How to source a Mission Critical Service

The purpose of this paper is to assist service providers in their understanding of what mission critical service is and what specific legal frameworks are being used today by governments to ensure that the service is always available. Mission Critical operations are being conducted by Public Protection and Disaster Relief (PPDR) organisations including Police, Fire, Rescue and Health organisations.

July 2013

1. INTRODUCTION

General definition:

- 'Mission Critical' is defined as a function whose failure leads to catastrophic degradation of service that places public order or public safety and security at immediate risk.

The 27 member states of the Law Enforcement Working Party (European Council) have agreed this definition:

- 'Mission critical operations' for PPDR organisations address situations where human life and goods (rescue operations, law enforcement) and other values for society are at risk, especially when time is a vital factor.
  - This means we define 'mission critical information' as the vital information for PPDR to succeed with the operation.
  - 'Mission critical communication solutions' therefore means that PPDR needs secure, reliable and available communication and as a consequence cannot afford the risk of having failures in their individual and group communication (e.g. voice and data or video transmissions).

It is not surprising given the potential impact to the public to find that in addition to specific mission critical functionalities governments require implementations that are resilient, have built in redundancy and excellent coverage coupled with technical solutions for security, reliability and availability there are also extraordinary legal provisions being used to guarantee mission critical service. Examples of today's government's contracts for mission critical voice service are listed below and have commitment periods where 10-15 years are normal and there are even contracts in place that runs into the 2030th.

2. EXAMPLES OF EXTRAORDINARY PROVISIONS

The following are examples of requirements from government customer contracts that are more stringent, or onerous, than obligations typically required by other customers. Because there are so many, the list is divided into three sections – from most stringent to least stringent.

Please bear in mind that the contractual protections required by a government customer will vary according to the type of procurement it is undertaking.

In a straightforward supply contract, a government customer may demand fewer of these onerous provisions. Also, the contractual risks in such a contract may be lower and/or more acceptable to the supplier.

If, however, the procurement is complex (e.g. a PPP deal build/own/operate a nationwide public security network), the risks to the government customer will be much greater. It will seek to pass as much risk as possible to the supplier. In these cases, the government customer is likely to impose very onerous contractual obligations on the supplier. And the risk to the supplier in accepting them is much greater.

2.1 MOST STRINGENT

2.1.1 Parent Company guarantee/Performance Bond: (i) PCG – The supplier's parent company agrees to meet the supplier's financial and/or performance obligations should the supplier fail to do so. (ii) PB – The supplier provides the government customer with a performance bond usually valued at between five and 10 percent of the contract price. The government customer can redeem the bond if the supplier fails to meet its contractual obligations (even if the financial costs of the failure are lower than the value of the bond). Both are standard in government customer contracts.

2.1.2 Intellectual Property: The government customer is to own the rights in any new, project-specific intellectual property developed by the supplier. Often a non-negotiable requirement of the customer. Standard approach.

2.1.3 Liability: Government customer contracts may not include a waiver of consequential and indirect damages, and the overall liability cap may be in excess of contract value. Losses for breach of the confidentiality provisions may be uncapped altogether. Light breaches will in some countries result in liabilities in the order of 500 M€ and in other cases be fully uncapped. Standard provision in many jurisdictions.

2.1.4 Open Book Accounting: The government customer has access to the supplier's financial records in order to see any reduction in the supplier's costs in performing the contract. If costs have reduced, the supplier and government customer will split the "profit". Sometimes the split is 50/50 although it is not uncommon for the government customer to receive the majority of any such profit. Provision is becoming more common.

2.1.5 Most Favoured Customer: The government customer must have the best price. The supplier cannot sell the same (or similar) products and services to another customer at prices lower than those paid by the government customer. Reasonably frequent, but not a standard provision.

2.2 MODERATELY STRINGENT

2.2.1 Step-in: The government customer has the right to take over the performance of the contract in certain circumstances. For example, where the supplier suffers an insolvency event (e.g. insolvency, arrangement with creditors, etc) or commits a material breach of the contract. The supplier is not paid during step-in, and may also have to meet the government customer's additional costs associated with step-in. The government customer may hand back the services to the supplier, or terminate the contract. Provision is becoming more common.

2.2.2 **Termination**: The government customer has extensive rights to terminate, often including termination for convenience. Whereas the supplier will only be permitted to terminate in very limited circumstances (for example, protracted failure to pay undisputed fees). Standard provision.

2.2.3 **Change of Control:** A change of control of the supplier will be subject to the government customer's approval, which often may be withheld at the customer's absolute discretion. In some instances, changes of control are prohibited altogether. Standard provision.

2.2.4 **Financial Strength:** The supplier is required to show financial strength on a regular, ongoing basis. If the supplier's financial strength diminishes, the government customer may terminate the contract. Provision is becoming more common.

2.2.5 **Control over performance:** This is typically very stringent in government contracts – the government customer takes a more involved role than is usual in other contracts, for example in testing and acceptance procedures. In our experience, government customers are slower and less inclined to approve and accept elements of a project than commercial customers, resulting in delayed payment to the supplier. Standard approach.

2.2.6 **Liquidated Damages/Service Credits:** Although they can vary from contract to contract, LD/SC regimes are, in our experience, often more onerous with government contracts as the government cannot allow or afford the project to fail or be delayed, or services to be compromised. Also see comments regarding force majeure events. Standard provision.

2.2.7 **Force Majeure:** Force Majeure Events are often defined much more narrowly than in commercial contracts. For example, industrial action is usually excluded from government customer contracts (although sometimes permitted if it is nation- or industry-wide). Force Majeure clauses may also include a proviso that, due to the very purpose of the contract (i.e. public safety), a circumstance will not be considered a Force Majeure event if the party invoking that event reasonably ought to have taken into account when the contract was signed. Standard provision.

2.2.8 **Export Control** – A US company is responsible for ensuring its products are not exported to prohibited countries. This responsibility extends to onward sale by the company's customers. Government customers will not accept such restrictions imposed on it by another government. Accordingly, standard export control provisions are routinely excluded from government customer contracts. Standard provision.

2.2.9 **Source Code Escrow:** The supplier must place the system source code into escrow with a third party, at the supplier's cost. The source code can be released to the government customer in specified events such as insolvency of the supplier, breach of contract by supplier, etc. Standard provision.

2.3 LEAST STRINGENT

2.3.1 Assignment: The supplier is not usually allowed to assign the contract without the government customer's prior consent, which may be withheld at the customer's discretion. Standard provision.

2.3.2 Security Clearance: The government customer may require certain supplier employees (e.g. those who have access to certain customer sites) to undergo national security clearance. Standard provision.

2.3.3 Data: Recording and retention obligations for data processed under government customer contracts may be subject to specific data protection legislation, which can be quite burdensome. Provision is becoming more common.

2.3.4 Continuous Improvement: The supplier must improve the operation of the system over time at no additional cost to the government customer. Reasonably frequent, but not a standard provision.

2.3.5 Taxes: Contractual obligation on the supplier to regularly pay its taxes. Failure to do so would amount to breach of contract by the supplier. Standard provision.

2.3.6 Confidentiality – Government customers are usually reluctant to agree to standard confidentiality provision, preferring to use their own. Standard provision.