was picked-up immediately by DSP monitoring and the 3rd party engaged to restore service via the reinstallation of the circuit. Following a post-incident review, the 3rd party has revised their decommissioning processes to include additional cross-referencing of circuit identifiers. During this event, the UIT-A environment was unaffected.

4.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

5 Reported List of Service Provider Performance Measures CSP North

5.1 Service Levels Attained

*Performance Measures are reported monthly unless otherwise specified.

A Service Level entry of “No Events” indicates that although the Performance Measure is applicable, no relevant events occurred during the Measurement Period and there is therefore no data to report upon.

A Service Level entry of “Data Exempted” indicates that although relevant events occurred during the Measurement Period, all events were exempt from measurement as they were agreed to be an Allowed Exception or Exclusion.

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.1	First time SMWAN connectivity at install	Monthly	98.35%	98.93%	80.00%	70.00%
	1.2	First time SMWAN connectivity within 30 days	Monthly	99.82%	99.76%	90.00%	80.00%
	1.4	SMWAN connectivity Level	Monthly	100.00%	100.00%	99.90%	99.00%
Availability	6.2	Percentage availability of DCC WAN Gateway Interface	Monthly	100.00%	100.00%	99.98%	98.25%
Service Management	11	Accuracy of Coverage Database provided to DCC Service Users	Monthly	99.64%	99.40%	99.00%	95.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	99.41%	99.50%	99.00%	96.00%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	396.20%	394.28%	99.00%	96.00%
Communications Hub delivery	1.1	Percentage of Communications Hubs delivered on time	Monthly	100.00%	100.00%	99.00%	95.00%
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	100.00%	100.00%	99.90%	99.00%
	1.3	Percentage of Communications Hubs determined not to be faulty following attempted installation	Monthly	100.00%	100.00%	99.90%	99.50%
Communications Hub "Incidents"	2.1	Percentage of Communications Hub Incidents resolved by remote maintenance	Monthly	100.00%	100.00%	99.00%	95.00%
Performance Area	**Performance Measure Number**	**Performance Measure Name**	**Measurement Period**	**Previous Qtr. Service Level 2020 Q4**	**Latest Qtr. Service Level 2021 Q1**	**Target Service Level**	**Minimum Service Level**
Communications Hub Connectivity	1.3	First time SMWAN connectivity within 90 days	Quarterly	99.97%	99.98%	99.00%	95.00%
Service Management	10	Notification of Planned Maintenance events within required target[4]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 13 - CSPN Reportable Performance Measures

PM12.2 - The calculation results for PM 12.2 comes as 394.28%. CSPN had a total of 10,343 CH power outages reported, in March, and all were sent to DSP within SLA (100%).

The formula (below) as given in Schedule 2.2.

[4] Measurement Period is a Calendar Quarter

For Power Outage Events which detect Power Loss Alerts from between fifty (50) Communications Hubs and five thousand (5,000) Communications Hubs, the Contractor shall measure:

$$PM12.2 = 100\% \times \left(\frac{\text{Number of Power Outage Event alerts}}{((\text{Number of Communications Hub Power Loss Alerts} - 50) \times 0.25) + 50} \right)$$

Using the calculation above PM12.2 = 100 * (10343/ ((10343 – 50) * 0.25) + 50) = 394.28%

5.2 Performance Measurement Exceptions

In accordance with the Performance Measurement Methodology[5] document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below. These Comms Hubs are in alignment with the SECAS Issues Log. Where user behaviour has been identified as the reason for the exclusions, DCC are facilitating work between the CSP and Service user/s to address these.

5.2.1 In Period Exceptions

5.2.1.1 PM1.4 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.4 (CSPN)	22,152	Failure to follow maintenance as per CHIMSM	These figures are for the reporting period (not cumulative)

Table 14 - CSPN PM1.4 Exclusions

22,152 x CH excluded for March 2021 due to several reasons^, covering: -

[5] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

^CSPN Performance Measures Exceptions Classification Definitions can be found in Section 16.2 Appendix B, Sub-section 16.2.1

- Communications Hubs where no incident has been raised for outage – 14,592
- Incomplete Communications Hub Install – 7,521
- Part of first 1,000 DBCH to be excluded for contractual reasons – 30
- Not Active – 7
- Communication Hub installed on non-consumer premises i.e. Live Labs – 2

5.2.2 Total Estate Exceptions

No events or periods of time were identified as an Allowed Exception

- No total estate exceptions

6 Reported List of Service Provider Performance Measures CSP Central

6.1 Service Levels Attained

A Service Level entry of “No Events” indicates that although the Performance Measure is applicable, no relevant events occurred during the Measurement Period and there is therefore no data to report upon.

A Service Level entry of “Data Exempted” indicates that although relevant events occurred during the Measurement Period, all events were exempt from measurement as they were agreed to be an Allowed Exception or Exclusion.

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.1	First time SMWAN connectivity at install	Monthly	99.98%	99.99%	90.00%	80.00%
	1.3	SMWAN connectivity Level	Monthly	100.00%	100.00%	99.90%	99.00%
Availability	6.2	Percentage availability of DCC WAN Gateway Interface	Monthly	100.00%	100.00%	100.00%	98.25%
Service Management	11	Accuracy of Coverage Database provided to DCC Service Users	Monthly	98.86%	99.05%	95.00%	90.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	100.00%	99.99%	98.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	397.76%	398.52%	98.00%	96.00%
Communications Hub delivery	1.1	Percentage of Communications Hubs delivered on time	Monthly	100.00%	100.00%	99.00%	95.00%
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	~~99.21%~~ 100.00%	100.00%	99.90%	99.00%
	1.3	Percentage of Communications Hubs determined not to be faulty following attempted installation	Monthly	99.97%	99.896%	99.90%	99.50%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub "Incidents"	2.1	Percentage of Communications Hub Incidents resolved by remote maintenance	Monthly	100.00%	100.00%	99.00%	95.00%
Performance Area	**Performance Measure Number**	**Performance Measure Name**	**Measurement Period**	**Latest Qtr. Service Level 2020 Q4**	**Latest Qtr. Service Level 2021 Q1**	**Target Service Level**	**Minimum Service Level**
Communications Hub Connectivity	1.2	First time SMWAN connectivity within 90 days	Quarterly	100.00%	100.00%	99.00%	90.00%
Service Management	10	Notification of Planned Maintenance events within required target[6]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 15 - CSPC Reportable Performance Measures

PM12.2 - The calculation results for PM 12.2 comes as 398.52% CSPC had a total of 40,419 CH power outages reported in March, and all were sent to DSP within SLA (100%).

The formula (below) as given in Schedule 2.2.

For Power Outage Events which detect Power Loss Alerts from between fifty (50) Communications Hubs and five thousand (5,000) Communications Hubs, the Contractor shall measure:

$$PM12.2 = 100\% \times \left(\frac{\text{Number of Power Outage Event alerts}}{((\text{Number of Communications Hub Power Loss Alerts} - 50) \times 0.25) + 50} \right)$$

Using the calculation above PM12.2 = 100 * (40419/ ((40419– 50) * 0.25) + 50)) = 398.52%

[6] Measurement Period is a Calendar Quarter

6.1.1 Service Level Below Target Service Level

CSPC CH1.3 The Target Service Level for this measure is 99.90%, the reported Service Level was 99.896% and is below the Target Service Level.
There were 89,172 attempted installations in relation to this measure, 92 of which were deemed to be faulty – 2 more than the SLA allowed. This failure is still under discussion between DCC Commercial Team, DCC Service Delivery Team and Telefonica teams.

6.2 Performance Measurement Exceptions

In accordance with the Performance Measurement Methodology[7] document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below. These Comms Hubs are in alignment with the SECAS Issues Log. Where user behaviour has been identified as the reason for the exclusions, DCC are facilitating work between the CSP and Service user/s to address these.

6.2.1 In Period Exceptions

6.2.1.1 PM1.1 First Time SMWAN Connectivity

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.1 (CSPC)	13,662	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 16 - CSPC PM1.1 Exclusions

13,662 CH excluded for March 2021 due to a number of reasons^, covering: -

^CSPC Performance Measures Exceptions Classification Definitions can be found in Section 16.2 Appendix B, Sub-section 16.2.2

- There were no, or incomplete address details provided by the Service User – 8.016*
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 2,644
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 1,415
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 701

[7] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 691
- Installed outside of region – 142
- Aborted Installation - 30
- CHIMSM Not Followed – CH Never connected but received 8.14.1 – 14
- CHIMSM Not Followed - 8.14.2 on Cellular – 9

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

6.2.1.2 PM11 Accuracy of Coverage Database

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Service Management	PM11 (CSPC)	13,662	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 17 - CSPC PM11 Exclusions

13,662 CH excluded for March 2021 due to a number of reasons^, covering: -

^CSPC Performance Measures Exceptions Classification Definitions can be found in Section 16.2 Appendix B, Sub-section 16.2.2

- There were no, or incomplete address details provided by the Service User – 8.016*
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 2,644
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 1,415
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 701
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 691
- Installed outside of region – 142
- Aborted Installation - 30
- CHIMSM Not Followed – CH Never connected but received 8.14.1 – 14
- CHIMSM Not Followed - 8.14.2 on Cellular – 9

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

6.2.2 Total Estate Exceptions

6.2.2.1 PM1.3 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.3 (CSPC)	212,138	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 18 - CSPC PM1.3 Exclusions

NOTE: these exception volumes relate to the whole estate not just CH's connected in the reporting period

212,138 x CH excluded for March 2021 due to a number of reasons^, covering: -

^CSPC Performance Measures Exceptions Classification Definitions can be found in Section 16.2 Appendix B, Sub-section 16.2.2

- There were no, or incomplete address details provided by the Service User – 123,050*
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 41,400
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 22,322
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 11,768
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 9,039
- Installed outside of region – 3,529
- Aborted Installation – 1,030

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

7 Reported List of Service Provider Performance Measures CSP South

7.1 Service Levels Attained

A Service Level entry of “No Events” indicates that although the Performance Measure is applicable, no relevant events occurred during the Measurement Period and there is therefore no data to report upon.

A Service Level entry of “Data Exempted” indicates that although relevant events occurred during the Measurement Period, all events were exempt from measurement as they were agreed to be an Allowed Exception or Exclusion.

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.1	First time SMWAN connectivity at install	Monthly	99.99%	99.98%	90.00%	80.00%
	1.3	SMWAN connectivity Level	Monthly	100.00%	100.00%	99.90%	99.00%
Availability	6.2	Percentage availability of DCC WAN Gateway Interface	Monthly	100.00%	100.00%	99.98%	98.25%
Service Management	11	Accuracy of Coverage Database provided to DCC Service Users	Monthly	98.88%	99.06%	95.00%	90.00%
Power Outage Events	12.1	Percentage of Power Outage Event alerts delivered: 50 Communications Hubs or fewer	Monthly	100.00%	100.00%	98.00%	96.00%
	12.2	Percentage of Power Outage Event alerts delivered: greater than 50 Communications hubs	Monthly	397.13%	398.10%	98.00%	96.00%
Communications Hub delivery	1.1	Percentage of Communications Hubs delivered on time	Monthly	~~98.75%~~ 100.00%	100.00%	99.00%	95.00%

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
	1.2	Percentage of Communications Hubs accepted by DCC Service Users	Monthly	100.00%	100.00%	99.90%	99.00%
	1.3	Percentage of Communications Hubs determined not to be faulty following attempted installation	Monthly	100.00%	99.98%	99.90%	99.50%
Communications Hub "Incidents"	2.1	Percentage of Communications Hub Incidents resolved by remote maintenance	Monthly	100.00%	100.00%	99.00%	95.00%
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level 2020 Q4	Latest Qtr. Service Level 2021 Q1	Target Service Level	Minimum Service Level
Communications Hub Connectivity	1.2	First time SMWAN connectivity within 90 days	Quarterly	99.99%	100.00%	99.00%	90.00%
Service Management	10	Notification of Planned Maintenance events within required target[8]	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 19 - CSPS Reportable Performance Measures

PM12.2 - The calculation results for PM 12.2 comes as 398.10%. CSPS had a total of 31,451 CH power outages reported in March, and all were sent to DSP within SLA (100%).

The formula (below) as given in Schedule 2.2.

[8] Measurement Period is a Calendar Quarter

For Power Outage Events which detect Power Loss Alerts from between fifty (50) Communications Hubs and five thousand (5,000) Communications Hubs, the Contractor shall measure:

$$PM12.2 = 100\% \times \left(\frac{\text{Number of Power Outage Event alerts}}{((\text{Number of Communications Hub Power Loss Alerts} - 50) \times 0.25) + 50} \right)$$

Using the calculation above PM12.2 = 100 * (31451/ ((31451 – 50) * 0.25) + 50)) = 398.10%

7.2 Performance Measurement Exceptions

In accordance with the Performance Measurement Methodology[9] document, the number of events that have been identified as an Allowed Exception and removed from the Service Level calculation this Performance Measurement Period are shown below. These Comms Hubs are in alignment with the SECAS Issues Log. Where user behaviour has been identified as the reason for the exclusions, DCC are facilitating work between the CSP and Service user/s to address these.

7.2.1 In Period Exceptions

7.2.1.1 PM1.1 First Time SMWAN Connectivity

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.1 (CSPS)	8,561	Failure to follow installations as per CHIMSM	SU's have not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 20 - CSPS PM1.1 Exclusions

8,561 CH excluded for March 2021 due to a number of reasons^, covering: -

[9] The outline methodology for calculating the Service Levels is provided in the DCC Performance Measurement Methodology which can be found on the DCC SharePoint site at SEC Parties Operations Live/Information for SEC Parties/Regulatory/Performance Measures

^CSPS Performance Measures Exceptions Classification Definitions can be found in Section 16.2 Appendix B, Sub-section 16.2.2

- There were no, or incomplete address details provided by the Service User – 4,728*
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,355
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 1,003
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 786
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 496
- Installed outside of region – 165
- CHIMSM Not Followed – CH Never connected but received 8.14.1 – 13
- Aborted Installation - 8
- CHIMSM Not Followed - 8.14.2 on Cellular – 7

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

7.2.1.2 PM11 Accuracy of Coverage Database

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Service Management	PM11 (CSPS)	8,561	Failure to follow installations as per CHIMSM	SU's have not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 21 - CSPS PM11 Exclusions

8,561 CH excluded for March 2021 due to a number of reasons^, covering: -

^CSPS Performance Measures Exceptions Classification Definitions can be found in Section 16.2 Appendix B, Sub-section 16.2.2

- There were no, or incomplete address details provided by the Service User – 4,728*
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 1,355
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 1,003
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 786
- CHIMSM Not Followed – Outside CSPC Committed Coverage Area – 496
- Installed outside of region – 165
- CHIMSM Not Followed – CH Never connected but received 8.14.1 – 13

- Aborted Installation - 8
- CHIMSM Not Followed - 8.14.2 on Cellular – 7

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

7.2.2 Total Estate Exceptions

7.2.2.1 PM1.3 SMWAN Connectivity Level

Performance Area	Performance Measure Number	Number of Exception Events	Exception Scenario	Further Information
Communications Hub Connectivity	PM1.3 (CSPC)	200,494	Failure to follow installations as per CHIMSM	SU has not submitted the appropriate Service Requests post Installation. These figures are for the reporting period (not cumulative)

Table 22 - CSPS PM1.3 Exclusions

NOTE: these exception volumes relate to the whole estate not just CH's connected in the reporting period

200,494 x CH excluded for March 2021 due to a number of reasons^, covering: -

^CSPS Performance Measures Exceptions Classification Definitions can be found in Section 16.2 Appendix B, Sub-section 16.2.2

- There were no, or incomplete address details provided by the Service User – 115,333*
- CHIMSM Not Followed – No aerial is attached for installed SKU2 Device – 45,892
- CHIMSM Not Followed - Postcode available in CCDB, but given address is not in CCDB – 16,327
- CHIMSM Not Followed – SKU1 Device installed when SKU2 Device is recommended – 9,919
- CHIMSM Not Followed – Outside CSPS Committed Coverage Area – 9,662
- Installed outside of region – 2,278
- Aborted Installation – 1,083

*This exception has been further investigated by the CSP and the exception remains as the issue is due to the service users not following the CHIMSM. Invalid data is being entered into the MPxN field.

8 Reported List of Service Provider Performance Measures S1SP SIE

8.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service Availability – S1SP Data Service (Production Services)	Monthly	100.00%	100.00%	99.99%	99.17%
	2.2	Service Availability – RPS Data Service (Production Services)	Monthly	100.00%	100.00%	99.99%	99.17%
	2.4	Percentage Service availability – S1SP Management Interface Availability (Production Services)	Monthly	100.00%	100.00%	99.50%	98.00%
	2.7	Service Availability - Test services	Monthly	100.00%	100.00%	99.00%	98.00%
Application Management	3.1	Category 1 or 2 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	1
	3.2	Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	5
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level 2020 Q4	Latest Qtr. Service Level 2021 Q1	Target Service Level	Minimum Service Level
Service Management	7	Planned Maintenance events	Quarterly	100.00%	100.00%	100.00%	90.00%

Table 23 – S1SP SIE Reportable Performance Measures

8.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

9 Reported List of Service Provider Performance Measures S1SP Capgemini

9.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service Availability – S1SP Data Service (Production Services)	Monthly	100.00%	99.84%	99.99%	99.59%
	2.2	Percentage Service availability – CP Service (Production Environment)	Monthly	100.00%	100.00%	99.95%	99.17%
Application Management	3.1	Category 1 or 2 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	1
	3.2	Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	5

Table 24 – S1SP Capgemini Reportable Performance Measures

9.1.1 Service Level Below Target Service Level

S1SP - Capgemini PM2.1 reported Service Level was 99.84% and is below the Target Service Level.

The service was impacted by Category 1 incident INC000000707890 which resulted in 100% failure of SMETS1 Service Requests. (Incident details can be found in the Executive summary of this document, page 12.)

Capgemini's third-party provider were carrying out maintenance to provision disk space on their storage node, however the incorrect node was placed into maintenance mode due to human error which subsequently led to the storage nodes crashing and a database cluster failure.
Second Pair of eyes have been implemented for future changes.

Investigation underway between Capgemini and their third party into the possibility of distributing the database servers storage across a higher number of storage nodes to improve resilience in case of further storage node issues.

9.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

10 Reported List of Service Provider Performance Measures S1SP Vodafone

10.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability		Monthly availability of the Radio Network across VF-UK network	Monthly	99.54%	99.57%	99.00%	99.00%
		Combined monthly IoT Core and Management Service Availability	Monthly	99.93%	99.85%	99.70%	99.70%
		Monthly IoT Core availability (Voice/Data/SMS)	Monthly	99.93%	99.85%	99.90%	99.90%
		Monthly Management Service Availability (API, Reporting, Provisioning, GUI, Portal)	Monthly	100.00%	100.00%	99.70%	99.70%
		Monthly Availability of DCC dedicated fixed links	Monthly	No Events	100.00%	99.95%	99.95%

Table 25 – S1SP Vodafone Reportable Performance Measures

Back-haul solution “dedicated fixed links” is not currently live therefore no data is available

10.1.1 Service Level Below Minimum Service Level

S1CSP - Vodafone Monthly IoT Core availability (Voice/Data/SMS) reported Service Level was 99.85% and is below the Minimum Service Level.

The published Core availability of the IoT platform is for the whole of the shared environment utilised by all of Vodafone’s customers, however DCC were not impacted by the service outage which impacted the availability performance during the period.
For the purpose of demonstrating what the SLA would have been excluding non-impacting DCC issues, the SLA achieved would have been 99.95% which would have been within SLA.

10.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

11 Reported List of Service Provider Performance Measures S1SP Critical Software

11.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Application Management	3.1	Category 1 or 2 Incidents directly related to a change release within 30 days of release	Monthly	No Events	No Events	0	1
	3.2	Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release	Monthly	No Events	No Events	0	5

Table 26 – S1SP Critical Software Reportable Performance Measures

11.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

12 Reported List of Service Provider Performance Measures S1SP Morrison Data Services (MDS)

12.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level 2020 Q4	Latest Qtr. Service Level 2021 Q1	Target Service Level	Minimum Service Level
Service Management	7	Notification of Planned Maintenance events within required target	Quarterly	No Events	No Events	100.00%	90.00%

Table 27 – S1SP Morrison Data Services Reportable Performance Measures

12.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

13 Reported List of Service Provider Performance Measures S1SP Secure

13.1 Service Levels Attained

Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Service Level	Service Level	Target Service Level	Minimum Service Level
Availability	2.1	Service Availability – S1SP Data Service (Production Services)	Monthly	100.00%	100.00%	99.30%	98.00%
	2.4	Percentage Service availability – S1SP Management Interface Availability (Production Services)	Monthly	100.00%	100.00%	99.30%	98.00%
	2.7	Service Availability - Test services	Monthly	100.00%	100.00%	99.00%	98.00%
Application Management	3.1	Category 1 or 2 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	1
	3.2	Category 3, 4 or 5 Incidents directly related to a change release within 30 days of release	Monthly	0	0	0	5
Performance Area	Performance Measure Number	Performance Measure Name	Measurement Period	Previous Qtr. Service Level 2020 Q4	Latest Qtr. Service Level 2021 Q1	Target Service Level	Minimum Service Level
Service Management	7	Planned Maintenance events	Quarterly	No Events	100.00%	100.00%	90.00%

Table 28 – S1SP Secure Reportable Performance Measures

13.2 Performance Measurement Exceptions

No events or periods of time were identified as an Allowed Exception.

14 Service Credits

CSP (N) failed to meet the Target Service Level for three Performance Measures. These Performance Measures are:

CSP (N) PM2 – Percentage of Category 1 Firmware Payloads completed within the relevant Target Response Time. The Target Service Level for this PM is 99.00% and the Actual Service Levels achieved was 23.74%. This failure resulted in the accrual of 175 Service Points which equate to Service Credits of £43,198. (This Performance Measure contributes to DCC Performance Measure 1.)

CSP (N) PM6.3 – Percentage Access Node availability. The Target Service Level for this PM is 99.80% and the Actual Service Level achieved was 99.44%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

CSP (N) PM7.4 – Percentage Incident Resolution of Severity 3, Severity 4 and Severity 5 Incidents within requirement based on Severity Level. The Target Service Level for this PM is 99.00% and the Actual Service Level achieved was 88.44%. This is a KPI and therefore has no associated Service Credit attached. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

These failures equate to Service Credits of £43,198.

CSP (C) – CH1.3 Percentage of Communications Hubs determined not to be faulty following attempted installation. The Target Service Level for this PM is 99.90% and the Actual Service Level achieved was 99.896%. This failure is still under discussion between DCC Commercial Team, DCC Service Delivery Team and Telefonica teams. Update on applicable Service credit to be provided in future report.

CSP (S) - No Service Failures have occurred during the month. Therefore, no Service Credits have accrued this month.

NB – In the November 2020 report, CSPS reported that PM2 performance was 98.87%, which is below the Target Service Level of 99.00%. CSPS invoked a contractual clause relating to forecasted SRV volumes and deeming this Performance Measure as a success. DCC Commercial team are continuing to review this with CSPS and any Service Credits due will be reported in a future report.

DSP – PM 2.7 Percentage Service availability: External test services (8am to 8pm UTC Mon to Sat.) The Target Service Level for this PM is 99.00% and the Actual Service Level achieved was 98.56%. This failure resulted in the accrual of 9 Service Points which equate to Service Credits of £1,357. (This Performance Measure does not contribute to any DCC Code Performance Measure.)

Capgemini PM2.1 – Percentage Service availability – DCO Service (Production Environment.) The Target Service Level for this PM is 99.999% and the Actual Service Level achieved was 99.841%. This failure resulted in the accrual of 62 points Service Points which equate to Service Credits of £5,688. (This Performance Measure contributes to DCC Performance Measure CPM1.)

A summary of last 12 months Service Credits is provided in the table below:
NB. This table has now been updated to reflect the amendments to Service Credits applied due to the Arqiva updates to PM2 Performance for March 2018 to June 2020.
Please see the accompanying Service Credits Tracker Report for full details of each impacted period.

SMETS2 Service Providers

Month	Arqiva	BT	CGI	Telefonica	Total
Apr – 20	£60,935	£0	£3,949	£0	**£64,884**
May – 20	£60,935	£0	£0	£0	**£60,935**
June – 20	£72,084	£0	£0	TBC	**£72,084**
July – 20	£51,859	£0	£0	£0	**£51,859**
Aug – 20	£105,533	£0	£0	£8,111	**£113,644**
Sept -20	£70,528	£0	£3,015	£0	**£73,543**
Oct – 20	£73,899	£0	£0	£0	**£73,899**
Nov – 20	£48,488	£0	£0	£0	**£48,488**
Dec – 20	£45,377	£0	£0	£2,301	**£47,678**
Jan – 21	£43,198	£0	£0	£0	**£43,198**
Feb - 21	£43,198	£0	£0	£0*	**£43,198**
Mar - 21	£43,198	£0	£1,357	£0	**£44,555**

Table 29 – SMETS2 Service Providers Service Credits

*February 2021 Service Credits for Telefonica update to reflect amendments as per 202102_DCCPerformanceMeasurementReport_V2.0.

SMETS1 Service Providers

Month	SIE	Capgemini	Vodafone	Critical	Secure	Total
Apr – 20	£11	£0	£0	£0	N/A	**£11**
May – 20	£316	£9,896	£0	£0	N/A	**£10,212**
June – 20	£4,539	£18,873	£0	£0	N/A	**£23,412**
July – 20	£6,704	£39,384	£0	£0	N/A	**£46,088**
Aug – 20	£0	£19,222	£0	£0	N/A	**£19,222**
Sept – 20	£0	£0	£0	£0	N/A	**£0**
Oct – 20	£0	£36,000	£0	£0	N/A	**£36,000**
Nov – 20	£0	£0	£0	£0	N/A	**£0**
Dec – 20	£0	£0	£0	£0	N/A*	**£0**
Jan – 21	£0	£0	£0	£0	N/A	**£0**
Feb - 21	£0	£0	£0	£0	N/A	**£0**
Mar - 21	£0	£5,688	£0	£0	N/A	**£5,688**

Table 30 – SMETS1 Service Providers Service Credits

* Secure are contractually exempt Service Credits in December despite failing a single Service Measure as currently in first 6 months of contract operation.

15 DCC's Internal Costs and/or External Cost

There is no impact on DCC's Internal Costs.

DCC's External Costs in the period of this report are reduced by the Service Credit total of **£50,432.**

16 Appendices

16.1 Appendix A – Open Problem & Incidents relating to Prior Periods

Performance Measurement Report	Volume of Related Problems on Current Report	Volume Closed in Current Performance Reporting Period	Volume Remaining Open at End of Reporting Period
2019 August	1	0	**1**
2019 October	1	0	**1**
2020 June	1	0	**1**
2020 September	3	1	**2**
2020 November	2	1	**1**
2020 December	1	0	**1**
2021 March	7	0	**7**

Table 31 – Problem Record Summary

(Correct as of 23/04/2021)

16.1.1 PBI000000116812

August Report 2019 - Key Incident **INC000000479406**

DCC SMS, SSI and SSMI service degradation

Problem: This Problem Record is with DSP. DCC Service Management System, Service Management Interface and Self-Service Management Interface observed service degradation when a power outage was experienced throughout the UK which impacted a single rack in DSP Data Centre causing multiple DCC systems to alert.

The Root Cause has not been identified. DSP has confirmed that they have exhausted all testing that can be done without a strategic / planned failover of the F5s with packet captures and sniffers in place. DSP have been unable to see anything other than packet loss/output drops but need to confirm if the loss is enough to have caused this issue. At this stage it is not believed that further testing will add any value to Root Cause Analysis without a failover and captures for analysis.

The final action remains for DSP to invoke a failover of the system management firewalls in isolation, under a controlled Change. The failover will look to prove resiliency and support the resolution of any issues that may present during the course of the change window. In parallel,

an additional network analyser, which may be available for use from another client account, will also be run to capture evidence that may help DSP determine Root Cause however, this is only a possibility as DSP is unable to replicate the events of the August 2019 power outage regardless.

A change has now been raised to support the progression of this work, dates remain to be confirmed for implementation.

Latest: Target Root Cause Date Expired 27/08/2019

16.1.2 PBI000000117240

October Report 2019 - Key Incident **INC000000503961**

CSP Central and South Comms Hubs not birthing with DSP

Problem: A Service User contacted the DCC to advise that Comms Hubs were not birthing in the Central and South region. This was directly affecting Service Users ability to complete install and commissioning activities. The issue was due to a database full-table scan on the CSP Meter Firmware Operation Logging table. This caused other messages to queue while this scan completed. The reasons behind the full-table scan starting and why it was long-running are under investigation.

The Root Cause of this issue was a configuration change from a CSP release. CSP C&S completed a change release (R8.5) where additional logging was introduced to capture 'Force Time Sync' data issues, this caused the table space to increase significantly. This resulted in increased query times when high volumes of requests were submitted in parallel, in this incident single meter firmware jobs, caused extensive queuing. (90 sec + query times across 1000's of transactions).

CSP C&S technical team added Indexes to the table (per their vendors recommendation). Before the Indexes were added each job could took between 90 and 1200 seconds, following the Indexes going in this has dropped to 11 milliseconds. Long term enhancements are also being devised. DSP is still working with the Vendor to ascertain the best upgrade options. DSP has confirmed that the HSM (Hardware Security Module) upgrade is still under analysis with the Vendor as testing of the new client software was unsuccessful. At this stage DSP cannot proceed any further without a re-compiled version for the supporting software.

All upgrade work for the networking (ADN) hosts completed successfully on 20th November 2020. DSP is now looking to secure an implementation date for the required HSM upgrade. Planning is underway with a view to commencing at the beginning of 2021, and complete Production upgrades due in Q2, but this could be subject to change.

Latest: Target Completion Date 30/06/2021

16.1.3 PBI000000120410

June Report 2020 - Key Incident **INC000000597373**(Excluded from PMEL)

SMETS1 SFTP issue Middle Operating Capability (MOC)

Problem: SMETS1 Migrations Are Paused Due To secure file transfer protocol (SFTP) Connectivity Errors.

Root cause was found to be twofold:
1. A software bug in the vendor firewall which triggered traffic to fill over to an available secondary link.
2. The availability of a secondary link for traffic which had been removed from the original design however not prevented from advertising availability.

Measures have been taken to avoid the service from failing over to the secondary redundant link. For the identified software bug, the vendor is developing a fix.

Latest: Target Completion Date 30/06/2021

16.1.4 PBI000000121400

September Report 2020 - Key Incident **INC000000627085**

Failure of primary Firewall device

Problem: This Problem record is with CSP North. Failure of primary Data Centre device and subsequent unsuccessful failover caused outbound communication loss across all Production CSP North gateways - these include Wide Area Network (WAN) gateway, CSP North Management gateway and Service Management gateway.

Root Cause has been confirmed as configuration issue. Application Visibility Reporting parameter was larger than required causing stability issues.

This Problem Record is related to PBI000000113813 which was closed with the Mitigation of periodic reboot of network management devices put in place along with the permanent solution coming at the end of Q4 2020 in form of Firewall Technical Refresh that will exchange the devices on the Firewall to ones that do not have the bug causing memory leak that attributed to the issue that occurred (This is being managed as a Risk that has been raised in DCC Central Risk Register).

Changes around memory, memory adjustment and logging configurations are progressing whilst mitigating restarts are carried out on a regular basis.

Latest: Target Completion Date for this Problem is 29/07/2021

16.1.5 PBI000000121900

September Report 2020 - Key Incident **INC000000629108 (Exclusions 628941, 628942 & 628943)**

Inbound motorway availability issue

Problem: This Problem Record is with DSP. During planned Change work, the inbound motorway access was down due to an issue with a database; the database crashed during motorway restart.

A database restore along with a restart of the northbound motorway restored service, taking DSP outside of the allotted Change window.

Root Cause was confirmed as a database crash during the motorway restart, which resulted in the requirement to rebuild the database during the Change window. Two factors led to the restoration activity not being completed within the Change window:

1. The decision to undertake database restores should have been made earlier.

2. Limited timeframes to undertake patching activity outside of high-risk maintenance windows.

Preventative actions being reviewed to ensure no reoccurrence.

To mitigate against a reoccurrence of this issue:

Short Term: A DSP Service Delivery Manager is to be available during Changes to support/ensure that target fixation is achieved.

Long Term: A process is to be developed to ensure that support outside of DSP Service Delivery Manager is available during Changes being implemented Out of Hours for High Risk Change Windows.

The final remediation action is being tracked to completion. This will investigate the possibility of Patching being deployed outside of maintenance windows, doing one cluster set of servers on separate days, giving loss of resiliency: similar to near zero downtime approach. Change due to be completed 20th May.

Latest: Target Completion Date for this Problem is 31/05/2021

16.1.6 PBI000000121704

September Report 2020 - Key Incident **INC000000629122**

Unavailability of Communication Hub Manager (CHM)

Problem: This Problem Record is with CSP North. Communication Hub Manager (CHM) unavailability was determined during post change checks for a related change. The change couldn't be successfully tested as there were issues noted with CHM routing connectivity. Service was restored by refreshing the IP routing tables by CSP North.

The Root Cause was Unidentified. Due to the network connectivity problem between CHM nodes and CMI, a connection could not be established between clustered environments (nodes). This was due to a port being blocked. The reasoning for the routing connectivity issue is undetermined currently, and key logs for investigation are no longer available due to an existing log rotation policy (1.5 days).

CSP North are increasing the log retention to enable RCA analysis in case of future occurrence. Additional monitoring to be added to capture a failure scenario of this nature a change to be implemented to reduce complexity of the solution - to be added in January 2021 patch run. Log rotation capabilities included within CHM upgrade on 30th March 2021.

Latest: Problem Closed

16.1.7 PBI000000121926

November Report 2020 - Key Incident **INC000000647725**

Loss of connectivity to multiple 3G sites in the CSP North Region

Problem: CSP North reported that a number of their sites within their infrastructure were seeing a degraded transmission service across the CSP North Region. The number of sites that were impacted was 92 macro sites and 47 micro sites but a lot of these had macro diversity which meant they were still up and available to service Comms Hubs. Service Users and DNO's could have seen a degradation in service on their Comms Hubs within the CSP North region.

The Root was a Resilience issue. The CSPs vendor had a network switch issue, resilience are in place, but the nature of the failure prevented the resilience operating as expected. A new switch was configured and installed to resolve the issue.

The long-term fix is being devised and will involve reviewing how resiliency works. As a mitigation, a project was set up looking into new type of banded SIM card, so other carriers could be utilised in similar circumstances. Project passed Proof of Concept stage (tested on 17 sites) and has been handed to a transition team to progress.

Latest: Target Completion Date for this Problem is 24/09/2021

16.1.8 PBI000000121821

November Report 2020 - Key Incident **INC000000652948**

Increase in Service Request failure due to birthing process not completing

Problem: This Problem Record is with CSP North. Newly birthed Comms Hubs were not moving to 'INSTALLED' state leading to an increase in failure across following Service Requests:

- Service Request 8.11 Update HAN Device Log
- Service Request 4.10
- Service Reference Variance 206.24.1

It was confirmed during Incident investigation that Comms Hubs were getting Internet Protocol (IP) allocation but were in a lifecycle state of 'INVALID_COMMS_HUB_STATE'; the inventory state should change when birthed to 'INSTALLED'. Service Users were able to reboot Comms Hub whilst at site in order to progress commission.

The Root Cause is unable to be fully determined - Latency was evident at times on the Database. Additional enhanced monitoring for Service Request 8.11 is in place to spot any symptom of the issue promptly. A technical refresh of Infrastructure has been completed to resolve this Problem.

Latest: Problem Closed

16.1.9 PBI000000122005

December Report 2020 - Key Incident **INC000000664388**

SSI3523 - SMETS Certificate

Problem: SMETS1 devices being migrated with the DS certificate in both the DS slot and the KAK slot. This Problem is with the DCC following an issue on 8th December 2020 whereby SMETS1 devices were being migrated with the DS certificate in both the DS slot and the KAK slot.

The Root Cause has been confirmed as incorrect data provision by the data provider whereby incorrect security credentials were submitted in the Migration Authorisation (MA) file for dormant meter migrations.

Following identification of root cause this problem record is used to track progress of the long-term solution for the issue through automated file processing to be developed which is anticipated to be in place by the end of Q2 2021.

Latest: Target Completion Date 30/06/2021

16.1.10 PBI000000122516

March Report 2021 - Key Incident **INC000000697994**

Loss of service - Northbound traffic to DSP

Problem: Degradation of service in CSP North followed by total loss of service with Northbound traffic to DSP. Southbound traffic (DSP to CSP North) was unaffected. Impact to Operations: Multiple Service Users reported impact on Install and Commission in CSP North region.

Root Cause was confirmed as relating to the Certificate Revocation List (CRL) update process. DSP discovered that the configuration of application delivery networking (ADN) hosts does not behave as expected when multiple browser windows are used to manage the same application delivery networking (ADN) appliance and the application of the CRL to multiple profiles. The additional windows sometimes show duplicate configuration pages instead of the page that had been originally chosen.

A review of the frequency of Certificate Revocation List (CRL) expiry was performed and a script on the ADN host is urgently being developed, which in the first instance can be run manually following CRL updates to check that CRLs have been updated as expected, and will also be run on a scheduled basis to provide details of CRLs and can trigger alerts for CRLs that are due to expire well in advance of the actual expiration. A peer review to double check all CRL Changes will be completed until the script is in.

An internal communication has been issues to ensure that multiple tabs are not used when applying changes on ADNs.

Other actions also being progressed by DSP and associated updates:

- Review the ADN flag to allow CRLs to go beyond end date - Testing remains ongoing to support this action; it has been confirmed that no change is required to the Design.
- Put a monitoring script in place that will be picked up by the monitoring tools via syslog - Two Changes are being raised, which will enable automated detection of any missed CRLs post publication.
- Review the results of the auto script in non-Production and look at other mitigations - No issues have been seen yet review continues to confirm when this last pushed CRLs.
- Ensure that CRL changes to the ADN are added to the Forward Schedule of Chane (FSC) - Under review and remains to be confirmed.
- Update of any scripts should a new Secure Socket Layer (SSL) profile ever be created on an ADN host – To be noted if new profiles are created – documentation to be updated - Remains under review; this is for information only; DSP needs to clarify where best to document this for future reference.

Latest: Target Completion Date 30/04/2021

16.1.11 PBI000000122229

March Report 2021 - Key Incident **INC000000698821**

Single DNO loss of traffic.

Problem: DNO identified issues with receiving traffic from the DSP and no AD1 alerts being seen. Impact to Operations: AD1 alerts are classed as critical to DNOs.

Root Cause was established during the course of the Major Incident; When the Service User upgraded their adaptor to DUIS 4, DSP were unaware of this change, and the DSP infrastructure was not configured to support DUIS 4.

To restore service, DSP reconfigured Management Gateway North (MGN) to send/receive DUIS 4 traffic. Remediation actions are now being progressed.

Latest: Target Completion Date 10/05/2021

16.1.12 PBI000000122418

March Report 2021 - Key Incidents **INC000000702177 & INC000000702810**

SR 8.11 failure rate increase and Install and Commission failures in CSP North region

Problem: Significant increase in Service Request (SR) 8.11 (Update HAN Device Log1) failure was noted with birthing issues seen as a consequence. Investigation established that route connections were not being established and Comms Hubs IP allocation was not happening in expectant timelines. Failover of Route Manager 1 to Route Manager 2 was performed, and although services improved, standard expected baseline was still not observed.

Root Cause was confirmed as a configuration issue. Traffic flow disruption aligned with insufficient virtual Central processing unit (CPU) and memory on core firewall appliances.

The Tech Refresh Programme tested prior to Production migration with more throughput than Production, yet only for a single flow (not multiple simultaneous flows). The solution for this issue requires a Virtual Central processing unit (CPU) increase, to be progressed via Change.

Latest: Target Completion Date 30/07/2021

16.1.13 PBI000000122422

March Report 2021 - Key Incident **INC000000707890**

SMETS1 - Failure for SMETS1 Service Requests 23/03

Problem: At 13:52 23/03 there was a database server cluster failure within in DCO's infrastructure resulting in a loss of capability to deliver any SMETS1 traffic (100% failure) this would have meant that SMETS1 migrations would not be able to be completed, but no migrations were planned for the day. DCO restarted their database cluster, which completed at 15:01 restoring service. For the duration of the outage Service users would not have been able to successfully send or receive any traffic across the SMETS1 Estate.

The Root Cause is an Application Issue. The DCO application was not processing transactions because the DCO Database was not available. The DCO database cluster became unavailable due to an issue on the DCOs vendors hosting platform where a number of virtual servers including the DCO PROD B database data node servers entered a read-only state. The database servers entered a read-only state due to both storage nodes in a resilient pair becoming unavailable, one storage node due to ongoing maintenance and the other due to the incorrect storage node being placed into maintenance mode in error. DCOs vendor has advised that under normal operating conditions, there is not a single point of failure present on the infrastructure as the storage nodes operate in resilient pairs.

The issue with replication occurred because the database was stopped ungracefully, and a replication reset was not sufficient to restore replication and required further engineer intervention. This replication is not an essential component or function of the DCO service or its Disaster Recovery capability and frequent backups of the PRODB database were captured throughout the process to ensure that DCO could meet its contractual Disaster recovery targets in case of a further issue with the PRODB DCO database.

DCOs vendor have advised they have implemented a second-pair-of-eyes check to validate the correct kit has been placed into maintenance mode in future. DCO have engaged their vendor to investigate the possibility of distributing the database servers storage across a higher number of storage nodes to improve resilience in case of further storage node issues.

Latest: Target Completion Date 30/04/2021

16.1.14 PBI000000122520

March Report 2021 - Excluded Incident **INC000000701200**

Global Virtual Private Network issues

Problem: On 07/03/2020 a number of users experienced issue accessing services which required connectivity through the virtual private network (VPN) capability.

Root Cause was a user access authentication policy issue. The access vendor requires verification of Multi-Factor Authentication (MFA) details and users are sent to an MFA registration page. There is a conditional access policy that stops users from getting to this area if they are not on a trusted access page. This affected the 'link' to the MFA challenge, not the actual MFA service itself. As users were working from home, and not at a Trusted Site (DCC office), the registration page took the users to NOT be on a trusted access page and therefore refused them access to the registration page, preventing the users' MFA action to complete.

There is currently no statement from the vendor on how often this happens, however, this can be actioned by the vendor at any time depending on what they feel is required

Latest: Target Completion Date 30/06/2021

16.1.15 PBI000000122415

March Report 2021 - Excluded Incident **INC000000701348**

Supplier multi-client major incident impacting DCC- Relating to issues accessing internet services.

Problem: On 08/03/2020 a number of users experienced issues accessing internet-based services due to a supplier multi-client major incident which impacted DCC connectivity to internet-based services which required connectivity through the virtual private network (VPN) capability.

Root cause in this incident is: Hardware Component Failure . The cause of the incident was the partial failure of the Modular Port Concentrator (MPC) card associated with the IT providers router equipment. This MPC houses the two daughter cards, one connects to the Core MPLS Network, and one onward to the internet service provider (ISP) service. The incident is attributed to cell errors detected between the Flexible physical interface card (PIC) Concentrator (FPC) and the Control Board (CB). Both the FPC and CB are core components of the MPC. Rebooting the chassis resolved the issue, but given the errors identified between the FPC and CB, the MPC Card has been replaced as a precautionary measure. The two daughter cards were not replaced as part of this process.

Service was restored on the day by restarting the IT providers router chassis. As a precaution, the parent Modular Port Concentrator (MPC) card has been replaced.

Latest: Target Completion Date 30/06/2021

16.1.16 PBI000000122237

March Report 2021 - Excluded Incident **INC000000708834**

Key DCC Systems experiencing issues

Problem: On 25/03/2021 a number of users experienced issues accessing internet-based services due to a supplier multi-client major incident which impacted DCC connectivity to internet-based services which required connectivity through the virtual private network (VPN) capability.

The IT provider and their vendor have been unable to determine root cause of the issue. In order to get to reach this decision that have advised the following: “We know that this was caused by bursts of traffic exceeding the session packet buffer limit on the gateway, but we do not know what the source was. The only lead was a file transfer, but this was ruled out once the first failback to the primary datacentre had been completed.

The possibility of a distributed denial of service (DDoS) attack was floated with the vendor however this was dismissed following their review of available logs and evidence captured the time of the incident. Remediation activities are progressing.

Latest: Target Completion Date 30/06/2021

16.2 Appendix B – Performance Measure Exception Definitions

16.2.1 CSPN

Communications Hubs where no incident has been raised for outage
CSPN see the Comms hub appear on its network but then do not see any traffic to or from the Comms hubs for more than 10 days. This is mostly driven by service users powering on a Comms hub and either not completing the install or correctly decommissioning it. As soon as the CSPN system sees the CH on the network, it will be looking for it forever. This is being investigated as part of problem ticket.

Incomplete Communication Hub Install
Installations that have been aborted by the service user, but no service requests submitted. If the installation results in an install and leave, then the SU should be submitting and 8.14.2 service request. If the install is fully aborted, then an 8.14.3 service request should be submitted. This is being investigated as part of problem ticket.

Data Error
Comms Hubs where the data shows that an additional outage started prior to the previous one ending. This is an error and is under investigated by CSPN.

Issue started and ended in prior month Comms Hubs where the outage incident started and ended in a previous month but are showing the in current reporting month. This reporting issue is being investigated by CSPN.

Communication Hub in Low Coverage database
Comms Hub is installed in a low coverage area.

Not Active
Comms Hubs where the Operational Status in the CSPN system is not set to Active, to be included in PM1.4 the device must be Active. These are devices where the SU has started the Returns Process

Communication Hub installed on non-consumer premises e.g. Live Labs
Hubs install is confirmed as not in scope because it not installed on a consumer's premises, i.e. Live Labs.

Part of first 1,000 DBCH to be excluded for contractual reasons

As per the CSPN contract, an allowance for exclusions until the measurement period after 1,000 Standard 420 or Variant 450 Dual Band Comms Hubs have been installed, to mitigate for early adoption difficulties.

16.2.2 CSPC & CSPS

No Address/Postcode in JSR
Missing address/postcode in received CHSU, so unable to determine CHIMSM compliance

CHIMSM Not Followed - No aerial is attached for installed SKU2 Device
Aerial not installed for a Cellular & Mesh Comms Hub as per BE. CHIMSM not followed

CHIMSM Not Followed - SKU1 Device installed when SKU2 Device is recommended

Service User Installed Cellular instead of Cellular & Mesh (CSPC/CSPS Coverage Recommendation – Cellular & Mesh). CHIMSM not followed

CHIMSM Not Followed - Comms Hub Never connected but received 8.14.1
CSPC/CSPS have never received Birth event to support 8.14.1. These should be 8.14.2 with Cellular & Mesh Installed.

Aborted Installation
Service User confirmed as Aborted as part of one of the incidents raised for these Comms Hubs

CHIMSM Not Followed - Outside CSPC/CSPS Committed Coverage Area
Comms Hub installed outside CSPC/CSPS Committed Coverage Area. CHIMSM not followed. CSP Automation also returns CHIMSM Not Followed – Postcode not available in CCDB

CHIMSM Not Followed - Associated with NEP
As per CSPC/CSPS, coverage is not available yet and the given postcode in CHSU is associated with Network Enhancement Plan (NEP). CHIMSM not followed

CHIMSM Not Followed - 8.14.2 on Cellular
Service User submitted 8.14.2 for Cellular Hub. Service User should have attempted with Cellular & Mesh if no connectivity. CHIMSM not followed

CHIMSM Not Followed - Install and Leave Incident raised for Cellular Hub
Service User raised Install and Leave Incident (Category 6) for a Cellular Hub and received 8.14.1 instead of 8.14.2. Service User should have attempted with Cellular & Mesh if no connectivity at the time of installation. CHIMSM not followed

CHIMSM Not Followed - Given UPRN is not available
UPRN received in CHSU is not available in CSPC/CSPS Coverage Database, so unable to determine CHIMSM compliance

Partial Address Match
Partial address received in CHSU, unable to determine CHIMSM compliance based on given partial address.
CSP Automation also returns CHIMSM Not Followed - Postcode available in CCDB but given address is not in CCDB

Installed Out of Region
Service User installed CSPC/CSPS Comms Hubs in CSPN Region. CHIMSM not followed

Test Lab Installations
Comms Hubs installed in Test Labs

CHIMSM Non-Compliant - No Comms Hub Install on Cellular
Service User submitted 8.14.2 for Cellular Hub. Service User should have attempted with Cellular & Mesh if no connectivity. CHIMSM not followed

16.3 Appendix C - Incident Reports Glossary

Report Title	Description
Incident Reference	Incident ID from DSMS
Problem Reference	Problem ID from DSMS
Category	Incident Category
Service(s) Impacted	E.g. Installs, Service Requests, DSMS
Service impacted date/time	Time the outage started confirmed by logs, alerts (Confirmed via Supplier(s))
Service restored date/time	Time the outage was confirmed as resolved
Incident raised date/time	Taken from "Reported Date+" field in DSMS
Incident resolved date/time	Time incident was marked as resolved in DSMS
DCC MIM Engagement date/time	Time the issue was escalated to the DCC MIM team for management as a high category incident
Actual Impact Duration	Duration of impact to service
Incident Duration	From logged to resolved in the DSMS ticket
Impacted Region	CSP Region: North, Central and South or all
Was the Incident prioritised correctly?	Outcome of the Post Incident Review, with a brief explanation why.
Resolved within SLA	Reference to the performance measure
Relevant Logs Captured	Evidence of the impact to service to determine root cause
Date Completed	Post Incident Review Completion Date
Summary of Incident	High level summary of the incident, the investigations and resolution activities
Customer Impact	The consequences of the service outage. Example: Users were unable to complete birthing events, affecting installs & commissions.
Actions Completed to Recover Service	Details of restorative work Example: DSP removed the failed application server from the pool which allowed traffic to flow through the alternate servers