



**TELECOM PROPOSAL PRESENTED  
TO MINISTRY OF ECONOMIC  
DEVELOPMENT**

**VARIATION OF TELECOM  
SEPARATION UNDERTAKINGS  
DATED 25 MARCH 2008**

**PROPOSAL DATED  
13 AUGUST 2009**

## EXECUTIVE SUMMARY

- 1 The Undertakings contain a number of provisions which protect information held by Chorus and Telecom Wholesale about their customers (**Customer Confidential information or CCI**). Access to CCI is restricted, and misuse of it is a breach of the Undertakings. In order to mitigate the risk of any such breach, Telecom has put in place a comprehensive set of systems changes and information-use rules and policies to enhance protection of this information. These measures are subject to continual oversight from the Independent Oversight Group (**IOG**) and ensure that retail staff do not misuse Telecom Wholesale or Chorus customer information. In the first year of separation for example, the IOG and Telecom have investigated more than 3000 information-related Honesty Box submissions, and found no evidence of any misuse of information in breach of the Undertakings.
- 2 The Undertakings also recognised, however, that rigidly partitioning all of this information right across Telecom's shared systems environment is a substantial task, and set a target date of 31 December 2009 for this task to be completed. In the interim, incidental viewing of CCI by Telecom employees accessing shared information systems in the ordinary course of their job is permitted.
- 3 Since the Undertakings were signed, Telecom has undertaken a complete bottom-up review of all of our shared information systems to identify those which contain CCI, and how it can best be partitioned off in accordance with the Undertakings. In all, 1321 systems have been reviewed, and 56 have been identified as requiring work.
- 4 Work on implementing the organisational, business process and systems changes solutions necessary to deliver the required separation is now well underway. Over \$11 million has already been spent on the project, of a total estimated spend of over \$30 million. The most high-risk shared information system – called PROBE – will be compliant by the December 2009 date, and we also expect to have addressed most (75%) high usage screens within our primary shared information system, ICMS, by that date.
- 5 However, this has proven to be an absolutely enormous programme of work, touching every aspect of Telecom's business and driving fundamental change into our shared systems environment. We originally struggled to design effective solutions for the large volumes of systems, which caused some delay in getting the right detail into our programme plan. Of more import though, the timing of the bulk of the work necessary – coincident with so many equivalence-related milestones and programmes – has led to increasing levels of congestion and risk within Telecom's systems environment and has significantly increased the complexity of change and associated risks.
- 6 Despite our best efforts to address this congestion and complexity, we are now at a point where we consider the risks to (a) Telecom's systems environment, which supports more than 800,000 transactions by New Zealanders per day, and (b) the five concurrent major Undertaking programmes of work also targeting delivery by 31 December 2009, are too great to responsibly accept.
- 7 Therefore, after exhausting all other options, Telecom has concluded it needs to seek a variation to the Undertakings, to extend the 31 December 2009 deadline to September 2010. We expect to be able to achieve compliance for

most of the systems in line with the existing date, in accordance with the plan for upgrading and migrating to meet the 31 December requirement. However, based on our current information we estimate we will need nine additional months to ensure compliance with the requirements of the Undertakings.

- 8 We also propose a more considered, sensible approach to a small number of aging information systems which contain extremely technical information that is unlikely to be of any material competitive value and for which a rigid logical separation of information would be disproportionately expensive.
- 9 We consider the alternative approach – compressing project and testing timeframes in an attempt to meet the 31 December date for all six Undertakings programmes of work - would be irresponsible and inappropriate, given the importance of some of the systems to our wholesale and retail customers and the importance of the other undertakings milestones to the delivery of equivalence.
- 10 This paper outlines the rationale for, and the details of, the changes sought. It also includes a mark-up of the Undertakings reflecting the proposed changes.
- 11 We ask the Minister to agree to our proposal and approve the necessary changes to the Undertakings.

Activity	Status	Outcome
Implement measures to protect against misuse of Chorus or Wholesale information in breach of Undertakings	Completed June 2008	Comprehensive measures put in place to protect CCI and provide effective oversight and monitoring (by Telecom compliance teams and IOG)
Analyse processes and systems to identify areas for remediation	Systems Analysis Completed August 2008 Screen Analysis Completed June 2009 Report Analysis Completed July 2009	1321 systems analysed, 56 identified for remediation 3200 ICMS screens and 2880 reports and extracts reviewed, over 300 identified for remediation
Implement compliant solutions for high-risk decision support (data mining) and market intelligence systems	On track for December 2009 completion	Highest risk data mining systems - PROBE and TRIAD - will be fully compliant by December 2009
Implement compliant solutions for high-risk screens within Telecom Retail's primary shared information system - ICMS	75% of high-usage screens completed by December 2009 System fully compliant September 2010	Existence of Wholesale broadband on customer line invisible to Telecom Retail.
Implement compliant solutions for remaining transactional and operational/technical support systems	23 Systems completed December 2009 10 Systems completed June 2010 Remaining (8) Systems completed September 2010	High-risk systems compliant (ICMS 75% compliant) December 2009 Full compliance September 2010

## BACKGROUND

- 1 The Undertakings contain provisions restricting access to Chorus and Wholesale Customer Confidential Information (**CCI**). These clauses provide that Wholesale CCI and Chorus CCI cannot be disclosed to any other part of Telecom, except in certain circumstances, for example where it is necessary operationally to provide a Relevant Service.
- 2 However, it was recognised at the time the Undertakings were agreed, that Telecom would require a transitional process to enable compliance with those restrictions, because of existing legacy shared information systems. Therefore, clause 9.3(e) of the Undertakings:
  - (a) Provides an exemption until 31 December 2009 to the clauses in the Undertakings that prohibit access to CCI;
  - (b) Provides that nonetheless, any Chorus or Wholesale CCI accessed must not be used or disclosed in a manner that is contrary to the Undertakings;
  - (c) Requires Telecom to ensure that all shared information systems (including certain named systems) are upgraded to prevent access to Chorus and Wholesale Customer Confidential Information that is not permitted by the Undertakings by 31 December 2009; and
  - (d) Required Telecom to develop, by 30 September 2008, a plan for upgrading or migrating its shared information systems to meet that 31 December requirement (the **September Plan**).
- 3 In accordance with clause 9.3(e) we prepared the September Plan, which identified 54 systems that required some form of remediation to achieve compliance with clause 9.3(e). We delivered the September Plan to the IOG.
- 4 Since we prepared the September Plan we have gained an increased understanding of the level and complexity of systems-related work necessary to meet the 31 December 2009 date. In short, the level of change that will be required to our systems environment as a result of this programme is unprecedented. At the same time, we also have five other major equivalence-related programmes of work which must be delivered into that systems environment – change on top of change.
- 5 The result is unacceptably high levels of congestion and risk, and we now have considerable concerns about our ability to meet the 31 December 2009 date for all of these programmes, without creating an irresponsible level of risk to the systems environment.
- 6 In turn this would impact on the wider industry because of the integral nature of some of these systems – Integrated Customer Management System (ICMS) in particular - in providing support to customers of Telecom Wholesale and Chorus and to their end-users.
- 7 We therefore consider it necessary to seek a variation of the timeframe for compliance.

## Protections in place for customer information

- 8 Telecom understands the importance of protecting our Wholesale and Chorus customer information. We have put in place comprehensive measures to protect customer information, and continue to augment these with system-based changes as this becomes possible. The measures we have put in place already include:
- Rigorous information-use policies and comprehensive training and monitoring programmes to support them;
  - Recording and auditing every instance of incidental views by retail of identified ICMS screens which contain CCI; and
  - Internal monitoring, and IOG oversight and investigation of over 2500 self-recorded “views” of CCI by retail staff.
- 9 We have clear evidence, from honesty box submissions, IOG investigations and auditing that these measures are being complied with.
- 10 We detail the measures below:

Risk mitigations	Description
Codes of Conduct Training	As required by the Undertakings, business unit specific Codes of Conduct were developed and rolled out. Supporting this was a comprehensive online training programme, which informed on both the Undertakings and the obligations they imposed on Telecom.
Honesty Box	<p>The Undertakings were the catalyst for the development and implementation of a process for Telecom employees to report potential breaches of the Undertakings. A self-reporting system (the Honesty Box) was implemented, and a Retail Compliance team formed to educate and oversee operation of the Honesty Box within Telecom’s retail units. Retail staff have been educated about their responsibilities in relation to CCI, and - in conjunction with auditing introduced to capture all such “views” (described below) - encouraged to self-report incidental views of this type of information.</p> <p>The Honesty Box was established July 08, and as at 30 May 2009:</p> <ul style="list-style-type: none"> <li>• It had received 3653 submissions in relation to Operational Separation. Each of these is investigated by Telecom and/or the IOG;</li> <li>• 97% of these submissions originated from Retail arising from concerns on the frontline about visibility of Wholesale data. Retail are currently getting 7-10 submissions /day; and</li> <li>• Submissions and conclusions are audited by compliance managers and the IOGSO.</li> </ul>
ICMS changes	<p>A project called ICMS Wave I, designed to mitigate the risk of any misuse of CCI, was implemented once the Undertakings were signed, and achieved the following:</p> <ul style="list-style-type: none"> <li>• Identified high risk scenarios and ICMS screens (and information accessed during these scenarios);</li> <li>• Created an automated audit capability to capture and track any activity around these scenarios and screens;</li> <li>• This information is used to identify Retail Customer Service Representatives (CSRs) accessing screens outside their expected workflow and then analysis is undertaken as to why this has happened. Any necessary action/training is developed off the back of this.</li> </ul>

	<p>The changes are now operationalised and documented as Standard Operating Procedures and there is a continuous improvement programme around the capability.</p> <p>ICMS Wave II is currently underway, with the objective of making ICMS fully compliant with Undertaking CCI requirements. We expect that CCI will be removed from all high-usage Telecom Retail ICMS screens, including winback screens, in the first drop of WAVE II code changes, between August and November this year (see table below at paragraph 20 for further detail)</p>
PROBE Changes	<ul style="list-style-type: none"> <li>• All users of PROBE have been categorised by business unit and assigned database roles to control their access, which means that all PROBE users are identifiable by business unit and their access to information within PROBE is controlled accordingly</li> <li>• A user survey has been completed, resulting in a cull of the user base where access was no longer required;</li> <li>• The detailed rules to categorise data as belonging to Chorus, Wholesale and Retail, respectively, has been determined;</li> <li>• Users have been restricted to access to certain key database tables, according business unit ownership of those tables, using conventional Oracle database security;</li> <li>• For certain key database tables with mixed ownership, user access has been restricted to rows within those tables, based on business unit ownership of the individual rows, using Oracle's Fine Grain Access Control security feature;</li> <li>• Users running reports are identified by the database and restricted according the measures detailed above.</li> </ul>
Retail Op Sep Taskforce	<p>Retail has established a dedicated team focused on addressing Operational Separation issues within the Retail part of the business – this is made up of 9 individuals:</p> <ul style="list-style-type: none"> <li>• The team is focussed on process change to ensure compliance, people change and Data Compliance;</li> <li>• The team has completed two risk workshops with frontline staff to date that have identified 240 scenarios that would need to be changed to ensure compliance post December 2009;</li> <li>• From this, analysis is completed and changes implemented – a good example is the creation of a “short leads” compliance dashboard to actively monitor Retail short lead activity.</li> </ul>
Outbound call centre (OBCC)	<ul style="list-style-type: none"> <li>• A top down review of the systems and process used by the Outbound Call Centre has been completed, and ongoing Undertakings compliance monitoring implemented;</li> <li>• The presales process has been identified as a potential risk area, as this is where the call schedules are created. A new presales process has been designed which is compliant with the Undertakings and is now documented as a Standard Operating Procedure.</li> <li>• As set out in the table at paragraph 20, we expect high-usage winback screens will be data compliant by the 31 December 2009 date.</li> </ul>
Compliance Frameworks	<p>All Telecom business units have established Compliance Frameworks that include measurement and monitoring that identifies ownership of Undertakings deliverables within each business unit, what will be done by whom and when.</p>

## Outline of the Data Compliance Programme

- 11 In addition to all the work done to mitigate risk, Telecom also undertook an analysis of all shared systems to determine which of them would require work to ensure compliance with clause 9.3(e)(iii).
- 12 This work identified 56 systems out of 1321 that would require work to meet the 31 December 2009 deadline. Telecom established a Data Compliance Programme, to design and implement the changes necessary to achieve compliance. The scope of the programme is to deliver the best solution – that might be technology, process or organisational, or a combination of these. The work to mitigate risk and analyse work required within our two largest and integrated shared access systems - ICMS and PROBE - began as soon as the Undertakings were signed in early 2008. Both are ongoing.
- 13 The Data Compliance Programme entails a significant amount of work. Telecom estimates that delivering the programme as currently scoped will cost over \$30 million. The programme involves more than 160 people from both the technical and business communities.
- 14 The programme involves analysing each system, ascertaining who the users are and what types of information are contained within the system. The analysis must also consider the system's underlying technical architecture and what controls are currently in place to govern access to the system's information. Having understood all this for each system, the team must then recommend a solution.
- 15 The range of solutions includes:
  - 15.1 Decommissioning – some systems could be made compliant by decommissioning them, either because an assessment indicated that they were no longer integral systems, or because they were already earmarked for decommissioning. An example of a system that has been decommissioned is Petunia. The Petunia application is used for retrieving the call flow information. Petunia 2 is used to test a customer's DSL details and Petunia 3 is a billing tool. Petunia is being replaced by INFO (Integrated Front Office Management), which is also being addressed by the Data Compliance Programme.
  - 15.2 Removing access – some systems are predominantly used by certain parts of Telecom. Where it will not affect business processes, the solution has been to remove access from representatives of certain business units. For example, Netmap is a system that contains inventory of outside plant assets owned and/or operated by Telecom. The recommended solution for Netmap is that it be limited to use by Chorus and Shared Services staff only and that an internal process is implemented to monitor and control access.
  - 15.3 Changing systems includes what is known as "logical separation", which requires systems change to ensure that access to information is governed by the user's business unit. ICMS is an example of a system undergoing logical separation. To undertake logical separation, especially of a system like ICMS, is a huge task. We need to understand the data contained within the system, the screen structure and analyse whether each piece of information is CI or CCI. We then need to understand who uses which parts of the system, and ultimately need to label each piece of information according to which business

unit “owns” it. For ICMS there are 3200 screens that have had to be reviewed, and over 300 of these require changes to be made. There are an additional 2880 reports and extracts from ICMS that must also be reviewed, and this work is ongoing. To complete logical separation we need to then define user role types and map all users to the define role types.

- 16 In addition to all this technical work, there is a huge component of business change involved. For each system, the business needs to assess whether the recommended solution is likely to have an impact on business processes and/or the customer experience. Even small changes like altering the way a screen looks must be assessed and managed – for example, people need training on any changes to ensure they can continue to perform their work as required, and any systems that link automatically to other systems must be checked to ensure we preserve necessary functionality.

### **Priority of systems**

- 17 We have prioritised the systems identified as requiring work to achieve compliance, to ensure that the systems that are more significant are addressed as a matter of priority.
- 18 First, we have focused on the six systems named in clause 9.3 of the Undertakings. We have also prioritised according to:
  - 18.1 The systems that are the biggest and most often used by the business units;
  - 18.2 Those systems that entail a greater risk of misuse of information (outlined below); and
  - 18.3 Systems used in customer-facing situations.
- 19 While the risk of inappropriate access to CCI is the same within each system, we perceive the risk of misuse of information to be greater in some than in others. Accordingly, we have differentiated the systems on the basis of whether they are decision support systems or transactional systems. Decision support systems, such as PROBE, are the systems that could be used to “mine” and aggregate data. Transactional systems are those that enable a user to access only one record at a time. We consider the decision support systems a priority because of the greater risk involved, and accordingly are working to ensure compliance for these systems by 31 December 2009.
- 20 We are also well advanced in addressing the most high-use and high-risk screens – including winback screens - within ICMS by December this year, through the introduction of the first two of seven anticipated separation-related “code drops”. As a result, we consider that ICMS will be largely compliant by this date. The subject of these “code drops”, and their purpose is set out below:

Code drop & proposed dates*	Purpose	What changes for Telecom retail CSRs?
Drop 1 – August – November '09	<ul style="list-style-type: none"> <li>• Removal of Wholesale broadband spot codes</li> <li>• Hide UBS spot codes from Retail &amp; Gen-i</li> <li>• Restrict view of service orders on mixed carriers</li> <li>• Service order / Dispute staging Provide a service order summary to Retail</li> <li>• Apply CCI rules to 70 high usage screens and 6 reports – including winback screens</li> </ul>	<ul style="list-style-type: none"> <li>• Retail CSRs can no longer see existence of Wholesale broadband services on customer's line.</li> <li>• Retail CSRs can no longer see details of ICMS service orders relating to Wholesale &amp; Chorus customers</li> <li>• Retail CSRs will not be able to view details associated with Wholesale or Chorus customers on high usage screens</li> <li>• ICMS service order entry rules will prevent Retail CSRs from entering orders which impact Wholesale UBS, as UBS is no longer visible.</li> </ul>
Drop 2 November – December '09	<ul style="list-style-type: none"> <li>• Restrict viewing of Chorus/ Wholesale CCI on further scoped screens</li> <li>• Restrict customer subtype allocation</li> <li>• Changes to messages and alerts</li> </ul>	<ul style="list-style-type: none"> <li>• Retail CSRs cannot select Chorus/ Wholesale customers via ICMS enquiry screens that contain CCI, examples; <ul style="list-style-type: none"> <li>◦ Direct debit / credit card payment</li> <li>◦ Local call enquiry view</li> </ul> </li> <li>• Retail CSRs cannot maintain an ICMS customer identifier that is used to identify a Wholesale or Chorus customer</li> </ul>
<p>As a result of these two drops, we expect over 75% of the highest-usage ICMS screens will have been addressed, including screens used in the winback process. The remaining "drops" address increasingly incidental screens, which are used much less frequently, and represent a much lower risk of information misuse.</p>		

Drops 3 & 4 – January – February '10	<ul style="list-style-type: none"> <li>• Changes to complex scrolling screens as identified in specific business scenarios</li> </ul>	<ul style="list-style-type: none"> <li>• Credit Check screens will no longer identify if a customer is a Wholesale or Chorus customer.</li> <li>• A Chorus ICMS access profile that has no operational need to review statement details, will not have access to statement enquiry screens.</li> </ul>
Drop 5 – February – March '10	<ul style="list-style-type: none"> <li>• Automated solution for identity &amp; access management</li> </ul>	<ul style="list-style-type: none"> <li>• No change to end Retail CSRs access expected as a result of this release.</li> </ul>
Drop 6 – March – April '10	<ul style="list-style-type: none"> <li>• Further changes to reports – terminate identified reports</li> </ul>	<ul style="list-style-type: none"> <li>• Any ICMS Reports that contain CCI and CI detail will be amended to remove/suppress CCI.</li> <li>• Some background ICMS menu changes where there is no operational requirement for Retail users to access the report, option will appear 'blank'.</li> </ul>
Drop 7 – April – May '10	<ul style="list-style-type: none"> <li>• Change requests (including Chorus CI screen changes)</li> <li>• Changes to any additional screens</li> </ul>	<ul style="list-style-type: none"> <li>• Currently being scoped</li> </ul>

- 21 During Drop 1 & subsequent drops the technical components will pass through Business Acceptance Testing and then be implemented into ICMS Production.
- 22 After we have successfully implemented Phase 1 we will start a pilot to migrate small groups from Retail, Gen-I, Wholesale and Chorus into their respective user profiles. The purpose of the pilot is to ensure that ICMS performance is not significantly degraded as users are added. The migration will continue until all users are fully migrated.
- 23 Prior to releasing drop 1 to Telecom, EDS & IBM will complete a full performance benchmark in Rochester USA, in order to assess the impact of the changes on ICMS before they are introduced in production.

## The need for a variation

- 24 The volume of work required to meet the December 31 data separation milestone is enormous. It is an order of magnitude larger than was anticipated at the time the Undertakings were signed, and as a standalone programme, requires more changes to our systems environment and business processes than any other programme we have delivered in the past decade.
- 25 Within ICMS alone for example, we have had to review over 3,000 individual screens, 2,800 reports and 18,000 ICMS objects. ICMS manages 2.95 million accounts every month and is not a relational database. This means it is not a case of simply identifying and flagging a category of data and applying a change to that category of data across the system. Rather we need to find each occurrence of the data and flag it individually for each given situation.
- 26 Further, because ICMS has over 200 other systems interfacing to it, we had to review all of those as well to gain understanding of the upstream and downstream impacts that could occur as a result of system changes.

## There are six major programmes of work due to be delivered by 31 December 2009

- 27 As the current project stands, most of the work – and in particular, most of the integration testing - will occur in late 2009, at the same time as we are delivering five other major regulatory projects which impact on the same systems and systems environments we need to change for data separation:
- (i) Inventory Management EOI building block;
  - (ii) New Retail primary line voice service using EUBA;
  - (iii) Chorus 2009 equivalence requirements;
  - (iv) Wholesale 2009 equivalence requirements; and
  - (v) New Retail broadband service consuming EUBA/BUBA;
- together the “**December 2009 Schedule 1 Programmes**”
- 28 Each of these represents a milestone in Schedule 1 of the Undertakings which must be delivered by 31 December 2009, and each is central to the Undertakings and to the delivery of equivalence to the industry. Further, each has follow-on milestone within Schedule 1 that are reliant on it being delivered on time.
- 29 For example, the Inventory Management programme 31 December 2009 milestone is necessary to enable Telecom to begin migrating inventory data out of existing systems such as ICMS, which is a key requirement for full EoI. There are two further Schedule 1 milestones that are directly dependant on Telecom meeting the 31 December 2009 inventory management milestone, in June 2010 and June 2011. Other initiatives required by the Undertakings that are directly linked to Inventory Management capability being available on 31 December 2009 are Service Order Management and WorkForce Management.

**The complexity of managing these six programmes together means the level of risk to each programme, and to Telecom's overall systems environment is too high**

- 30 The sheer complexity of launching the December 2009 Schedule 1 Programmes into a systems environment that we are re-coding and separating at exactly the same time creates what we consider to be unacceptable risk for all six programmes of work, and for the continued day to day operation of Telecom's systems. We simply cannot support the level of integration testing or manage the significant potential for project contention that would be required to successfully deliver all six programmes to the same date, and have therefore made the decision to seek a variation in order to reduce overall risk levels for these programmes.
- 31 ICMS, for example, supports over 800,000 transactions per hour for our Chorus, Wholesale and Retail customers, and is central to all six programmes of work. One problem with the code being released into ICMS by any of those programmes could cause all six to be delayed or, in a worst case scenario, bring down the entire ICMS systems.
- 32 In these circumstances, we firmly believe that the alternative course of action – aiming to deliver all six programmes to a 31 December 2009 completion date – would be irresponsible. It would require that we condense the timelines for key integration and business acceptance testing far beyond what we consider prudent. This significantly increases the risk that one or more of the programmes will conflict with existing code and or business/industry processes, which would result in that programme – and any of the other six which share code or other objects with it being removed from production and potentially delayed. Given the proximity of the milestone date to Christmas and the industry's network and system brownout period, any delay will likely be measured in months not weeks.

**We believe a variation to the date for completion of the data separation programme is the best way to mitigate this risk level**

- 33 The congestion and risks we have identified in the second half of this year have resulted in a number of non-regulatory programmes being deferred or cancelled. However, we still need to further de-risk the release programme by deferring one of the six major Undertakings-related programmes being delivered in that period.
- 34 Of the six programmes of work, the five December 2009 Schedule 1 Programmes all form part of what is an inter-dependent transition towards full equivalence. There are strong inter-dependencies between a number of them and all have future milestones which are dependant on their completion. The Chorus and Wholesale December 2009 equivalence requirements for example, are dependant on the Inventory Management building block being completed. Similarly, the Retail primary line replacement and new broadband service programmes require the Chorus and Wholesale December 2009 equivalence requirements to be completed. Delays in any of these programmes will impact our Chorus and Wholesale customers, and the transition to equivalence.
- 35 In contrast, the Data Separation programme is a discrete programme that does not feed in to any other equivalence-related milestones, but is simply designed to cover off the last remaining risk of systemic misuse of CCI within Telecom. As a result of the significant work already done by Telecom and the IOG to protect CCI and CI within Telecom's systems, we are confident that

there is no systemic misuse of CCI occurring today, and that a delay to the completion date for this work will have minimal impact, if any, on our Chorus or Wholesale customers.

- 36 We consider that a staged approach to Data Separation – which sees most of the systems being compliant by the December date as well as 75% of the highest-usage screens with ICMS, and the rest made compliant over a further nine month period – best manages these risks.

#### **Case study of contending programmes: July 2008**

- 37 In July 2008, Telecom implemented two major regulatory programmes of work into our systems environment at the same time – the launch of EUBA, and the WAVE 1 systems changes. During the release, a significant fault was discovered that needed to be fixed during the release window or have part of the release backed out of ICMS. Because ICMS Wave 1 and EUBA shared the same ICMS objects, it was not possible to back out one without the other. This highlights the risks associated with programmes being inextricably linked within the same releases.

- 38 The 56 systems touch every aspect of Telecom’s business, and each is inter-dependant with other systems and processes meaning for every system we need to:

38.1 review all of the data in that system, all of screens viewable in it;

38.2 identify and review all of the reports and business uses for that system;

38.3 design and build the solution for each system including any code changes required;

38.4 put the solution into production, and test that it is compatible with it.

#### **Incidental technical PSTN Systems**

- 39 As work has progressed in the Data Compliance Programme, we have gained a greater understanding of the systems and the work that is required. There is a group of aging PSTN systems that contain extremely technical information about the PSTN, which are old and difficult to change. A list of these systems, and the information they contain, is provided at Annex 3. As an example however, these systems record what copper bearer or NEAX port a particular line is associated with, and record the line numbers affected by any particular network fault event.

- 40 The information is not of a nature that could provide any party with a competitive advantage, and is not used by frontline retail staff (except those staff working in Telecom’s 111 Emergency Call Centre) or by marketing staff, yet the cost of rigidly partitioning it is extremely high.

- 41 Further, given their age, if Telecom were required to logically separate these systems, there is a risk to system function.

- 42 We propose to comply with the Undertakings in respect of these systems by putting in place reasonable non-technical solutions to limit access to the systems to those people who have an operational need to access them. These measures will include:

- 42.1 Reducing access to those who genuinely need to access the system;
- 42.2 Putting in place additional training for users of these systems to increase awareness of obligations;
- 42.3 Requiring users of these systems to sign acknowledgement that use of system must be compliant with the Undertakings;
- 42.4 Periodic monitoring to ensure access remains compliant;
- 42.5 Reporting any inappropriate access to the Honesty Box.

## **FAIMS**

- 43 Finally, there is one system, called FAIMS, for which an effective separation solution is still being defined. FAIMS is a legacy system used for fault reporting and circuit inventory for a number of data services, including ISDN, Leased lines, data circuits, FR, ATM, One Office. It is a particularly proprietary system, and there are an extremely limited number of personnel (two) able to re-programme FAIMS code (this is largely a result of the original design of FAIMS, which saw the entire code written in a single stream). There are approximately 165 users throughout Telecom who need access to FAIMS. However, it is also possible for users to access information directly from the database without going through the front end application.
- 44 EDS has been asked to build and deploy an "Impersonation Tool" which will capture the IP address of those that access FAIMS, so that we can establish clearly both front end application users and back-end database / script users.
- 45 Due to resource contention with other Undertakings' deliverables this tool is not scheduled to be deployed until October 2009. Therefore any solution design or planning prior to this user information will have an element of risk.
- 46 We therefore propose a variation to enable Telecom to present a plan for protection of CCI within FAIMS to the IOG by 31 December 2009.
- 47 This would provide time for us to switch on the impersonation tool in October, log information for at least one month, then develop requirements and a design before the end of the year.
- 48 Our expected approach is that we will then:
  - 48.1 Lock out all write-access to FAIMS except for T&SS users;
  - 48.2 Lock down the database to so that the only user access is via the front end application; and
  - 48.3 Develop a set of reports / web services for those need read access, restricted to information that they are allowed to see.
- 49 We expect to be able to deploy this capability in September 2010, but as noted above, we are not able to be certain of this until the impersonation tool has been switched on and its results analysed in October.

## CONSEQUENTIAL CHANGES TO SCHEDULE 1 OF THE UNDERTAKINGS

- 50 Attached to this document as Annex 2 is a marked-up version of the Undertakings showing all of the changes needed to the Undertakings to reflect our proposed new approach. We summarise the changes below.

### Delayed Milestones

Milestone	Telecom's shared information systems are upgraded to prevent ANS Unit and Wholesale Unit Customer Confidential Information being accessed by Employees in the ordinary course of business, except as expressly permitted by 33, 58, 88.4 and 88.5
Date	Moved from 31 December 2009 to 30 September 2010.

Milestone	From 1 July 2008 until 31 December 2009, any ANS Unit or Wholesale Unit Customer Confidential Information so accessed by Employees will not be used or disclosed in a manner that is contrary to these Undertakings
Date	Moved from 31 December 2009 to 30 September 2010
Comments	Change is necessary in order to line up with extension above.

### New tracking milestones:

The following systems will be upgraded to prevent ANS Unit and Wholesale Unit Customer Confidential Information being accessed by Employees in the ordinary course of business, except as expressly permitted by 33, 58, 88.4 and 88.5, by 31 December 2009:

System Name	Information within system
PROBE	Database which enables recording and analysis of custom data. Also used to provide tools and packages to support marketing activities.
TRIAD	Decision support data warehouse that allows users to report on data downloaded from other databases.
Singl.eview	Rating and billing platform.
CTMS	Incident and fault management system.
SDG Vantive	Incident and fault management system.
Docs Online	Stores internal information.
Project Central	Stores internal information.
Telecom Exchange	Stores internal information.
Integrated Front Office	A common presentation layer for customer-facing applications such as customer management, sales, provisioning and faults
Petunia 2 and 3	Petunia 2 tests customers' DSL details, Petunia 3 is a billing tool.
Actuate Reporting	Business Intelligence systems reporting on Retail services such as mobile and 0800 numbers
Proviso	Information about equipment within Telecom network and provides alarm when thresholds breached.
Geographic Access Pricing	Maps addresses against geographic marketing boundaries
NetMAP	Contains inventory of outside plant assets owned and/or operated by Telecom.

PDMC	Contains inventory of outside plant assets owned and/or operated by Telecom.
AIN	Provides management service for VPN and WAC (Wide Area Centrex)
GeneCIS	Used by Retail Credit and Collections team to manage customer collections.
BCMS	Stores details of business cases.
People Management Process	A legacy HR system – the Intranet version of the old Employee Information System (EIS). Contains employee and position description information. (The non-Intranet version of EIS has been migrated to SAP)
BillView Online	Allows customers to see own bills online.
CARS	Reconciles services provisioned against services billed.
Computerland Peoplesoft	Contains historical financial and procurement information for legacy Computerland services.
Reg Gen-i Peoplesoft	Contains historical financial and procurement information for legacy Gen-i services.

The following systems will be upgraded to prevent ANS Unit and Wholesale Unit Customer Confidential Information being accessed by Employees in the ordinary course of business, except as expressly permitted by 33, 58, 88.4 and 88.5, by 30 June 2010:

<b>System Name</b>	<b>Information within system</b>
AXIOSS/FSS	Fulfilment support for broadband and NGN users.
SOAP	is used for provisioning and allows entry of commands to be processed by the AutoSOD system and then on to NAS supporting manual manipulation of service orders.
BUBBLE	As per SOAP
On Demand	Stores billing images from ICMS
TIPS	An investment planning and management tool that provides a consolidated view of all in-flight and pipeline investment in NZ.
Service Assistant	Information on both planned and unplanned service-impacting events,
SAP Business Warehouse	Provides business warehousing information via one-source data store for strategic management information.
SAP R3 Cost Centre Reporting	Contains modules such as HR Payroll, etc.
TM1	Front end for SAP business warehouse.
CAMS/Digital workflow	EDS owned system which Telecom uses to track changes to its systems.

The following systems will be upgraded to prevent ANS Unit and Wholesale Unit Customer Confidential Information being accessed by Employees in the ordinary course of business, except as expressly permitted by 33, 58, 88.4 and 88.5, by 30 September 2010:

<b>System Name</b>	<b>Information within system</b>
ICMS	holds all our customer records as well as the details of the services a customer has with Telecom.
TCDATA	Provides quotation entry of data circuit orders, provisioning (or engineering) for the management fo service delivery and data circuit billing of Telecom National Leased data circuits.
Wireline	Used for provisioning Retail and Wholesale customers.
Open Up Time	Contains information on customer reported faults
Network Dimensioning System	Contains network performance information which is cut into a number of different reports to which different Active Directory groups are given access
ONDP	Used for provisioning Retail and Wholesale customers.
Safecopy	A secure file download application for transferring files between Telecom and its customers
FTP Server	A shared file server containing FTP files to which different AD groups are given access

Telecom will present a detailed plan for upgrading the following system to prevent ANS Unit and Wholesale Unit Customer Confidential Information being accessed by Employees in the ordinary course of business, except as expressly permitted by 33, 58, 88.4 and 88.5:

<b>System Name</b>	<b>Information within system</b>
FAIMS	Logs, tracks and reports customer reported faults and customer requested moves/adds/changes for enhanced services.

#### **New clause 9.3(e) (iv)**

<b>PSTN System Name</b>	<b>Information within system</b>
NetEvents	Used for recording plan affected by faults and the customers impacted by the faults.
SED	Used in conjunction with NetEvents.
NetRec	Allows for configuration of the PSTN and provides off-line records for some network elements.
NetConfig	Part of a suite of applications holding network configuration data.
NetBuild	Part of a suite of applications holding network configuration data.
Spanlines/Transman	Contains a record of 2Meg connections over copper
NetSOC	Holds a list of the network objects in the network and provides information on state of network performance.
WMS	Field force management tool which hands work requests to service companies.

TLRD	Shows the logical configuration of the transport network, provide outage impact reports for bearer outages and work orders to maintenance staff involved in installing bearers.
NetReport	Reports on performance and configuration of the network
BORG	Contains network performance and availability information for a range of network services.
NTS	Enables remote testing of the copper network
NFWMS	Allows field force personnel/service companies to complete line tests
OTIS	Used to configure the PSTN

## **Other matters – minor corrections**

- 51 Since the Undertakings were accepted by the Minister, Telecom has become aware of some minor errors contained within the Undertakings. We have set these out below and ask the Minister to approve the necessary changes to the Undertakings.

### ***Clause 16, Schedule 1***

- 52 Clause 16 of Schedule 1 of the Undertakings requires Telecom Retail to Stop Innovation on certain listed services by 31 December 2008 and withdraw those same services by 31 December 2009.
- 53 One of the services listed is “Metro IP”, which and was listed in error and is actually a Wholesale service. Therefore there is no ability for Telecom Retail to withdraw this service.
- 54 We therefore request that the references to Metro IP be deleted.

### ***Outlier Broadband Products***

- 55 Clause 14, Schedule 1 of the Undertakings requires Telecom to commit to a migration plan for Outlier Broadband Products. The migration plan requires that all orders for Outlier Broadband Services received after 31 December 2009 be provisioned using Outlier Broadband Services that are based on a Telecom Retail Broadband Service that consumes BUBA or EUBA delivered to the December 2009 Requirements standard as an input.
- 56 Outlier Broadband Products are defined, and include the “SecureMe” service. As with Metro IP, subsequent analysis has identified that its inclusion in the definition of “Outlier Broadband Services” was an error. SecureMe is a security product made up of customer premise-located hardware and software which protects the customer from viruses (i.e. it acts as a firewall) and has not and never will “consume” a Telecom Retail or Telecom Wholesale broadband service. This makes the current Undertakings requirement nonsensical and redundant, and we therefore request that the references to SecureMe be deleted.

### ***Product Management EOI Building Block***

- 57 Finally, in clause 2.8 of Schedule 1 of the Undertakings “Product Management EOI Building Block Completed” is defined. It includes a requirement that:
- “(a) the product catalogue of services in relation to the Relevant Service is visible to Service Providers and Telecom Business Units through the B2B Gateway and Online Portal...”*
- 58 The B2B Gateway is defined in Schedule 1 but essentially is an automated machine to machine interface. It is not a suitable mechanism for publishing information for people to access. Clause 2.8(a) should mirror the wording of clause 2.8(c), which requires the information to be published through the Online Portal or Internet website of the Telecom Business Unit.

## Annex 1: Proposed Changes to Undertakings

### Clause 9.3

9.3 The following transitional provisions apply to these Undertakings:

- (a) to the extent that clause 32 requires the ANS Unit to have written arrangements in place for the supply to other Telecom Business Units of Relevant Network Asset Services that the ANS Unit does not provide to Service Providers, Telecom will use its best endeavours to have those arrangements in place as soon as possible, but by no later than 31 December 2008;
- (b) to the extent that clause 57 requires the Wholesale Unit to have written arrangements in place for the supply to the Retail Units of Relevant Wholesale Services that the Wholesale Unit does not provide to Service Providers, Telecom will use its best endeavours to have those arrangements in place as soon as possible, but by no later than 31 December 2008;
- (c) to the extent that clause 96 requires arrangements with agents and contractors, Telecom will use its best endeavours to have those arrangements in place as soon as practicable but, subject to clause **Error! Reference source not found.**, by no later than 31 December 2008;
- (d) to the extent that clause 97 requires Telecom to obtain the agreement from a person (whom Telecom has, prior to the Approval Date, contracted with to operate Telecom's assets or perform Telecom's functions or activities in respect of Relevant Services) to be subject to the same obligations as an Employee working for the Telecom Business Unit whose business is being outsourced under that contract, Telecom will use its best endeavours to have those arrangements in place as soon as practicable but, subject to clause 9.4, by no later than 31 December 2008;
- (e) in relation to clauses 33, 58, 88.4(c) and 88.5(c), Telecom will ensure that in respect of access by Employees to information contained in shared information systems (including those Telecom systems called ICMS, FAIMS, TCDATA, Probe, AXIOSS and TRIAD at the Approval Date) in the ordinary course of business:
  - (i) from 1 July 2008 until 30 September 2010 ~~31 December 2009~~, any ANS Unit or Wholesale Unit Customer Confidential Information so accessed by Employees will not be used or disclosed in a manner that is contrary to these Undertakings;
  - (ii) by 30 September 2008, it has developed a plan for upgrading or migrating its shared information systems to meet the

requirements in clause 9.3(iii), and provided that plan to the IOG;

- (iii) subject to clause 9.3(e)(iv), by 31 December 2009 30 September 2010, Telecom's shared information systems are upgraded in accordance with the commitments contained in the migration plan in Part A of Schedule 6 to prevent ANS Unit and Wholesale Unit Customer Confidential Information being accessed by Employees in the ordinary course of business, except as expressly permitted by clauses 33, 58, 88.4 and 88.5;
- (iv) by 31 December 2009, the systems listed in Part B of Schedule 6 will be deemed compliant with clause 9.3(e)(iii) as long as Telecom has put in place:
- restrictions to ensure that only users who require access in the ordinary course of business are permitted to access those systems;
  - a requirement that users of those systems acknowledge that any ANS Unit or Wholesale Unit Commercial Information or Customer Confidential Information so accessed by Employees will not be used or disclosed in a manner that is contrary to these Undertakings;
  - additional training for users of those systems on the information sharing requirements of the Undertakings; and
  - systems and process to confirm that only users who require access in the ordinary course of business are permitted to access those systems.

**Schedule 6 – Telecom Shared Information Systems**

**Part A**

<b><u>Shared Information System migration milestone obligation</u></b>	<b><u>Date by which milestone obligation must be achieved</u></b>	<b><u>Status of milestone obligation</u></b>
<p><u>The following systems will be upgraded to comply with clause 9.3(e)(iii) by 31 December 2009:</u></p> <ul style="list-style-type: none"> <li>- <u>PROBE</u></li> <li>- <u>TRIAD</u></li> <li>- <u>Singl.eview</u></li> <li>- <u>CTMS</u></li> <li>- <u>SDG Vantive</u></li> <li>- <u>DOCS Online</u></li> <li>- <u>Project Central</u></li> <li>- <u>Telecom Exchange</u></li> <li>- <u>Integrated Front Office</u></li> <li>- <u>Petunia 2 and 3</u></li> <li>- <u>Actuate Reporting</u></li> <li>- <u>Proviso</u></li> <li>- <u>Geographic Access Pricing</u></li> <li>- <u>NetMAP</u></li> <li>- <u>PDMC</u></li> <li>- <u>AIN</u></li> <li>- <u>GeneCIS</u></li> <li>- <u>BCMS</u></li> <li>- <u>People Management Process</u></li> <li>- <u>BillView Online</u></li> <li>- <u>CARS</u></li> <li>- <u>Computerland Peoplesoft</u></li> <li>- <u>Red Gen-i Peoplesoft</u></li> </ul>	<p><u>31 December 2009</u></p>	<p><u>Tracking Milestone</u></p>

<p><u>The following systems will be upgraded to comply with clause 9.3(e)(iii) by 30 June 2010</u></p> <ul style="list-style-type: none"> <li>- <u>AXIOSS/FSS</u></li> <li>- <u>SOAP</u></li> <li>- <u>BUBBLE</u></li> <li>- <u>On Demand</u></li> <li>- <u>TIPS</u></li> <li>- <u>Service Assistant</u> <u>SAP Business Warehouse</u></li> <li>- <u>SAP R3 Cost Centre Reporting</u></li> <li>- <u>TM1</u></li> <li>- <u>CAMS/Digital workflow</u></li> </ul>	<p><u>30 June 2010</u></p>	<p><u>Tracking Milestone</u></p>
<p><u>The following systems will be upgraded to comply with clause 9.3(e)(iii) by 30 September 2010</u></p> <ul style="list-style-type: none"> <li>- <u>ICMS</u></li> <li>- <u>TCDATA</u></li> <li>- <u>Wireline</u></li> <li>- <u>Open Up Time</u></li> <li>- <u>Network Dimensioning System</u></li> <li>- <u>ONDP</u></li> <li>- <u>Safecopy</u></li> <li>- <u>FTP Server</u></li> </ul>	<p><u>30 September 2010</u></p>	<p><u>Tracking Milestone</u></p>
<p><u>Subject to clauses 9.3(e)(iv), by 30 September 2010, Telecom's shared information systems are upgraded in accordance with the commitments contained in the migration plan in Part A of Schedule 6 to prevent ANS Unit and Wholesale Unit Customer Confidential Information being accessed by Employees in the ordinary course of business, except as expressly permitted by clauses 33, 58, 88.4 and 88.5</u></p>	<p><u>30 September 2010</u></p>	<p><u>Enforceable Milestone</u></p>
<p><u>Telecom will provide to the IOG a plan for upgrading FAIMS to comply with the obligation in clause 9.3(e)(iii)</u></p>	<p><u>31 December 2009</u></p>	<p><u>Enforceable Milestone</u></p>
<p><u>Telecom will ensure FAIMS complies the obligation in clause 9.3(e)(iii)</u></p>	<p><u>The date specified in the plan for upgrading FAIMS</u></p>	<p><u>Enforceable Milestone</u></p>

## **Part B**

The following systems will be deemed compliant with clause 9.3(e)(iii) as set out in clause 9.3(e)(iv):

- NetEvents
- SED
- NetREc
- NetConfig
- NetBuild
- Spanlines/Transman
- NetSOC
- WMS
- TLRD
- NetReport
- BORG
- NTS
- NFWMS
- OTIS
- Any other systems of a similar nature to those listed above that Telecom and the IOG agree are appropriately dealt with by clause 9.3(e)(iv).

**Annex 1 (continued) Changes to Undertakings for minor corrections**

**Clause 1.1, Schedule 1:**

*Outlier Broadband Products* means the Telecom services called (as at the Approval Date) Remote Office, ~~SecureMe~~, School Zone Starter and Eftpos Service;

**Clause 2.8, Schedule 1:**

- 2.8 *Product Management EOI Building Block Completed* means for a particular Relevant Service and a particular Telecom Business Unit:
- (a) the product catalogue of services in relation to the Relevant Service is visible to Service Providers and Telecom Business Units through the ~~B2B Gateway and Online Portal~~ or the Internet website of the Telecom Business Unit;
  - (b) the product catalogue contains definitive information on the specification, price, order mechanisms, availability, geographic coverage and service level options (if any) in relation to the Relevant Service;
  - (c) the Product Plans of Intent and Product Plans of Record (if any) for the Relevant Service are visible to Service Providers and other Telecom Business Units through the Online Portal or the Internet website of the Telecom Business Unit; and
  - (d) the Manager of the ANS Unit or the Manager of the Wholesale Unit (as relevant) has certified to the Commission in writing that the conditions (a), (b) and (c) above are met;

**Clause 16.1, Schedule 1**

- 16.1 Rather than redesigning Other Legacy Data Services to consume EOI inputs, Telecom commits to the following alternative migration plan:

<b>Other Legacy Data milestone obligation</b>	<b>Date by which milestone obligation must be achieved</b>	<b>Status of milestone obligation</b>
---	--	---------------------------------------

Other Legacy Data milestone obligation	Date by which milestone obligation must be achieved	Status of milestone obligation
<p>The Retail Units will Stop Innovation and Stop Sell to New Customers for all of the following services:</p> <ul style="list-style-type: none"> <li>• DSTN Services;</li> <li>• X25; and</li> <li>• Netway Integrated Access.</li> </ul>	31 December 2007	Enforceable Milestone
<p>The Retail Units will Stop Innovation for all of the following services:</p> <ul style="list-style-type: none"> <li>• Analogue Data services;</li> <li>• ATM;</li> <li>• Corporate Internet Data;</li> <li>• Dedicated Internet Access;</li> <li>• High Speed Digital Data (using ATM);</li> <li>• IP Net;</li> <li>• Lanlink;</li> <li>• Megalink;</li> <li>• <del>Metro IP</del>; and</li> <li>• MetroLAN Extension.</li> </ul>	31 December 2008	Enforceable Milestone
<p>The Retail Units will Withdraw Service for DSTN Services.</p>	31 December 2008	Enforceable Milestone
<p>The Retail Units will Withdraw Service for all of the following services:</p> <ul style="list-style-type: none"> <li>• X25; and</li> <li>• Netway Integrated Access.</li> </ul>	30 June 2009	Enforceable Milestone

Other Legacy Data milestone obligation	Date by which milestone obligation must be achieved	Status of milestone obligation
<p>The Retail Units will Stop Sell to New Customers for all of the following services:</p> <ul style="list-style-type: none"> <li>• Analogue Data services;</li> <li>• ATM;</li> <li>• Corporate Internet Data;</li> <li>• Dedicated Internet Access;</li> <li>• High Speed Digital Data (using ATM);</li> <li>• IP Net;</li> <li>• Lanlink;</li> <li>• Megalink;</li> <li>• <del>Metro IP</del>; and</li> <li>• MetroLAN Extension.</li> </ul>	31 December 2009	Enforceable Milestone

## Annex 2: BT Experience

Similar to Telecom's obligations, BT must partition CI and CCI in its shared information systems to meet the information sharing rules. However, BT's obligations are generally premised on the idea that systems will ultimately be physically separated. Logical separation of systems (to limit user access) is an interim step.

BT's system separation obligations apply to:

- **Operational Support Systems (OSS)** – which are support systems that carry out functions and processes which help run a network and business, including customer ordering, configuring network components, creating a bill and managing faults;
- **Management Information Systems (MIS)** – which are management information systems which hold CI or CCI and which are used by BT to help plan and direct business and organisation operations, decision making and competitive strategy; and
- Any **other systems** that hold CI and CCI.

BT's obligation to "logically separate" its systems (also variably called "User Access Control" and "Level 1 Separation") requires implementation of user access controls to limit access to information in accordance with the information sharing rules. This type of separation is similar to the approach being taken by Telecom to meet the requirements of clause 9.3(e)(iii).

BT was given 1-2 years to achieve logical separation of OSS and MIS, and about 4 ½ years to achieve full separation of OSS and MIS. However, through a number of variations and exemptions to BT's undertakings, these timeframes have been extended slightly, and numerous systems have been carved out from the general separation requirements.

Key messages from the BT experience include the following:

- Logical separation was originally assumed to take 12 – 26 months. This timeframe has been extended to 13 – 26 months, with exceptions for particular systems for up to 4 years;
- Physical separation was originally assumed to take at least 4 ½ years. While this timeframe has been retained, at least 11 systems have been exempted from the obligation to physically separate;
- Separation of systems between BT Wholesale and downstream division had no set timeframe, with completion required "as soon as possible"; and
- The extensions of timeframe and/or system carve outs have been coupled with migration plans and audit requirements;