Request for non-disclosure of information in certification application

1. Confidential information identification

- S1000 (FlySight) Schematic, fifteen (15) pages
- S1000 (FlySight) Parts list, three (3) pages
- Lucent/Agere OEM radio module processing gain report:
  Word Document: ***011734b_Spr_gainHighSpeed_HS.doc***
  Excel Spreadsheet: ***015127a_Spr_gainFCC_HSI3E Number2.xls***

2. Application in which the information appears

- FCC part 15 certification application. FCC ID #……..

3. Degree to which information is confidential

All information identified above is confidential

4. Degree to which information concerns a product or service that is subject to competition

The wireless digital video market is highly competitive. There are several large players like Axis Communications and VCS, offering high-end networked digital video solutions. There is also a myriad of smaller players offering or preparing to offer less sophisticated solutions.

5. How disclosure of the information can cause competitive harm

SmartSight Networks inc. is the only company whose product allows wireless digital voice, video and data with a single wireless transceiver. Disclosure could enable competitors to benefit from intellectual property unique to SmartSight Networks, contained in the product.

6. Measures taken to keep the information confidential

All SmartSight Networks employees must sign a confidentiality agreement at the time of hiring. Furthermore, all confidential information is released only to employees who are required to use it for official company business only. Finally, all confidential information is stored in electronic form on a file server residing on the

company premises and is accessible only by authorized employees from workstations located exclusively on-premises.

…/2

7. Availability of information

The information identified above has never been made available to the public. Certain parts of it have been disclosed, under confidentiality agreements, to third parties involved in supply, production and consulting activities for SmartSight Networks.

8. Period of time over which protection of confidentiality is requested

SmartSight Networks request a protection period of 5 years for the confidential information identified above. We estimate this information will continue to provide a competitive advantage over the life of the product and are not planning to release it to the public within the stated period.

9. Additional info

SmartSight Networks' intellectual property is contained in the hardware and in the firmware used in the product. The complexity of the product and the fact the firmware source code is not available to the public make reverse engineering the product virtually impossible. However, since ComLink makes the latest versions of executable firmware available to its customer base for ease of product maintenance and upgrade, making the schematics and parts lists available to the public would make copying our product very easy for interested parties. It would be a simple matter of building the product as per the schematics and parts lists, obtaining the latest version of the firmware from a current ComLink customer and downloading that firmware in the copied product. No other knowledge or expertise would be required from the third party. Because of the international market for the product, the threat of piracy by an unscrupulous third party is very real. Keeping the information identified above confidential is essential in protecting SmartSight Networks' intellectual property.

Requested by: _____
Willie Kouncar, Vice-President Engineering

Date _____