广东省统筹区域传染病监测预警与应急指挥信息平台（一期）项目网络安全等级保护测评服务采购需求

1 项目概况

1.1 基本信息

（一）项目名称：广东省统筹区域传染病监测预警与应急指挥信息平台（一期）项目网络安全等级保护测评服务

（二）采购人：广东省疾病预防控制中心

（三）服务地点：广东省疾病预防控制中心指定地点

（四）项目总体目标：根据公安部等级保护规定要求，做好信息系统的系统等级备案、安全评估、整改、验收测评、测评报告提交、等级保护回执工作。依据《中华人民共和国网络安全法》、GB/T22239-2019《信息安全技术 网络安全等级保护基本要求》、《广东省计算机信息系统安全保护条例》等标准公正、独立、自主地开展定级、测评工作，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。

1.2 省统筹项目概况

为健全我省疾病预防控制网络，增强传染病疫情和突发公共卫生事件早期监测预警能力，提高疫情防控和突发公共卫生事件应急处置水平。我省将建立以国家级传染病监测预警与应急指挥信息平台为主体，“全国一网统管、平台两级建设，数据统一收集、业务分级应用”的一体化的省统筹区域平台，实现“共建、共治、共享”目标，完

善整合现有传染病监测和应急相关信息系统。加快完善省统筹项目制定立项方案，尽快推进省统筹项目实施等工作，确保加快我省传染病监测预警与应急指挥能力提升。包括不限于升级完善传染病疫情监测数据自动采集系统、集成重大和重点传染病管理信息系统、传染病疫情症候群监测信息系统、传染病病原监测信息系统、大数据协同监测信息系统、舆情监测信息系统、态势感知与预警系统、应急值守管理信息系统、智能流调信息系统、跨地区信息协查信息系统、可视化展示信息系统、辅助决策信息系统、应急指挥调度综合管理信息系统、卫生应急资源保障综合管理信息系统等 14 个应用系统。

2 项目预算

本项目总预算为 **78.4** 万元。

3 服务期限

自合同签订之日起至省统筹区域传染病监测预警与应急指挥信息平台（一期）项目终验合格为止。

4 服务内容

4.1 测评对象

序号	测评对象	拟定级情况	备注
1	广东省统筹区域传染病监测预警与应急指挥信息平台	三级	包括不限于升级完善传染病疫情监测数据自动采集系统、集成重大和重点传染病管理信息系统、传染病疫情症候群监测信息系统、传染病病原监测信息系统、大数据协同监测信息系统、舆情监测信息系统、态势感知与预警系统、应急值守管理信息系统、智能流调信息系统、跨地区信息协查信息系统、可视化展示信息系

序号	测评对象	拟定级情况	备注
			统、辅助决策信息系统、应急指挥调度综合管理信息系统、卫生应急资源保障综合管理信息系统等子应用系统。

4.2 测评需求

网络安全等级保护是国家网络安全保障的基本制度、基本策略、基本方法。开展网络安全等级保护工作是保护信息化发展、维护国家网络安全的根本保障，也是《中华人民共和国网络安全法》的要求。2017 年 6 月 1 日实施的《中华人民共和国网络安全法》第二十一条规定，国家实行网络安全等级保护制度，履行安全保护义务，保障网络免受干扰、破坏或者未经授权的访问，防止网络数据泄露或者被窃取、篡改。

随着信息化程度的越来越普及，而且国内外信息安全形式非常严峻，结合国家信息安全等级保护的安全要求，同时根据《网络安全法》与广东省相关网络安全文件的要求，在此基础上，我中心按照国家有关规定和标准规范要求对信息系统进行安全建设整改，并达到相关要求，并取得符合公安要求的 2025 版网络安全等级保护等级测评报告。

4.3 测评依据

4.3.1 法律法规

《中华人民共和国网络安全法》

《中华人民共和国计算机信息系统安全保护条例》（国务院 147 号令）

《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发[2003]27 号）

《中共中央办公厅国务院办公厅转发<国家信息化领导小组关于加强信息处理安全保障工作的意见>的通知》（中办发[2003]27 号）

《关于印发<关于信息安全等级保护工作的实施意见>的通知》（公通字[2004]66号文）

《关于印发<信息安全等级保护管理办法>的通知》（公通字[2007]43 号文）

《关于开展全国重要信息系统安全等级保护定级工作的通知》（公信安[2007]861号文）

《国家网络与信息安全协调小组关于开展信息安全风险评估工作的意见》（国信办[2006]5 号）

卫生部关于印发《卫生行业信息安全等级保护工作的指导意见》的通知卫办发[2011]85 号

卫生部办公厅《关于全面开展卫生行业信息安全等级保护工作》的通知卫办综函[2011]1126 号

4.3.2 技术标准

《计算机信息系统安全保护等级划分准则》

《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）

《信息安全技术 网络安全等级保护测评要求》（GB/T 28448-2019）

《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）

《信息安全技术 网络安全等级保护安全设计技术要求》（GB/T 25070-2019）

《信息安全技术 网络安全等级保护实施指南》（GB/T 25058-2019）

《信息安全技术 信息系统安全通用技术要求》（GB/T 20271-2006）

《信息安全技术 网络基础安全技术要求》（GB/T 20270-2006）

《信息安全技术 操作系统安全技术要求》（GB/T 20272-2019）

《信息安全技术 数据库管理系统安全技术要求》（GB/T 20273-2019）

《信息安全技术 服务器安全技术要求》（GBT 21028-2007）

《信息安全技术 终端计算机系统安全等级技术要求》（GA/T 671-2006）

除上述规范以外，还遵循国家现行的相关标准和规范要求。

4.4 测评原则

1.客观公正性，测评检查人员不带偏见，减少主观判断实施检查活动；

2.先进性：确保先进性同时，使用成熟稳定技术；

3.实用性：满足业务功能需求的前提下，做到简单、实用、人性化；

4.安全性：保证系统数据、交易数据、数据传输以及交易过程的安全性，防止数据被截取、篡改和丢失；

5.可重复性和可再现性，不论谁执行检查，依照同样的要求，使用同样的检查方式，对每个检查实施过程的重复执行应该得到同样的结果。

4.5 测评服务内容

4.5.1 等级保护辅助服务

配合采购人完成等级保护测评资产收集、资料准备、项目整体协调等工作，等级保护流程辅助服务需成交投标人全程协助采购人完成等级保护测评工作，直至完成测评。如采购人有包括但不限于上述测评对象的等保证撤销、备案更新、新增备案等需要，需配合采购人直至工作完成。

4.5.2 风险梳理服务

为采购人测评系统提供资产核查、风险识别服务。以等级保护标准要求为依据，按照等级保护标准要求对本次项目范围的信息系统在安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理方面进行综合安全风险梳理，发现信息系统

的安全保护现状，并为确立安全策略、制定安全规划、开展安全建设提供改进建议，为后续采购人通过网络安全等级保护测评提供指导。判定各系统安全防护能力是否能达到上述列表相应级别的要求，提交《问题整改清单》。

4.5.3 等级保护整改咨询服务

根据风险梳理服务中的《问题整改清单》中提出的问题，在采购人整改过程中，提供完整的网络安全整改建议，协助指导采购人的运维人员开展整改加固工作。主要包括：讲解网络安全整改问题清单，提出整改措施建议，解答采购人运维人员提出的整改疑问、审核采购人的整改材料，推进采购人的整改实施进度等相关工作，该服务不涉及软件整改及相关设备采购。

4.5.4 等级保护测评服务

协助采购人目标系统完成上述风险梳理和整改服务工作后，根据《信息系统安全等级保护基本要求》（GB/T22239-2019）等标准聘请具有网络安全等级测评与检测评估认证的测评机构组织开展网络安全等级保护符合性测评，衡量采购人信息系统的安全保护管理措施和技术措施是否符合等级保护基本要求，是否具备相应的安全保护能力。

依据信息系统的安全保护等级，通过人员访谈、文档查、实地察看、配置检查、工具检测等方法从安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心、安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理等方面，判断信息系统现有的安全保护水平与国家信息安全等级保护管理规范和技术标准要求项之间的符合情况。

开展系统整体测评，涉及到信息系统的整体拓扑、局部结构，也关系到信息系统的具体安全功能实现和安全控制配置，与特定信息系统的实际情况紧密相关。在安全

控制测评的基础上，重点考虑安全控制点间、层面间、区域间的相互关联关系，分析评估安全控制点间、层面间、区域间是否存在安全功能上的增强、补充和削弱作用以及信息系统整体结构安全性、不同信息系统之间整体安全性。

综合测评对信息系统进行整体、全面、公正的评估，对不符合项进行风险分析，组织专家评审，编写安全等级保护测评报告，最终完成验收测评工作，达到国家规定的信息安全要求，并完成向广东省公安厅提交测评备案工作。

4.5.4.1 安全物理环境测评

安全物理环境测评中，测评人员应以文档查阅与分析和现场观测等检查方法为主，访谈为辅来获取测评证据，用于评测机房的安全保护能力。

安全物理环境测评涉及的测评对象主要为机房和相关的安全文档。

具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述
1	物理位置选择	通过访谈物理安全负责人，检查机房，测评机房物理场所在位置上是否具有防震、防风和防雨等多方面的安全防范能力。
2	物理访问控制	通过访谈物理安全负责人，检查机房出入口等过程，测评信息系统在物理访问控制方面的安全防范能力。
3	防盗窃和防破坏	通过访谈物理安全负责人，检查机房内的主要设备、介质和防盗报警设施等过程，测评信息系统是否采取必要的措施预防设备、介质等丢失和被破坏。
4	防雷击	通过访谈物理安全负责人，检查机房设计/验收文档，测评信息系统是否采取相应的措施预防雷击。
5	防火	通过访谈物理安全负责人，检查机房防火方面的安全管理制度，检查机房防火设备等过程，测评信息系统是否采取必要的措施防止火灾的发生。
6	防水和防潮	通过访谈物理安全负责人，检查机房及其除潮设备等过程，测评信

		息系统是否采取必要措施来防止水灾和机房潮湿。
7	防静电	通过访谈物理安全负责人，检查机房等过程，测评信息系统是否采取必要措施防止静电的产生。
8	温湿度控制	通过访谈物理安全负责人，检查机房的温湿度自动调节系统，测评信息系统是否采取必要措施对机房内的温湿度进行控制。
9	电力供应	通过访谈物理安全负责人，检查机房供电线路、设备等过程，测评是否具备为信息系统提供一定电力供应的能力。
10	电磁防护	通过访谈物理安全负责人，检查主要设备等过程，测评信息系统是否具备一定的电磁防护能力。

4.5.4.2 安全通信网络测评

安全通信网络测评中，测评人员将以配置核查和文档查阅为主，访谈和分析为辅来获取证据，用于测评信息系统的网络安全保护。

安全通信网络测评涉及的测评对象主要为网络设备和安全。

具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述
1	网络架构	测评分析网络架构与网段划分、隔离等情况的合理性和有效性。
2	通信传输	测评通信过程中的完整性、保密性等。
3	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证。

4.5.4.3 安全区域边界测评

安全区域边界测评主要涉及边界防护、访问控制、入侵防范、恶意代码和垃圾邮件防范、安全审计、可信验证等方面的安全保护能力，具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述
1	边界防护	测评分析信息系统网络边界安全防护的状况。
2	访问控制	测评分析信息系统对网络区域边界相关的网络隔离与访问控制能力。
3	入侵防范	测评分析信息系统对攻击行为的识别和处理情况。
4	恶意代码和垃圾邮件防范	测评分析信息系统网络边界和核心网段对病毒等恶意代码及垃圾邮件的防护情况。
5	安全审计	测评分析信息系统审计配置和审计记录保护情况。
6	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等 进行可信验证，并在应用程序的关键执行环节进行动态可信验证。

4.5.4.4 安全计算环境测评

安全计算环境测评主要涉及身份鉴别、访问控制、安全审计、入侵防范、恶意代码防范、可信验证、数据完整性、数据保密性、数据备份恢复、剩余信息保护、个人信息保护等方面的安全保护能力，具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述
1	身份鉴别	检查服务器的身份标识与鉴别和用户登录的配置情况。
2	访问控制	检查服务器的访问控制设置情况，包括安全策略覆盖、控制粒度以及权限设置情况等。
3	安全审计	检查服务器的安全审计的配置情况，如覆盖范围、记录的项目和内容等；检查安全审计进程和记录的保护情况。
4	入侵防范	检查服务器在运行过程中的入侵防范措施，如关闭不需要的端口和服务、最小化安装、部署入侵防范产品等。
5	恶意代码防范	检查服务器的恶意代码防范情况，如服务器是否安装统一管理的恶意代码防范软件，是否及时升级病毒库等。

6	可信验证	基于可信根对通信设备的系统引导程序、系统程序、重要配置参数和通信应用程序等进行可信验证，并在应用程序的关键执行环节进行动态可信验证。
7	数据完整性	测评操作系统、数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的完整性保护情况。
8	数据保密性	测评操作系统和数据库管理系统的管理数据、鉴别信息和用户数据在传输和保存过程中的保密性保护情况。
9	数据备份恢复	测评信息系统的安全备份情况，如重要信息的备份、硬件和线路的冗余等。
10	剩余信息保护	测评鉴别信息所在的存储空间被释放或重新分配前是否得到完全清除。
11	个人信息保护	测评是否仅采集和保存业务必需的用户个人信息；是否禁止未授权访问和使用用户个人信息。

4.5.4.5 安全管理中心测评

安全管理中心测评主要涉及系统管理、审计管理、安全管理、集中管控等方面的安全保护能力，具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述
1	系统管理	测评信息系统的系统管理员对系统的管理情况。
2	审计管理	测评信息系统的安全审计员对系统的审计情况。
3	安全管理	测评信息系统的安全管理员对系统的安全策略的配置情况。
4	集中管控	测评网络链路、安全设备、网络设备和服务器等设备的运行状况的集中监测、分析、报警等。

4.5.4.6 安全管理制度测评

安全管理制度测评主要涉及安全策略、管理制度、制定和发布、评审和修订等方

面的安全保护能力，具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述
1	安全策略	测评信息安全工作的总体方针、安全策略，总体目标、范围、原则和安全框架等。
2	管理制度	测评信息系统管理制度在内容覆盖上是否全面、完善。
3	制定和发布	测评信息系统管理制度的制定和发布过程是否遵循一定的流程。
4	评审和修订	测评信息系统管理制度定期评审和修订情况。

4.5.4.7 安全管理机构测评

安全管理制度测评主要涉及岗位设置、人员配备、授权和审批、沟通和合作、审核和检查等方面的安全保护能力，具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述
1	岗位设置	测评信息系统安全主管部门设置情况以及各岗位设置和岗位职责情况。
2	人员配备	测评信息系统各个岗位人员配备情况。
3	授权和审批	测评信息系统对关键活动的授权和审批情况。
4	沟通与合作	测评信息系统内部部门间、与外部单位间的沟通与合作情况。
5	审核和检查	检查信息系统安全工作的审核和测评情况。

4.5.4.8 安全管理人员测评

安全管理人员测评主要涉及人员录用、人员离岗、安全意识教育和培训、外部人员访问管理等方面的安全保护能力，具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述

1	人员录用	测评信息系统录用人员时是否对人员提出要求以及是否对其进行各种审查和考核。
2	人员离岗	测评信息系统人员离岗时是否按照一定的手续办理。
3	安全意识教育和培训	测评是否对人员进行安全方面的教育和培训。
4	外部人员访问管理	测评对第三方人员访问（物理、逻辑）系统是否采取必要控制措施。

4.5.4.9 安全建设管理测评

安全建设管理测评主要涉及定级和备案、安全方案设计、产品采购和使用、自行软件开发、外包软件开发、工程实施、测试验收、系统交付、等级测评、服务供应商选择等方面的安全保护能力，具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述
1	定级和备案	测评是否按照一定要求确定系统的安全等级并完成备案工作。
2	安全方案设计	测评系统整体的安全规划设计是否按照一定流程进行。
3	产品采购和使用	测评是否按照一定的要求进行系统的产品采购。
4	自行软件开发	测评自行开发的软件是否采取必要的措施保证开发过程的安全性。
5	外包软件开发	测评外包开发的软件是否采取必要的措施保证开发过程的安全性和日后的维护工作能够正常开展。

6	工程实施	测评系统建设的实施过程是否采取必要的措施使其在机构可控的范围内进行。
7	测试验收	测评系统运行前是否对其进行测试验收工作。
8	系统交付	测评是否采取必要的措施对系统交付过程进行有效控制。
9	等级测评	测评是否依据国家要求完成等级测评和整改工作。
10	服务供应商选择	测评是否选择符合国家有关规定的安全服务单位进行相关的安全服务工作。

4.5.4.10 安全运维管理测评

安全管理人员测评主要涉及环境管理、资产管理、介质管理、设备维护管理、漏洞和风险管理、网络和系统安全管理、恶意代码防范管理、配置管理、密码管理、变更管理、备份与恢复管理、安全事件处置、应急预案管理、外包运维管理等方面的安全保护能力，具体测评指标描述包括但不限于如下表所示：

序号	安全子类	测评指标描述
1	环境管理	测评是否采取必要的措施对机房的出入控制以及办公环境的人员行为等方面进行安全管理。
2	资产管理	测评是否采取必要的措施对系统的资产进行分类标识管理。
3	介质管理	测评是否采取必要的措施对介质存放环境、使用、维护和销毁等方面进行管理。
4	设备维护管理	测评是否采取必要的措施确保设备在使用、维护和销毁等过程安全。

5	漏洞和风险管理	测评是否采取必要的措施识别安全漏洞和隐患，对发现的安全漏洞和隐患及时进行修补。测评是否定期开展安全测评。
6	网络和系统安全管理	测评是否采取必要的措施对网络和系统的安全配置、系统账户、漏洞扫描和审计日志等方面进行有效的管理。
7	恶意代码防范管理	测评是否采取必要的措施对恶意代码进行有效管理，确保系统具有恶意代码防范能力。
8	配置管理	测评是否记录和保存系统的基本配置信息。
9	密码管理	测评是否能够确保信息系统中密码算法和密钥的使用符合国家密码管理规定。
10	变更管理	测评是否采取必要的措施对系统发生的变更进行有效管理。
11	备份与恢复管理	测评是否采取必要的措施对重要业务信息，系统数据和系统软件进行备份，并确保必要时能够对这些数据有效地恢复。
12	安全事件处置	测评是否采取必要的措施对安全事件进行等级划分和对安全事件的报告、处理过程进行有效的管理。
13	应急预案管理	测评是否针对不同安全事件制定相应的应急预案，是否对应急预案展开培训、演练和审查等。
14	外包运维管理	测评外包运维服务商的选择是否符合国家的有关规定并签订相关协议。

4.6 服务成果内容

服务中产生的全部档案资料版权归采购人所有，未经采购人允许的情况下，不得

以任何形式向第三方提供安全技术文档的全部或部分内容，交付文件包括但不限于如下成果和报告：

1、等保测评实施计划

2、定级备案材料

3、问题整改清单

4、《网络安全等级保护等级测评报告》（2025 版）

5、其他采购人认为有必要的交付物

5 服务要求

5.1 服务技术要求

5.1.1 测评实施要求

（1）投标人提供的资格、资质等证明文件应真实有效，签订合同前采购人有权核查这些证明文件的原件。

（2）网络安全等级保护测评服务必须按照等级保护的标准要求展开，并最终达到广东省公安厅、广州市公安局等级保护的相关要求。

★（3）中标人需要具有广东省网络安全等级测评记录平台账户。（提供中标人对应广东省网络安全等级测评记录平台账户截图作为佐证材料）

（4）根据公安机关要求，中标人在测评过程中，必须通过“广东省网络安全等级测评记录平台”(简称“粤证链”)把首次会议、风险告知、离场确认、末次会议等关键节点，通过拍照打卡方式上传固定，以保证测评服务的合规性。

5.1.2 测评工具要求

（1）在等级保护测评过程中使用的第三方测评工具严格遵循可控性原则，即所有使用的测评工具将事先提交给采购人检查确认，确保在双方认可的范围之内，中标

人所使用软件均取得正版授权，免受第三方提出的侵犯其知识产权的起诉。

（2）必须保证所使用的所有工具和软件不会产生所有权和知识产权纠纷，需要针对该项目承诺无所有权和知识产权纠纷的说明；并保证工具和软件的可用性和可靠性。由此产生的一切责任由投标人负完全责任。（响应文件中须提供说明函，格式自拟）。

（3）本项目使用的所有服务工具和软件无需本项目采购方购买，均由成交中标人自行提供。（响应文件中须提供承诺函，格式自拟）。

（4）测评过程须对应用系统进行代码、数据、网络安全及相关移动应用等相关层面进行安全性分析，投标人应具备等保测评过程中所使用到的专业服务工具。

1）Web 应用源代码渗透扫描管理软件；

2）测评报告管理软件；

3）等级测评质量监控管理软件；

4）网络安全等级保护测评项目智能管理软件；

5）网络安全扫描平台管理软件；

6）等级测评综合管理软件；

7）网络安全检验检测预警管理软件；

8）网络安全等级保护测评管理及及风险评估软件；

9）信息安全测评漏洞信息检测软件。

5.2 管理要求

5.2.1 服务人员

1.项目负责人（1 人），需具一项及以上备以下能力资质：

（1）高级等级测评师证书；

（2）高级网络与信息安全管理师证书；

（3）注册信息安全专业人员（CISP）证书；

（4）项目管理专业人士资格认证证书（PMP）；

（5）国家重要信息系统保护人员（CIIP-T）证书。

2.技术负责人（1 人），需具备一项及以上以下能力资质：

（1）高级等级测评师证书；

（2）高级网络与信息安全管理师证书；

（3）注册信息安全专业人员（CISP）证书；

（4）项目管理专业人士资格认证证书（PMP）。

3.技术队伍人员不少于 5 人，不含项目负责人和技术负责人，全体人员都需具备公安部信息安全等级保护评估中心或中关村信息安全测评联盟颁发的初级或以上的网络安全等级测评师证书或初级或以上的信息安全等级测评师证书。

采购人有权要求报价人提供报价企业资质证书和团队成员证书原件进行复查，全部符合上述要求后，方可继续执行实施工作。实施过程中发现虚假证书、证书有效期过期、团队成员与证书人员不一致，采购人有权单方面中止合同。

5.2.2 进度要求

中标人需合理安排服务时间的进度安排，无条件配合采购人的时间管理。

5.2.3 服务响应要求

中标人应在采购人的监督、指导下，按照本项目管理要求、技术要求和方案编制要求开展等级保护测评工作，并承诺在服务期间项目团队成员能够在工作时间 4 小时内提供现场服务。

5.2.4 服务质量要求

需保证网络安全等级保护测评服务成果符合广东省公安厅、广州市公安局要求。

根据公安机关要求，中标人在测评过程中，必须通过“广东省网络安全等级测评记录平台”(简称“粤证链”)把首次会议、风险告知、离场确认、末次会议等关键节点，通过拍照打卡方式上传固定，以保证测评服务的合规性。

中标人需要具有广东省网络安全等级测评记录平台账户。

5.3 验收标准

中标人协助采购人完成省统筹区域传染病监测预警与应急指挥信息平台的等级保护备案工作，开展等级保护测评、提供整改技术指导服务，提交省统筹区域传染病监测预警与应急指挥信息平台的《网络安全等级保护测评报告》（2025 版），并协助采购人提交至广州市公安局。

5.4 其他要求

5.4.1 资产权属

（1）本服务项目所涉及的数据所有权归采购人所有，中标人只能用于履行义务之目的。

（2）本服务项目不会引起任何已申请、登记的知识产权所有权的转移。

（3）中标人为履行义务所形成的服务成果的知识产权归采购人所有。

（4）中标人保证向采购人提供的服务成果不存在任何侵犯第三方专利权、商标权、著作权等合法权益。如因中标人提供的服务成果侵犯任何第三方的合法权益，导致该第三方追究采购人责任的，中标人应负责解决并赔偿因此给采购人造成的全部损失。

5.4.2 保密要求

中标人须建立项目实施保密管理制度，对于因本项目接触到的涉密文件、涉密数据等信息，必须严格按照保密管理规范进行信息查阅、存储、传输，且严格控制涉密信息的知悉范围；

中标人必须按照国家相关保密规定与采购人签订《保密协议》，一旦违反保密事项，采购人可依法上报监管部门，确定是否终止与中标人的合同关系，并追究法律责任；

项目实施过程中至中标人正式向业主方交付最终技术文档资料时止，中标人必须采取措施对本项目实施过程中的数据、技术文档等资料保密，否则，由于中标人过错导致的上述资料泄密的，中标人必须承担一切责任。项目完成后，采购单位、中标人双方均有责任对本项目的技术保密承担责任。

5.4.3 风险防范要求

在测评过程中，必须充分考虑各种可能对被测系统造成的影响及其危害并准备好相应的应对措施，尽可能减小对目标系统正常运行的干扰，从而减小损失，明确可能存在的风险及控制措施。

6 付款方式

中标人在合同签订后十五个工作日内，向采购人提供下列单据，采购人在收到下列单据 15 个工作日内向中标按合同总价的 100%一次性支付货款。中标人需向采购人提供的单据：

1.合同；

2.相应金额的正式发票；

3.银行出具并经采购人认可和审核无误、以采购人为受益人、金额为合同总价的 50%预付款保函正本 1 份（有效期须长于服务期，晚于省统筹区域传染病监测预警与

应急指挥信息平台（一期）项目终验时间；保函有效期到期前，合同未履行完毕的，中标人须在保函有效期到期前一个月内负责保函续保事宜；保函约定的有效期期满时，银行担保义务履行完毕，中标人必须凭保函原件到银行办理保函担保资金解冻手续；如遗失保函原件，遗失方需向银行提交经合同甲、乙双方签审确认的公函说明）。

省统筹区域传染病监测预警与应急指挥信息平台（一期）项目建设完成并通过终验后的 7 个工作日内，中标人向采购人申请退还预付款保函原件，需提供单据如下：

1、采购合同；

2、需测评信息系统《网络安全等级保护等级测评报告》（2025 版）。

由于财政资金拨款不到位而导致采购人逾期付款的，采购人不承担违约责任，并且此情况不能成为测评服务单位拖延提交成果和拒绝提供服务的理由。采购人有义务配合相关拔付部门完成付款。

7 采购方式

采用择优选取-方案择优采购方式。中心通过广东省网上中介服务超市发布采购公告并明确报价要求，投标商响应时间为 3 个工作日。中介服务机构通过广东省网上中介服务超市进行报价及上传响应方案。在规定报价时间结束后，中心组建项目评审专家组，按照《综合评分细则》，比较服务响应、人员、价格等因素后进行综合评分，推荐 1 家中选服务机构。

8 投标人资格要求

（1）投标人应具备《政府采购法》第二十二条规定的条件。

（2）投标人必须是在中华人民共和国境内注册的具有独立承担民事责任能力的法人，取得合法企业工商营业执照。

（3）未被列入“信用中国”网站中“记录失信被执行人或重大税收违法案件当事人

名单或政府采购严重违法失信行为”的记录名单；不处于“中国政府采购网”中“政府采购严重违法失信行为信息记录”的禁止参加政府采购活动期间。

（4）本项目不接受联合体投标，不允许分包。

★（5）投标人必须具有公安部第三研究所颁发的网络安全服务认证证书等级保护测评服务认证证书（提供中标方对应的有效期内的公安部第三研究所颁发的网络安全服务认证证书等级保护测评服务认证证书复印件）。

★（6）投标人承诺近三年未被全省各级信息安全等级保护工作主管部门或保密及密码工作行政主管部门通报批评（投标人需出具承诺函加盖投标人公章）。

9 递交材料格式

（一）投标人营业执照及相关资格证明资料复印件（企业资质与认证、测评团队人员资质证书、测评工具证明材料，加盖投标人法人公章）

（二）法定代表人授权书（加盖投标人法人公章）

（三）报价表

（四）同类项目业绩

（五）业绩良好评价证明复印件（如有，加盖公章）

（六）最近 3 年企业牵涉的诉讼案件（如有）

（七）详细实施方案（包括总体实施方案、进度计划、服务质量保障方案等）

（八）承诺函

投标人请应根据实际情况编订成册。

10 评分细则

综合评分表

分值构成	价格部分 10.0 分 技术部分 45.0 分 商务部分 45.0 分			
评分项及评分规则				**评分**
一、价格部分				
价格分计算方法：满足招标文件要求且投标价格最低的投标报价为评标基准价，其价格分为满分。其他投标人的价格分统一按照下列公式计算：投标报价得分=(评标基准价／投标报价)×价格分值。				
二、技术部分				
序号	**评分项**	**权重**	**评分规则**	**评分**
1	项目实施方案	10	投标人应针对采购需求对本项目制定实施方案，根据项目实施方案进行综合评审： 1.实施方案完善、科学、可行，技术手段、管理方式、保障措施全面、详细，对项目内容具有支撑性，得 10 分； 2.实施方案较完善、科学、可行，技术手段、管理方式、保障措施等方面较全面、较详细，对项目内容较有支撑性，得 6 分； 3.实施方案基本完善、科学、合理，基本能支撑项目内容，得 3 分； 4.其他情况或未提供总体实施方案，不得分。	
2	项目服务质量保障	10	投标人应针对采购需求对本项目制定测评服务质量保障方案，方案内容包括但不限于测评服务项目质量目标、质量指标、风险防范、质量管理等，根据投标人提供的方案进行综合评审： 1.方案内容详细具体，充分响应项目的实际情况，具有可操作性、可行性的，加 10 分； 2.方案内容较详细具体，基本响应项目的实际情况，具有一定的可操作性、可行性，加 6 分； 3.方案内容较简单，未全面考虑项目的实际情况，可操作性及可行性一般，加 3 分； 4.其他情况不加分。	
3	漏洞挖掘能力	7	投标人具有近 5 年取得国家信息安全漏洞共享平台（CNVD）原创漏洞证明，每提供 1 个证明得 1 分，最高得 7 分。 注：须提供国家信息安全漏洞共享平台	

			（CNVD）出具的原创漏洞证明扫描件，原创漏洞证明的贡献者单位必须为投标人。	
4	测评工具配备情况	18	对投标人为完成本项目服务目标所使用的专用测评工具情况进行评审： 1）Web 应用源代码渗透扫描管理软件； 2）测评报告管理软件； 3）等级测评质量监控管理软件； 4）网络安全等级保护测评项目智能管理软件； 5）网络安全扫描平台管理软件； 6）等级测评综合管理软件； 7）网络安全检验检测预警管理软件； 8)网络安全等级保护测评管理及及风险评估软件； 9）信息安全测评漏洞信息检测软件。 每提供一个以上的工具证明材料，得 2 分，最高得 18 分。 注：须提供采购工具的合同和发票扫描件（如果工具是投标人自主研发的则提供工具的软件著作权登记证书扫描件，否则不得分）	
三、商务部分				
序号	**内容**	**权重**	**评分规则**	**评分**
1	企业资质与认证	10	对投标人提供的企业资质与认证证书进行评审： 1.质量管理体系认证证书； 2.CMA 检验检测机构资质认定证书 3.中国合格评定国家认可委员会检验机构认可证书（CNAS） 4.《计算机信息系统安全服务等级证》二级或二级以上证书 5.中国网络安全审查技术与认证中心颁发的信息安全服务资质认证证书信息安全风险评估、信息安全服务资质认证证书信息安全应急处理、国家信息安全测评信息安全服务资质证书风险评估。 以上每个证书每提供一个得 2 分，最高得 10 分。	

			注：需提供认证证书扫描件，不提供或材料不齐全均不得分。	
2	同类项目经验	10	自 2022 年 11 月 1 日至今承担过相关网络安全等级保护测评服务案例的，每个得 1 分，最高得 10 分。 注：时间以合同签署时间为准。须提供相关业绩合同关键页（含签订合同双方的单位名称、合同项目名称与含签订合同双方的落款盖章、签订日期的关键页），否则不得分；	
3	项目负责人	10	投标人为本项目拟配备项目经理 1 名： 1.具有计算机相关专业研究生学历证书或硕士以上学位证书，得 2 分。 2.具有以下资质证书： （1）高级等级测评师证书； （2）高级网络与信息安全管理师证书； （3）注册信息安全专业人员（CISP）证书； （4）项目管理专业人士资格认证证书（PMP）； （5）国家重要信息系统保护人员（CIIP-T）证书。 每提供一项证书得 2 分，最高得 8 分。 注：须提供该人员上述有效证书复印件，及其在投标人单位近 3 个月以来任意一个月的社保证明（或单位代缴个人所得税税单等），否则对应项不得分。	

4	测评团队人员	15	1.投标人为本项目拟配备技术负责人 1 名，具备以下资质证书： （1）高级等级测评师证书； （2）高级网络与信息安全管理师证书； （3）注册信息安全专业人员（CISP）证书； （4）项目管理专业人士资格认证证书（PMP）。 每提供一项证书得 2 分，最高得 8 分。 2.投标人为本项目拟配备团队成员（不含项目负责人和技术负责人）： （1）技术团队人员不少于 5 人，不含项目负责人和技术负责人，得 4 分； （2）技术团队人员均具备公安部信息安全等级保护评估中心或中关村信息安全测评联盟颁发的初级或以上的网络安全等级测评师证书或初级或以上的信息安全等级测评师证书，得 3 分；若有 1 人未具备该证书，不得分。 注：须提供以上人员上述有效证书复印件，及其在投标人单位近 3 个月以来以来任意一个月的社保证明（或单位代缴个人所得税税单等），否则对应项不得分。	