项目验收报告

根据网络和信息系统安全大数据监测分析和管理服务项目合同的约定，我单位对深圳市民意速办和智慧城市建设中心政府采购项目中标/成交供应商深圳市能信安科技股份有限公司提供的货物/服务进行了验收，验收情况如下：

<table>
<tr><td rowspan="4">项目基本情况</td><td>项目名称</td><td>网络和信息系统安全大数据监测分析和管理服务项目</td><td>项目编号（如有）</td><td>FTDL2022000015</td></tr>
<tr><td>采购单位</td><td>深圳市民意速办和智慧城市建设中心</td><td>中标/成交供应商</td><td>深圳市能信安科技股份有限公司</td></tr>
<tr><td>中标/成交金额</td><td>1175000 元</td><td>合同履约时间</td><td>自 2023 年 3 月 5 日
至 2024 年 3 月 4 日</td></tr>
<tr><td colspan="4">货物型号规格、标准及配置（或者服务内容、标准）：
提供福田区政府政务网络的网络和信息系统安全大数据监测分析和管理服务。</td></tr>
<tr><td rowspan="9">验收记录</td><td>验收分项</td><td>验收情况</td><td>是否通过</td><td>备注</td></tr>
<tr><td>1. 网络和信息系统安全大数据监测分析和管理服务</td><td>按合同要求完成维保服务</td><td>☑是 □否</td><td></td></tr>
<tr><td>2. 网络流量监测服务</td><td>按合同要求完成维保服务</td><td>☑是 □否</td><td></td></tr>
<tr><td>3. 重要业务系统运行状态监测</td><td>按合同要求完成维保服务</td><td>☑是 □否</td><td></td></tr>
<tr><td>4、渗透测试服务
5、网络安全攻防演练服务</td><td>按合同要求完成维保服务</td><td>☑是 □否</td><td></td></tr>
<tr><td>6、移动应用安全漏洞及个人信息保护合规性检测服务</td><td>按合同要求完成维保服务</td><td>☑是 □否</td><td></td></tr>
<tr><td>7、移动应用安全加固服务</td><td>按合同要求完成维保服务</td><td>☑是 □否</td><td></td></tr>
<tr><td>8、配合做好信息安全联合检查服务</td><td>按合同要求完成维保服务</td><td>☑是 □否</td><td></td></tr>
<tr><td rowspan="2">验收结论</td><td colspan="4">验收结论性意见：
2023 年 3 月 5 日至 2024 年 3 月 4 日乙方已按合同要求完成各项工作，服务质量符合此次服务要求，履约验收合格。</td></tr>
<tr><td colspan="4">有异议的意见和相关说明（如有）：
提出异议人员签字：</td></tr>
</table>

参与验收人员签字/盖章	采购单位验收小组成员签字（单位公章）： 组长：梁俊　组员： 2024 年3月13日
	中标/成交供应商参与人员签字（单位公章）： 2024 年3月13日

附件 11

项目履约情况评价表

采购单位名称：深圳市民意速办和智慧城市建设中心　　联系人及电话：杨宏声，82918699

<table>
<tr><td colspan="3">采购项目名称</td><td>网络和信息系统安全大数据监测分析和管理服务项目（2023-2024 年）</td><td>项目编号（如有）</td><td>FTDL2022000015</td></tr>
<tr><td colspan="3">中标/成交供应商</td><td>深圳市能信安科技股份有限公司</td><td>供应商
联系人及电话</td><td>李德庆
18922849880</td></tr>
<tr><td colspan="3">中标/成交金额</td><td>￥1,175,000.00 元</td><td>合同履约时间</td><td>自 2023 年 3 月 5 日
至 2024 年 3 月 4 日</td></tr>
<tr><td rowspan="7">履约情况评价</td><td colspan="2">总体评价</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td rowspan="6">分项评价</td><td>质量方面</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>价格方面</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>服务方面</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>时间方面</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>环境保护</td><td colspan="3">☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td>其他</td><td colspan="3">评价内容为：
评价等级为：☑ 优　□ 良　□ 中　□ 差</td></tr>
<tr><td colspan="3">具体情况说明</td><td colspan="3">一、总体服务内容：
承担福田区政府政务网络的网络和信息系统安全大数据监测分析和管理服务。
二、具体服务要求如下：
1、网络和信息系统安全大数据监测分析和管理服务的要求；
（1）资产的全面发现与台账建设为基础，建立统一的“资产管理、漏洞管理、安全监测和安全技术保障”闭环管理机制，形成安全管理工作流程。每年一次。
（2）结合现有安全态势感知大数据系统，进行每日安全态势大数据监测，利用各设备威胁情报、机器学习、用户行为画像等技术对报警数据进行综合研判，输出分析报告，报告每月一次。
（3）在服务期内对福田区政府的政务网络资产每月进行一次梳理工作，包括网络设备、安全设备、服务器、办公终端、复印机、打印机</td></tr>
</table>

	等并更新客户单位在市业务支撑平台上的相关数据，每月一次。 （4）针对目标地址段不明确的资产，通过流量还原和大数据平台的用户行为分析功能，对福田区各单位访问部署在互联网的应用系统的行为进行识别、过滤，发现私自搭建的业务系统要发出安全预警通告，需发现当天发出通告。 （5）经过研判，核定的安全事件发出安全通告，需包含事件详情、溯源过程、分析结果、解决方案。发现安全事件的当天需发出安全通告。 （6）网络和信息系统安全大数据监测分析相关系统对 APT 攻击、勒索软件、远控木马、僵尸网络、窃密木马、间谍软件、网络蠕虫、邮件钓鱼等各类高级网络攻击进行监测，并对恶意攻击源 IP 进行封堵，需形成工作记录表，每日更新。 （7）担任甲方单位计算机网络和主机系统的安全顾问，在网络和主机系统进行升级、扩建时，提供安全修补建议。 （8）需监控的网络资产数量：机房不少于三个；信息系统不少于 180 个；安全设备不少于 70 套；服务器不少于 800 台（包括云虚拟服务器）；终端电脑不少于 15000 台（包括桌面云主机）。 2、网络流量监测服务的要求； （1）监测政务网各节点网络流量数据，分析全区网络的带宽、网络设备转发瓶颈、各类网络协议流量分配情况，研判增长趋势，提出合理的网络资源控制策略。监测各个重要业务系统访问用户量、访问流量、响应速率、Nginx 代理服务器状态、DNS 服务器状态等，保障重要业务系统稳定运行。 （2）协助各业务系统运维团队排查业务系统网络问题，分析性能瓶颈，排查僵尸业务、服务器、终端主机等。 （3）应急响应服务。需提供 24 小时的应急响应服务。一旦发生网络安全故障，需半小时内赶到现场提供应急响应技术支持，协助网络系统运维团队在指定时间内恢复网络正常运行。 3、重要业务系统运行状态监测要求； （1）每天利用网络和信息系统安全大数据监测分析相关系统对各业务系统运行安全状态进行监测，监测内容包括业务访问量，网络流量、响应延时、业务会话量等指标，发现异常立即预警并分析问题，并协助各系统管理排查和解决问题，每月提交系统安全状态监测报告。 （2）每日监控 Nginx 代理服务器状态和 DNS 服务器状态，包括业务日志、响应速率、服务器资源利用率等，做好安全维护工作，保障全区业务系统对外提供访问能力及办公终端访问互联网能力正常。 （3）应急响应服务。需提供 24 小时的应急响应服务。一旦发生业务安全故障，需半小时内赶到现场提供应急响应技术支持，协助业务系统运维团队在指定时间内恢复业务系统正常运行。 4、渗透测试要求； （1）利用资产漏洞管理功能模块组织专业力量对福田区业务系统每半年进行一次全方面深层次的渗透，提前发现并解决存在的或潜在的深层次安全漏洞。

	（2）在系统运行状态通过对目标进行模拟黑客入侵，进行非破坏性质的攻击性测试，直观地暴露系统所面临的威胁与风险点，最大程度挖掘潜在安全漏洞和威胁，以攻促防，最终形成详细的漏洞位置，成因，修复建议等内容的专业安全渗透测试报告。每年一次。 5、网络安全攻防演练服务要求； （1）开展网络安全实战攻防演练，开展以获取指定目标系统的管理权限为目标的攻防演练，由攻防领域经验丰富的专家组成攻击队，在保障业务系统稳定运行的前提下，采用“不限攻击路径，不限制攻击手段”的贴合实战方式，而形成的“有组织”的网络攻击行动。 （2）针对福田区网络安全、网站安全、各应用系统安全、数据库安全和数据备份系统安全等，协助福田区数据管理中心制定和修订各类系统应急预案，制定应急演练方案，评估演练可能出现的问题，模拟真实应急场景的灾难恢复，提高信息化部门的应急应变能力。 每年组织一次网络安全实战应急演练，需交付给客户单位应急演练脚本、应急演练视频。 6、移动 APP 安全漏洞及个人信息保护合规性检测要求； （1）每月对福田区的移动应用开展一次安全检测，安全检测服务范围涵盖福田区移动 APP 客户端（含 IOS）、微信小程序、微信公众号、通信链路和服务器端的多方面和多维度。检测内容主要包含以下七个方面：运行环境安全检测、软件自身安全检测、用户操作安全检测、数据安全检测、通信安全检测、业务安全检测、服务器端安全检测。每月提交给客户单位 App 安全检测报告。 （2）移动应用系统上线前根据《中央网络信办、工业和信息化部、公安部、市场监督总局关于开展 App 违法违规收集使用个人信息专项治理的公告》、《App 违法违规收集使用个人信息自评指南》、《APP 违法违规收集使用个人信息行为认定方法》等文件要求开展 App 的个人信息保护合规性评估。根据评估结果指导 App 开发单位完成整改。 7、服务期内提供 5 次移动 APP（Android、iOS）安全加固服务要求； （1）加固能力：Android 加固能力至少包括：App Java 代码防逆向、App 防篡改、App 防调试/注入、App So 库保护、防模拟器,HOOK；iOS 加固能力至少包括：iOS 应用代码定制化混淆、APP 防调试、支持 APP 越狱检测、防止 APP 被二次签名、禁止山寨、防截屏监听。 （2）兼容性：适配主要的手机厂家的移动设备、适配基于原生 Android 进行修改的其他 OS、加固前后程序首次启动时间与加固前相比延时<1 秒、加固前后程序 CPU 占有率变化比例<5%、Android 代码安全加固后 APK 体积变化比例 ± 5%。 （3）安全保证：采用自身实现的安全机制或开源级源代码混淆方案、防止静态反编译工具、防 JAVA 动态调试、进程调试等动态调试手段、多重验证防御二次打包攻击。 8、配合做好信息安全联合检查要求； （1）配合甲方做好迎接上级主管部门信息安全检查：协助甲方做好每年上级党政机关信息安全和保密安全检查及培训工作，以及做好迎接全市党政机关信息安全联合检查工作组对福田区信息系统安全检

	查的准备工作。 （2）配合甲方对福田区党政机关单位信息安全检查和绩效评估：协助甲方做好每年对对福田区党政机关单位的信息安全检查和绩效评估工作。 9、其他要求； （1）乙方负责提供并保管其安全技术服务人员的工作电脑；服务期间若发生的交通费、误餐费等均由乙方承担。 （2）乙方负责其安全技术服务人员的工资、奖金、福利待遇及其他一切费用，必须为其安全服务人员购买劳动保险，对其安全服务人员做好安全生产教育。如乙方的安全技术服务人员在甲方工作现场发生工作事故或工伤事故的，由乙方负全责。 （3）若乙方指派到甲方现场服务的安全技术服务人员的工作表现不能符合甲方要求，且经过教育后仍不能改正的，甲方可要求乙方更换相关技术服务人员。 （4）甲方的政务办公网、政务公共网及其主机系统发现有安全问题时，安全服务公司在接到甲方通知（含电话通知）后，即安排资深安全维护工程师前往甲方现场，查明发生问题的原因，采取有效的措施尽快恢复网络和主机的正常运行。一般问题安全服务公司维护人员应在2小时内到达，重大问题应在1小时内到达。 对于每次安全服务，安全服务公司应保存现场资料，分析产生问题的原因，记录维护使用的方法、步骤和参数，制定防止类似问题发生的解决方法。安全服务公司将保存的现场资料和有关文档资料提交给甲方。
采购单位意见（公章）	乙方在服务期限内的完成了网络和信息系统安全大数据监测分析和管理服务项目，履约评价等级为优。 日期：2024年3月13日

备注：采购人可根据项目实际情况增减分项内容。本表必须在合同履行完毕后30日内反馈。