Information Security Strategy

Version 1.0

Publication Date: 01 October 2008

Table of Contents

1. Introduction

On 8 August 2007, the Office of Fair Trading, in exercise of its duty under section 22 Enterprise Act 2002, referred the completed acquisition by Macquarie UK Broadcast Ventures Limited ("MUKBV"), a subsidiary of Macquarie UK Broadcast Holdings Limited ("MUKBH"), of National Grid Telecoms Investment Limited, Lattice Telecommunications Asset Development Company Limited and National Grid Wireless No. 2 Limited (together the "National Grid Wireless Group") to the Competition Commission ("CC").

The CC published its report entitled Macquarie UK Broadcast Ventures Limited/ National Grid Wireless Group: Completed Acquisition on 11 March 2008 (the "Report"). In the Report, the CC concluded that:

- the acquisition had resulted in the creation of a relevant merger situation and that the creation of that situation may be expected to result in a substantial lessening of competition ("SLC") in relation to the markets for the provision of Managed Transmission Services ("MTS") and Network Access ("NA") to television broadcasters and certain radio broadcasters within the UK and that the SLC may be expected to result in the adverse effects specified in paragraph 9.2 of the Report;
- the CC should take action to remedy, mitigate or prevent the SLC and any adverse effects flowing from it and to that end Undertakings should be given to give effect to the CC's decision on remedies specified in the Report.

The CC published a notice of proposal to accept Undertakings on 25 June 2008. In light of responses received to that consultation the CC published a revised proposal on 06 August 2008. No further representations were received and on 01 September 2008 the CC accepted Undertakings in the form consulted on.

Paragraph 16 of the Undertakings contains provisions related to confidentiality of information, including the requirement for Arqiva to publish an Information Security Strategy as set out specifically in paragraph 16.2 which states that "within one (1) month of the Commencement Date, Arqiva shall publish an Information Security Strategy which shall set out the principles for access and use of the confidential information referred to in paragraph 16.1 in the form of a protocol which identifies the different categories of information held by Arqiva and how these will be treated to ensure compliance with paragraph 16.1. The Information Security Strategy shall also require Arqiva to implement appropriate measures:

- to ensure the security of Arqiva's information storage systems and data systems (including data collection, storage and archiving), particularly where confidential information referred to in paragraph 16.1 is stored in systems shared between business units;
- to ensure the physical security of confidential information referred to in paragraph 16.1;
- to ensure that an employee of one business unit does not disclose or use the confidential information referred to in paragraph 16.1 of which the employee had become aware whilst working for another business unit;
- to ensure the security of the confidential information referred to in paragraph 16.1 in the event that Arqiva is a bidder in a spectrum auction in competition with a Customer or prospective customer; and
- to ensure that staff receive adequate training in relation to the Information Security Strategy as part of the education programme pursuant to paragraph 18.5.4."

Paragraph 16.1 of the Undertakings states that “where Arqiva holds confidential information from:

- a Customer in relation to an Existing Transmission Agreement;
- a prospective customer or Customer before, during or after the process of negotiating a New Transmission Agreement pursuant to paragraph 9 and 10 or a renewal pursuant to paragraph 8.1.1; or
- an MTS Provider before, during or after the process of negotiating an agreement for Network Access pursuant to paragraph 11.1,

Arqiva shall use that confidential information solely for the purpose for which it was supplied and shall respect at all times the confidentiality of that information. The confidential information referred to in this paragraph 16.1 shall not be passed on to any other business units, departments, subsidiaries or partners of Arqiva for whom such confidential information could provide a competitive advantage. Nothing in this paragraph 16 shall prevent Arqiva from providing confidential information to the Adjudicator, the DSO Auditor, Ofcom or the Office of Fair Trading.”

By publishing this document Arqiva sets out its Information Security Strategy in line with the requirements of the Undertakings for its treatment of confidential information as defined in paragraph 16 of the Undertakings (“Confidential Information”). Arqiva will further develop and implement this strategy as soon as reasonably practicable as part of the integration of the National Grid Wireless Group.

2. Principles for Access and Use of Confidential Information

The following overriding principles will guide the treatment of Confidential Information by Arqiva.

- The working groups within Arqiva that are required to access and use Confidential Information will be distinct from those for whom such confidential information could provide a competitive advantage. In this sense distinct is intended to mean that the staff will not be shared and will have separate line management, each headed by a separate manager whose personal objectives will include an obligation to ensure that the arrangements set out in the Information Security Strategy are understood and adhered to. In particular, the following business activities will be distinct from the working groups within Arqiva that are required to access and use Confidential Information:
    - staff responsible for the day to day management of Arqiva owned DTT multiplex operations (DTT multiplexes C&D);
    - staff responsible for the day to day management of any bid that Arqiva might consider for a spectrum auction in competition with a Customer or prospective customer (as defined in the Undertakings);
    - staff responsible for requesting and specifying self provision of MTS and/or NA.
- As a key component of ensuring that there are distinct working groups within Arqiva that are required to access and use Confidential Information, contact points into Arqiva for any Customer or prospective customer (as defined in the Undertakings) will be managed through two controlled channels, specifically:
    - a nominated account manager to manage MTS or bundled MTS/NA requirements for transmission services;
    - an identified contact point to manage NA only requirements from prospective MTS providers,

  and staff responsible for these contact points will be distinct from staff responsible for business activities for whom such confidential information could provide a competitive advantage, including the day to day management of DTT multiplexes C&D, any bid that Arqiva might consider for a spectrum auction in competition with a Customer or prospective customer (as defined in the Undertakings), or requesting and specifying self provision of MTS and/or NA.
- Appropriate measures will be implemented and maintained to ensure the security of Confidential Information received and held by working groups that are required to access and use Confidential Information.
- Arqiva shall use Confidential Information solely for the purpose for which it was supplied and shall respect at all times the confidentiality of that information.
- Confidential Information shall not be passed on to any other business units, departments, subsidiaries or partners of Arqiva for whom such confidential information could provide a competitive advantage.

3. Protocol for the Identification and Treatment of Different Categories of Confidential Information

Arqiva consider that any Confidential Information should be treated in accordance with the principles described in section 2 and be protected through the measures described in section 4. However, it may be appropriate to identify “Very High Risk” Confidential Information for which confidentiality security is exceptionally important for the Customer or prospective customer (as defined in the Undertakings).

Very High Risk Confidential Information would include:

- information which indicates the intention of a Customer or prospective customer (as defined in the Undertakings) to bid or consider a bid for any spectrum auction that could be in competition with Arqiva;
- information which indicates the intention of a Customer or prospective customer (as defined in the Undertakings) to launch a new service where that service launch is not in the public domain.

For such Very High Risk Confidential Information additional measures, further to those described in section 4, would be implemented and would include:

- dissemination on a strictly need to know basis within the working groups that are required to access and use Confidential Information;
- extra protection around the storage systems and data systems used to hold Confidential Information, such as storage of electronic material in systems with highly restricted access;
- where appropriate, code names to be used to describe the work relating to the Very High Risk Confidential Information.

4. Measures to Ensure the Security of Confidential Information

Paragraph 16.2 of the Undertakings requires that the Information Security Strategy sets out appropriate measures to ensure:

- the security of Arqiva's information storage systems and data systems (including data collection, storage and archiving), particularly where Confidential Information is stored in systems shared between business units;
- the physical security of Confidential Information;
- that an employee of one business unit does not disclose or use the Confidential Information of which the employee had become aware whilst working for another business unit;
- the security of Confidential Information in the event that Arqiva is a bidder in a spectrum auction in competition with a Customer or prospective customer (as defined in the Undertakings); and
- that staff receive adequate training in relation to the Information Security Strategy.

This section 4 deals with each of these in turn.

4.1 Security of Information Storage and Systems

The following measures will be implemented to ensure the security of Arqiva's information storage systems and data systems.

- Restricted access to information systems / electronic storage space that is used to receive and hold Confidential Information. Access to be restricted to working groups within Arqiva that are required to access and use Confidential Information (as further described in section 3). Access restriction may be by means of username based profile control, password protection or other electronic access controls as appropriate. Such restricted access will be comprehensive and ensure that Confidential Information stored in systems shared between business units is soundly protected.
- Up to date record to be maintained of staff within working groups that are required to access and use Confidential Information to ensure the effective administration of restricted access controls.
- Disposal of electronic copy Confidential Information by means of permanent deletion from information systems / electronic storage space.

4.2 Physical Security of Confidential Information

The following measures will be implemented to ensure the physical security of Confidential Information.

- In line with the principle of distinct working groups within Arqiva that are required to access and use Confidential Information (described in section 3), access to office space accommodating those staff will where reasonably possible be controlled by means of restricted door access, or where feasible, district geographic locations from other staff working in areas that could gain competitive advantage from access to Confidential Information, most notably staff responsible for the day to day management of Arqiva owned DTT multiplex operations (DTT multiplexes C&D).

- Up to date record to be maintained of staff within working groups that are required to access and use Confidential Information to ensure the effective administration of restricted access controls.
- Where restricted door access is not reasonably possible hard copy Confidential Information to be stored in securely locked storage units when not in use.
- Disposal of hard copy Confidential Information by means of shredding or other controlled waste disposal.

4.3 Employee Disclosure

The Undertakings require the Information Security Strategy to set out appropriate measures to ensure that an employee of one business unit does not disclose or use the Confidential Information of which the employee had become aware whilst working for another business unit. Under the area of employee disclosure Arqiva also considers it appropriate to ensure that all staff within working groups that are required to access and use Confidential Information (described in section 3) comply with ongoing confidentiality measures.

To address issues of employee disclosure a confidentiality policy has been established by Arqiva and customer facing groups have been informed to maintain confidentiality in line with the principles of the Undertakings. However, the following additional measures will be implemented to further protect the security of Confidential Information from employee disclosure.

- A Code of Conduct will be published internally within Arqiva specifically in relation to the treatment of Confidential Information and will be added to the company policies handbook.
- Relevant staff will be briefed to ensure they understand and abide by the Code of Conduct.
- All relevant staff will review this Code of Conduct at least annually with their line manager who will be responsible for ensuring that at all times staff understand and accept the staff obligations.
- The Code of Conduct will include obligations relating to any member of staff that were to change role or project from a working group within Arqiva that is required to access and use Confidential Information to one where this information could be of competitive advantage, such obligations to include a requirement not to disclose or exploit any Confidential Information.
- Training and staff awareness measures relating to the Code of Conduct as detailed further in section 4.5.

4.4 In the Event that Arqiva is a Bidder in a Competitive Spectrum Auction

The following measures will be implemented to ensure the security of Confidential Information in the event that Arqiva is a bidder in a spectrum auction in competition with a Customer or prospective customer (as defined in the Undertakings).

- Arqiva's staff responsible for the day to day management of any bid that Arqiva might consider for a spectrum auction in competition with a Customer or prospective customer (as defined in the Undertakings), will be distinct from those staff that are required to access and use Confidential Information (as described in section 3).

- The identification and treatment of Very High Risk Confidential Information as described in section 3.

4.5 Staff Training and Awareness

The following measures will be implemented to ensure that staff receive adequate training in relation to the Information Security Strategy and its implementation.

- Initial and training programme specifically in relation to the Information Security Strategy and the staff Code of Conduct that will be compulsory for all relevant staff.
- An on-going staff awareness programme including refresh training, group briefings, internal publicity, and intranet based information in relation to the Information Security Strategy and its implementation and the staff Code of Conduct.
- Annual process built into line manager performance review process to ensure relevant staff understand and agree to Code of Conduct obligations in relation to the security of Confidential Information.

5. Next Steps

As part of the ongoing implementation of the Undertakings, Arqiva will further develop and test the proposed measures set out in this Information Security Strategy and as soon as reasonably possible complete the implemention of these measures in full.

This Information Security Strategy will be subject to regular review and may be updated from time to time as appropriate. In accordance with Paragraph 16.4 of the Undertakings Arqiva shall also, if required, make modifications to the Information Security Strategy as the Adjudicator or Ofcom may direct from time to time. Any modifications to the Information Security Strategy made by Arqiva must be notified to the Adjudicator and published.

END