

Description of the Services to be Procured Pursuant to the TRAS Contract

The text of this service description is intended to be the same in both the SPAA and the DCUSA. In this text, references to "**Suppliers**" are references to licensed electricity suppliers and licensed gas suppliers collectively (and references to a "**Supplier**" are to one of them).

1. Theft Risk Assessment Methodology (TRAM) Overview

1.1 The TRAS Service Provider's TRAM is a two stage process established in accordance with the TRAS Contract.

- **Stage 1:** Identifies low consumption customers ("**Outliers**") by comparing actual consumption at a supply point against a modelled consumption for that property/customer type ("**Classification**"). Classifications will be constructed based on the TRAS Service Provider's data sets covering property type and occupant information. The TRAS Service Provider will use its data to calculate expected consumption for each Classification. By processing actual consumption data compared to expected consumption data pertaining to a given Classification per Supply/Metering Point, this will generate the low consumption Outlier file.
- **Stage 2:** Qualification of Outliers by looking for markers which indicate a motivation and propensity for a customer to perpetrate theft. Such qualification will be undertaken using the TRAM decision engine which will apply scorecards based on customer and property variables from both Supplier and TRAS Service Provider data sources such as property, credit and fraud. Such scorecards will rank Outliers based on their propensity to be committing theft, which will subsequently be provided to relevant Suppliers ("**Qualified Outliers**").

1.2 The TRAS Service Provider will refine those aspects of the TRAM which are within its control based on:

- actual data gathered in year 1 of operation; and

- analysis performed on Qualified Outliers and associated outcomes across all Suppliers as consolidated within the "**Supplier Data Warehouse**" (as defined in the TRAS Contract); and
- publicly available industry data where appropriate.

- 1.3 The TRAS Service Provider will use the data recorded in its theft alert and case management system ("**Hunter System**") to see a consolidated cross Supplier perspective on theft trends in a way that will not compromise security of Supplier Data between Suppliers. The TRAS Service Provider will use this to identify theft hotspots enabling further refinement of the TRAM.
- 1.4 The TRAS Service Provider will analyse the theft trends and patterns to enable evaluation and fine-tuning of the detection rules.
- 1.5 The TRAS Service Provider will use the Hunter System tools to analyse the comparative performance of each Supplier's theft investigations to identify areas of best practice.

2 Theft Target Overview

The TRAS Service Provider will use a data and analytics driven approach to establishing the Theft Target.

- 2.1 Within 12 months of the services start date (as defined in the TRAS Contract) using the theft target methodology developed during the initial 9 months after go-live date under the TRAS Contract, the TRAS Service Provider will establish separate annual targets for the detection of theft of gas and electricity for the gas and electricity supply markets (the "**Theft Target**").
- 2.2 The TRAS Service Provider will recalculate the Theft Target every twelve months thereafter using the theft target methodology (and making any refinements required to the methodology based on operational experience) and deliver this to SPAA Ltd and DCUSA Ltd for their agreement recognising the expectation that any revised Theft Target supports further reductions in theft of gas or electricity when compared to the existing Theft Target.

3 **TRAS Service Provider Solution Overview**

- 3.1 The TRAS Service Provider solution will accumulate energy usage and customer information, creating a history of activity for each meter point in Great Britain. The primary sources for such data will be the Supplier Data Files, input from the 'tip-off line' and investigation results data from Suppliers.
- 3.2 Data standardisation and quality check routines developed pursuant to the TRAS Contract convert and verify the Supplier Data Files, provided in computer readable formats, agreed separately with each Supplier.
- 3.3 Supplier Data Files will be sent to the TRAS Service Provider via a Secure Transfer System in a format agreed individually with each Supplier. The data will be standardised. The TRAS Service Provider will provide Supplier management information reports regarding the success of each Supplier's data file load.
- 3.4 The initial Supplier Data File (to be provided between 30 June and 31 July 2015) will be used in conjunction with the TRAS Service Provider Data to create commercial and residential peer group classifications which the TRAS Service Provider will use to calculate normalised consumption figures for each Classification.
- 3.5 The TRAS Service Provider solution will utilise data matching and comparison algorithms which will compare consumption figures contained within Supplier Data Files to an expected consumption model. If a statistically significant variation is detected, such variation will be identified by the TRAS Service Provider as consumption and written to the Outliers File for further processing against the scorecards by the TRAM decision engine.
- 3.6 The TRAS Service Provider will develop "**Service Output**" from both the data contained in Supplier Data Files and TRAS Service Provider data. Service Outputs will contain that information required to assign Qualified Outliers to the correct Supplier. The TRAS Service Provider will provide a summary of the components, rationale and resulting data variables used to create Qualified Outliers.

- 3.7 The TRAS Service Provider will deliver Service Output to Suppliers via its Hunter System or via the Secure Transfer Service "STS" interface. The method of delivery will be agreed with SPAA Ltd and DCUSA Ltd.
- 3.8 The TRAS Service Provider will make available a 24 hour, 7 days a week 'tip-off line' for the public to report energy theft. This information will be collated, , the Supplier(s) identified and the tip-off information will be processed monthly against the TRAM then the tip-off leads will be distributed to the relevant Suppliers with their monthly Qualified Outliers.

4. Operation of TRAS Service Provider Solution

- 4.1 Key interaction points between Suppliers and the TRAS Service Provider shall be measured from an agreed cut-off point each month. The key interaction points between The TRAS Service Provider and each Supplier are identified in table 1 below:

Table 1 (Supplier and TRAS Service Provider Key Interaction Points)

Calendar Day	Outline Service Level Definition
Supplier Data Cut-Off Point	The point at which all Suppliers will set their data extracts being fifth calendar day of each month for electricity and the fifth gas day of every month for gas.
Data File Delivery Date (DFDD)	The latest date each month by when the Suppliers must submit their Supplier Data Files to the TRAS Service Provider's STS which is defined as 17:00 hours on the fifth working day following the Supplier Data Cut-Off Point.
DFDD+1 to DFDD+8	TRAS Service Provider validates, converts, undertakes quality checks and loads Supplier's Data Files into the TRAS Service Provider solution.
DFDD+9	TRAS Service Provider makes available the monthly data file Management Information reports to the Supplier STS instances and notifies nominated Supplier contacts via

		email.
DFDD+9	to	Theft Lead processing – Outliers identified, TRAS Service Provider data introduced, TRAM process completed.
DFDD+26		
DFDD+27		Qualified Outliers delivered to Suppliers via the Supplier Hunter System or STS interface.
DFDD+29		Monthly output service level report provided to SPAA Ltd and DCUSA Ltd.

- 4.2 The TRAS Service Provider will host the infrastructure required to operate TRAS architecture within its data centre.
- 4.3 The TRAS Service Provider will provide a frontline help desk to receive calls, log them and handle issue escalation as identified in the TRAS Contract.
- 4.4 The TRAS Service Provider will provide a dedicated team who will undertake the following activities:
- receipt of Supplier Data Files;
 - conversion;
 - quality checks and loads;
 - monthly Supplier Data File reports;
 - management of second line support;
 - database maintenance and fixes;
 - data queries;
 - minor upgrades; and
 - amendments.

4.7 The TRAS Service Provider will provide specialist resource to undertake the following activities:

- analytic activities to annually refresh theft propensity scorecards;
- annual refresh of the residential and commercial segmentation;
- assess performance improvement recommendations;
- perform benchmarking activities; and
- Theft Target definition.

5 DATA PROTECTION AND PRIVACY

The TRAS Service Provider will take steps to ensure that all personal data provided by the Suppliers and held in the Supplier Data Warehouse is accurate and up to date and additionally:

- 5.1 The TRAS Service Provider's compliance team will perform regular reviews of the Supplier data in the Supplier Data Warehouse to ensure the data is amended or deleted when it is no longer necessary for the purposes of TRAS and this will also be communicated to SPAA Ltd and DCUSA Ltd.
- 5.2 The TRAS Service Provider will receive Supplier Data Files and will load these to the Supplier Data Warehouse in accordance with paragraph 3.1 above.
- 5.3 The TRAS Service Provider will validate Supplier data before being loaded to the Supplier Data Warehouse to ensure the data is correctly associated with the correct individual.
- 5.4 The TRAS Service Provider will ensure that sensitive personal data will not be shared between Suppliers; this information will only be available to view by the Supplier who originates the record.
- 5.5 For the TRAS services, appropriate retention periods and justifications will be agreed between Suppliers and the TRAS Service Provider prior to the submission

of ongoing monthly data feeds, and a documented retention schedule will be developed covering Supplier data items.

6 RESILIENCE AND AVAILABILITY

6.1 The TRAS Service Provider solution shall be deployed in such a way as to ensure that the failure of any single hardware component does not affect the availability of any of the services or result in loss of or loss of access to, the services or data.

- a. The TRAS Service Provider shall configure the TRAS Service Provider solution and implement backup procedures so as to ensure that no more than one day's on-line data will be lost as a result of any failure of the TRAS Service Provider solution or services. Any lost Supplier Data shall be recovered or recreated and where required retransmitted to the Suppliers.
- b. The TRAS Service Provider shall implement all necessary measures to ensure that there is no permanent loss of Supplier Data.

7 INFRASTRUCTURE MONITORING

7.1 The TRAS Service Provider shall demonstrate that all parts of the infrastructure used to provide the service are proactively monitored.

7.2 Without prejudice to the generality of paragraph 7.1, the TRAS Service Provider shall:

- a. use an industry recognised proactive monitoring system for both system and network infrastructures;
- b. provide procedures for undertaking trend analysis, problems escalation and capacity management in accordance with the Information Technology Infrastructure Library (ITIL) guidelines;
- c. demonstrate the use of appropriate thresholds depending on the device being monitored and the service being provided; and

- d. configure automatic notification, logging and escalation of potential issues ensuring sufficient time to rectify any problem before it impacts the provision of the services.

8 SYSTEM AND DATA BACKUP

- 8.1 The TRAS Service Provider shall run, and record successful completion within a backup log of, daily backup procedures for all on-line databases. SPAA Ltd and DCUSA Ltd shall be entitled to check on a random basis, subject to a process and frequency agreed with the TRAS Service Provider, that all back-ups are completed and that a backup log is being maintained.
- 8.2 The TRAS Service Provider shall identify each backup and ensure that all backups are held on appropriate media, labelled accurately and clearly, in line with media manufacturer's recommendations and in accordance with the TRAS Contract.
- 8.3 The TRAS Service Provider shall ensure that all backups are secured in offsite locations in fire proof and flood proof, safe environments, appropriate to the type of backup, and in accordance with any recommendations by the media manufacturer.
- 8.4 The TRAS Service Provider shall ensure that all data stored on external media is encrypted.
- 8.5 The TRAS Service Provider shall ensure that backup and recovery procedures do not prejudice achievement of the service levels under the TRAS Contract, and are timed to minimise the risks of loss of data.
- 8.6 The TRAS Service Provider shall ensure that back up recovery times are compatible with service availability requirements.
- 8.7 The TRAS Service Provider shall ensure that all data and software necessary to support the services are backed up at regular intervals in accordance with the requirements of the TRAS Contract.

- 8.8 The TRAS Service Provider shall, at regular intervals, not exceeding three months, test to ensure that, the backup files could be restored if required.
- 8.9 The TRAS Service Provider shall ensure that the system data, including operating system, RDBMS and application software, is backed up at the regular intervals detailed in the disaster recovery plan established under the TRAS Contract to support disaster recovery and archive retrieval procedures.
- 8.10 The TRAS Service Provider shall ensure a full backup is made immediately prior to the installation of a new operating system, RDBMS or application software. A check shall be made as soon as reasonably practical to ensure that the backup files can be restored if required before any changes are made.
- 8.11 The TRAS Service Provider shall operate appropriate library and configuration management systems for the control and management of backups and archives.

9 HARDWARE AND SYSTEM

- 9.1 The TRAS Service Provider shall use hardware which meets the requirements of the TRAS Service Provider Solution as set out in the TRAS Service Provider's Hosting Services Specification and the requirements of this Schedule.
- 9.2 Without prejudice to paragraph 9.1, the TRAS Service Provider shall ensure that the System architecture is scalable. The System architecture shall be designed such that from the Operational Services Commencement Date the Service Levels specified in Schedule 3 will be met after the baseline volumes are increased by up to 40% without the need for an upgrade.
- 9.3 At the time of selection the TRAS Service Provider shall:
- (a) use commercially available hardware wherever possible and shall use the latest stable release of the hardware product; and
 - (b) ensure that there is a demonstrable commitment to the hardware product from the supplier.

10 SOFTWARE

10.1 Subject to TRAS Contract Schedule 17 (Change Management Procedure), the TRAS Service Provider shall use the third party software listed in TRAS Contract Schedule 8 (Software & Escrow).

10.2 The TRAS Service Provider shall:

- (a) use widely available software languages in respect of software development tools;
- (b) remain within the support window of third-party software;
- (c) use commercially available software from an established supplier at the time of selection wherever possible;
- (d) use the latest stable release of the software at the time of selection; and
- (e) ensure there is, at the time of selection, a demonstrable commitment to the software product from the supplier.

11 THIRD PARTY SOFTWARE

If the TRAS Service Provider wishes to use third-party software not listed in the TRAS Contract at the time of its selection, it shall provide to SPAA Ltd and DCUSA Ltd information on the third-party supplier, including their licensing and maintenance arrangements, their product development plans and any restrictions inherent in the usage of the product.

12 PHYSICAL HOSTING AND INFRASTRUCTURE ENVIRONMENT

12.1 The TRAS Service Provider shall provide Data Centre Sites.

12.2 The TRAS Service Provider shall ensure that the Data Centre Site:

- (a) is located within the European Economic Area;
- (b) satisfies the Tier III Data Centres standards for the TRAS Service;
- (c) is located so as to reduce the potential impact of an external incident;

- (d) is protected against fire - the TRAS Service Provider shall demonstrate that the fire suppression used is maintained regularly and conforms to the TRAS Service Provider's health and safety policy;
- (e) is protected against flood - the TRAS Service Provider shall demonstrate that the flood detection system used is maintained regularly and conforms to the TRAS Service Provider's health and safety policy; and
- (f) is maintained in a climate controlled environment - the TRAS Service Provider shall ensure that there is sufficient capacity to maintain the environment within the systems operating temperatures at all times including times of preventative maintenance and failure of any single air conditioning device.

12.3 The TRAS Service Provider shall ensure that shared communication infrastructure either internally or externally is monitored and secure.

12.4 The TRAS Service Provider shall ensure that appropriate procedures are in place to allow preventative maintenance of the system to be carried out without affecting the provision of the services subject to the service levels under the TRAS Contract.

12.5 The TRAS Service Provider shall ensure that all hardware in use in the delivery of the hosting and infrastructure services are clearly labelled enabling easy identification of components.

13 PROVISION OF THE COMMUNICATIONS INFRASTRUCTURE

13.1 The TRAS Service Provider shall provide and use an appropriate network communications infrastructure to support external interfaces to enable the secure transfer of information from the Suppliers.

13.2 The TRAS Service Provider shall in respect of the Suppliers specified by SPAA Ltd and/or DCUSA Ltd:

- (a) provide any software, other than Commercially Off The Shelf (COTS) software, necessary to be resident on a computer on the Supplier's site to support access to the services;
- (b) provide the ability to configure the network allowing for testing for upgrades, outages and disaster recovery tests to take place whilst not affecting the running of the live service in accordance with the service levels under the TRAS Contract; and
- (c) if the TRAS Service Provider uses a common network provider, then the boundaries between the TRAS Service Provider and the common network provider shall be clearly defined and documented; and the TRAS Service Provider shall not be relieved of its obligations under the TRAS Contract.

13.3 If the TRAS Service Provider shares a common network provider with other service providers, the TRAS Service Provider shall remain responsible for its own data transmission.

13.4 The network communications infrastructure shall adhere to good industry practice and not use proprietary standards.

13.5 The network communications infrastructure shall:

- (a) support automatic retry and time out facilities; and
- (b) meet the security requirements as set out in the TRAS Contract.

13.6 Any networking product used shall be a fully supported release of a Commercially Off The Shelf product.

13.7 The TRAS Service Provider shall ensure that there is an audit trail of modifications to all hardware and communications infrastructure.

13.8 The TRAS Service Provider shall ensure that all output files and reports produced are uniquely identifiable and time stamped.