Lucent Technologies
Bell Labs Innovations

Subject: **Safeguarding Lucent Technologies Proprietary and Confidential Information.**

Michael P. Farina
Member of Technical Staff
Lucent Technologies, Inc.
67 Whippany Road, Room 4E-326
Whippany, NJ 07981-0903
Desk: 973-386-4344
E-Mail: mpfarina@lucent.com

February 27, 2006

Applicant:	**Lucent Technologies**
RE:	**FCC ID AS5ONEBTS-09**
Correspondence Reference Number:	**25561**
731 Confirmation Number:	**TC637695**

Mr. George Tannahill
Federal Communications Commission
Office of Engineering and Technology Laboratory Division
FCC Equipment Authorization Branch
7435 Oakland Mills Rd
Columbia MD 21046-1609

Dear Mr. Tannahill:

This is in response to your email to Eric Dobson, Timco Engineering, of February 1, 2006, that was forwarded to me, in which you requested: (a) information regarding the typical security measures that are taken by Lucent's customers to restrict access to Lucent base station equipment: and (b) the nature of Lucent's typical confidentiality agreements.

Base Station Installation Security:

Lucent sells its base station equipment in two equipment cabinet types: 1) for indoor installation, and 2) for outdoor installation. In each case, the physical on-site security is the responsibility of the customer and service provider. Typically, the customer maintains a high level of security at all installations/sites to protect both their asset investments and their network. The indoor cabinets are installed in environmentally controlled enclosures, either in building interiors or in remote huts (enclosed structures) located at the base of cell towers. In commercial building installations, access to the cabinet interior is prevented by a key locked cabinet door and the cabinet itself is installed in a designated restricted area, which is protected by security doors and security locks. Public access to these areas is restricted. Access is restricted to the customer's technical staff that have a specific need. Both the commercial building and its access are further protected by an on-premise security staff. The remote hut type enclosures are located at the base of the customer's cell tower. The hut is protected by customer installed security locks and alarm system; access is limited to and restricted to the customer's designated service technicians. In addition, both the hut and the cell tower are fully enclosed within a locked security fence. There is no public access to this site.

Outdoor cabinet installation differs from the indoor cabinet, but ordinarily employs similar security measures and public access denial to protect both their asset investments and their network. The outdoor equipment cabinet door is normally securely key-locked and mounted on a concrete pad at the base of the cell tower. Both are enclosed within a locked security fence. All access is limited to and restricted to the customer's designated service technicians. There is no public access to this site.

Confidentiality Agreements:

Lucent typically enters into non-disclosure agreements with its customers in master supply agreements, in discrete contracts, or in stand-alone agreements. The confidentiality provisions in these agreements ordinarily provide that the customer will protect and not disclose Lucent's proprietary and confidential information, in whatever form or medium transmitted. Confidential information is usually defined to include Lucent's intellectual property, which, among other items, would comprise installation handbooks, manufacturing information and drawings, circuit pack schematics, circuit pack assemblies, equipment pack schematics, circuit module schematic type drawings, and source and disassembly code documentation. Also deemed confidential information is any such technical or business information that a third party furnishes or discloses to Lucent and which, in turn, is disclosed to the customer. This latter requirement stems, in part, from contractual nondisclosure obligations that Lucent has entered into with its suppliers.

Sincerely,

Original Signed By

Michael P. Farina
Member of Technical Staff
Whippany FCC/EMC Certification and Compliance Group

Copy To:

Eric Dobson, Quality Manager, Timco Engineering, Inc., Newberry, FL
C. S. Donovan, Product Compliance Manager, Holmdel, NJ
R. Geilich, Corporate Counsel, Whippany, NJ
P. J. Hollern, Technical Manager, FCC/EMC Compliance Group, Columbus, Ohio
D. D. Moongilan, DMTS, Global Products Compliance Laboratory, Holmdel, NJ
H. R. Noguchi, Technical Manager, Global Products Compliance Laboratory, Holmdel, NJ
R. J. Pillmeier, Technical Manager, FCC/EMC Compliance Group, Whippany, NJ