附件 4

珠海市国家保密局互联网保密检查系统等保测评服务项目采购需求书

一、项目名称及预算

项目名称：珠海市国家保密局互联网保密检查系统等保测评服务项目

项目预算：人民币 3.5 万元。本项目投标报价为包干价，投标供应商的报价应包括但不限于以下内容：测评费用、人员服务费用、验收及本项目的其他相关服务费用。

二、中介服务机构资格要求

1. 测评机构须具有由公安部第三研究所认证发放的、有效的《网络安全等级测评与检测评估机构服务认证证书》；

2. 测评机构须在中国网络安全等级保护网（http://www.djbh.net）最新发布的《全国网络安全等级测评与检测评估机构目录》中；

3. 测评机构在中国网络安全等级保护网（http://www.djbh.net）没有被通报处于整改期或取消等级保护测评机构服务认证证书。

三、项目技术服务要求

（一）本次服务范围

完成珠海市保密局互联网保密检查系统（三级）的信息

安全等保测评服务。

设备清单如下：

序号	类别	数量
1	VPN	1 台
2	交换机	1 台
3	计算机终端	1 台
4	检测器管理系统	1 套
5	服务器	3 台
6	防火墙	1 台
7	网络安全审计系统	1 套
8	日志审计系统	1 套
9	漏洞扫描系统	1 套
10	入侵检测系统	1 套
11	主机审计系统	1 套
12	计算机防病毒软件	1 套
13	堡垒机	2 台

本项目按照等级保护 2.0 相关标准的要求：

第一步：测评方协助采购人完成系统定级备案工作（如有必要）；

第二步：测评方对采购人的信息系统进行测试评估、分析差距、输出差距测评报告和安全整改建议；

第三步：采购人根据差距测评报告与安全整改建议实施安全整改；测评方需协助我方按照等级保护相关标准完善安

全管理制度；

第四步：测评方再次对采购人的信息系统进行测试评估、输出2.0验收测评报告，并协助用户方通过公安机关的备案与检查。

为此，测评方专业测评师需要通过规范的等级保护测试评估，对采购人信息系统从安全技术和安全管理两个方面的各个层面的安全控制进行整体性验证。

（二）项目工期

签订合同之日起60个日历日内完成本次项目服务工作。项目启动后，完成测试评估，并出具差距测评报告和安全整改建议。项目最终验收前，需完成对信息系统整改后的测试评估、输出2.0验收测评报告，并协助用户方通过公安机关的备案与检查。

（三）验收要求及付款方式

投标人提交符合国家信息安全等级保护主管部门要求的测评报告，完成国家信息安全等级保护主管部门备案后，提出验收申请，采购人审核同意后在15个工作日内在服务地点组织验收。

合同签订后，甲方在乙方送达付款所需发票等报账材料之日起15个工作日内向乙方支付合同款的70%；乙方提交符合国家信息安全等级保护主管部门要求的测评报告，完成国家信息安全等级保护主管部门备案，通过甲方组织验收后，

甲方在乙方送达付款所需发票等报账材料之日起15个工作日内向乙方支付合同剩余款项。

因采购人使用的是财政资金，采购人在前款规定的付款时间为向政府财政支付部门提出办理财政支付申请手续的时间（不含政府财政支付部门审核的时间），在规定时间内提出支付申请手续后即视为采购人已按期支付。

（四）测评依据

信息系统等级保护测评依据《信息系统安全等级保护基本要求》、《信息系统安全等级保护测评要求》，在对信息系统进行安全技术和安全管理的安全控制测评及系统整体测评结果基础上，针对相应等级信息系统遵循的标准进行综合性测评，提出相应的安全评审意见。

主要参考标准如下：

《信息安全等级保护管理办法》

《计算机信息系统安全保护等级划分准则》

《信息安全技术 信息系统安全等级保护定级指南》

《信息安全技术 信息系统安全等级保护基本要求》

《信息安全技术 信息系统安全等级保护测评要求》

《信息安全技术 信息系统安全等级保护实施指南》

《信息安全技术 信息系统安全等级保护测评过程指南》

《信息安全技术 信息系统通用安全技术要求》

《信息安全技术 网络基础安全技术要求》

《信息安全技术 操作系统安全技术要求》

《信息安全技术 数据库管理系统安全技术要求》

《信息安全技术 服务器技术要求》

《信息安全技术 终端计算机系统安全等级技术要求》

《信息安全技术 信息安全风险评估规范》

（五）测评原则

项目的方案设计与实施应满足以下原则：

符合性原则：应符合国家信息安全等级保护制度及相关法律法规。

标准性原则：方案设计、实施与信息安全体系的构建应依据国内、国际的相关标准进行。

规范性原则：项目实施应由专业的等级保护测评师依照规范的操作流程进行，在实施之前将详细量化出每项测评内容，对操作过程和结果提供规范的记录，以便于项目的跟踪和控制。

可控性原则：项目实施的方法和过程要在双方认可的范围之内，实施进度要按照进度表进度的安排，保证项目实施的可控性。

整体性原则：等级保护测评与安全体系设计的范围和内容应当整体全面，包括安全涉及的各个层面，避免由于遗漏造成未来的安全隐患。

最小影响原则：项目实施工作应尽可能小的影响网络和信息系统的正常运行，不能对信息系统的运行和业务的正常

提供产生显著影响。

保密原则：对项目实施过程获得的数据和结果严格保密，未经授权不得泄露给任何单位和个人，不得利用此数据和结果进行任何侵害客户利益的行为。

同时，在等级保护测评实施的过程中遵循以下原则：

客观性和公正性原则：虽然测评工作不能完全摆脱个人主张或判断，但测评人员应当没有偏见，在最小主观判断情形下，按照测评双方相互认可的测评方案，基于明确定义的测评方式和解释，实施测评活动。

经济性和可重用性原则：基于测评成本和工作复杂性考虑，鼓励测评工作重用以前的测评结果，包括商业安全产品测评结果和信息系统先前的安全测评结果。所有重用的结果，都应基于结果适用于目前的系统，并且能够反映出目前系统的安全状态基础之上。

可重复性和可再现性原则：不论谁执行测评，依照同样的要求，使用同样的测评方式，对每个测评实施过程的重复执行应该得到同样的结果。前者与不同测评者测评结果的一致性有关，后者与同一测评者测评结果的一致性有关。

结果完善性原则：测评所产生的结果应当证明是良好的判断和对测评项的正确理解。测评过程和结果应当服从正确的测评方法以确保其满足了测评项的要求。