Jooran Lee 小姐您好：

2004 年 **7** 月，**ISO/IEC JTC1** 中国国家委员会以现行的中国国家标准 **GB15629.11** 为基础向 **ISO/IEC JTC1** 提交了新工作项目建议，并建议采用快速程序。项目名称为：“信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 **11** 部分：无线局域网媒体访问控制和物理层规范补篇 **1**：增强的安全规范”。

JTC1 秘书处于 **2004** 年 **8** 月 **2** 日公布 **JTC1 N7506**（见附件 **1**）对中国提案进行评论。该文件状态为：“该文件分发给 **JTC1** 各国家成员体进行符合性评论。如果 **JTC1** 秘书处在规定的期限内没有收到对该提案的反对意见，此项工作将被批准为 **SC6** 的工作项目”。但是 **JTC1** 公布“**N7506** 已无效”，并随后公布 **N7537**（见附件 **2**）对 **IEEE 802.11i** 进行评论。中国国家成员体是遵照 **JTC1** 导则提交的中国提案。中国国家成员体认为 **JTC1** 在公布 **N7506** 无效之前若与我们取得联系并告知其原因更为妥善。

因此，中国国家成员体期望：

1. JTC1 秘书处告知我们公布 **N7506** 的原因，并在如何处理该提案的问题上与我们取得联系。

2. 国际标准应该广泛采纳各国家成员体国家标准的优点。作为 **ISO/IEC/JIC1** 的 **P** 成员，中国国家成员体有义务和权利参与 **ISO/IEC/JTC1** 标准的制定和维护，并为标准的完善做出贡献。就该提案，中国专家针对 **DIS 8802.11** 中存在的安全及射频传输特性缺陷，进行了长期地深入地研究。中国国家标准 **GB15629.11** 已于 **2003** 年 **5** 月正式公布，该标准能够很好地解决 **DIS 8802.11** 中的缺陷。以 **GB15629.11** 为基础，中国国家成员体遵照 **JTC1** 导则向 **JTC1** 提交了提案“信息技术 系统间远程通信和信息交换 局域网和城域网 特定要求 第 **11** 部分：无线局域网媒体访问控制和物理层规范补篇 **1**：增强的安全规范”。**JTC1** 在进行 **ISO/IEC 8802.11**：**1999** 修订时，应该考虑中国成熟的、已经具有市场影响力的技术内容和成功经验，使其更加完善、应用更加广泛。因此，我们不能理解为何 **JTC1** 秘书处在 **N7506** 被分发后不久就公布其无效。

中国专家认真研究了 N7537，认为在技术上存在以下不足：

1、非双向认证，存在用户如何信任网络的问题

STA 只是通过与认证服务器(Radius)进行相互认证来间接实现 AP 与 STA 的双向认证，这不是 AP 和 STA 之间真正的双向认证。

2、扩展性差

N7537 在 AP 和认证服务器间必须手工设置共享密钥，因而扩展性不强。大规模网络应用时，网络管理困难。

3、认证协议复杂

N7537 认证协议复杂，且认证服务器不易扩充

4、主密钥的安全性

在 N7537 中主密钥是由移动终端和认证服务器协商出的，并由认证服务器通过物理信道传输给 AP，密钥在网络上传递，引入了新的安全攻击点。

为真正完善 DIS 8802.11，将更多的经验和技术优点包括其中，

1. 中国国家成员体不同意在对我国提案进行慎重考虑之前对 N7537 进行快速程序投票。

2. 中国国家成员体建议将我国提案与 N7537 在 11 月 8~11 日 SC6 年会期间同各国家成员体代表进行讨论。中国国家成员体将派代表参会，并愿意同各国家成员体代表交换意见。

ISO/IEC JTC1 中国国家委员会秘书处

2004 年 10 月 14 日