**采购需求**

**一、项目概况：**

随着佛山市政务信息化智能化的发展、智能交通信息化的日新月异，以及车联网、自动驾驶技术的普及和革新，智能交通领域的网络信息安全形势越来越严峻，落实做好各项网络信息安全工作越来越系统化专业化，在此背景下，系统化开展网络信息安全防护服务项目工作便显得十分必要。项目依据《广东省数字政府网络安全指数指标体系》、《广东省数字政府网络安全指数评估报告指导要求》和佛山市数字政府网络安全体系建设2022专项工作方案，通过网络安全管理、网络安全建设、网络安全运营和网络安全效果四个维度的建设，全面提升佛山市交通运输局网络安全保障能力，满足国家以及部、省相关网络安全监管要求。

**1.主要商务要求**

|  |  |
| --- | --- |
| 标的提供的时间 | 自合同签订生效后1年。 |
| 标的提供的地点 | 采购人指定地点。 |
| 付款方式 | 1期：支付比例40%, 合同签订生效后，采购人向成交供应商支付合同总价的40%；2期：支付比例30%, 2025年12月15日前，成交供应商向采购人提交项目阶段实施报告，采购人确认后10个工作日内向成交供应商支付合同总价的30%；3期：支付比例30%, 项目实施完毕并通过验收后，采购人向成交供应商支付合同总价的30%。如项目发生合同融资，采购人应当将合同款项支付到合同约定收款账户。 |
| 验收要求 | 1期：1）合同期满，收到成交供应商项目验收建议之日起7个工作日内按照合同的约定对履约情况进行验收，成交供应商需为验收提供必需的一切条件及相关费用，并提供本项目的相关文档和验收所需资料，积极配合采购人完成验收工作。2）由采购人组织相关专家进行评审验收（验收地点：佛山市）（费用由成交供应商支付）。 3）验收通过后，向佛山市政务服务数据管理局申请符合性验收，并最终通过验收。 4）验收标准：磋商文件中约定的所有内容。 5）成交供应商应于验收后向采购人提供验收报告、技术文档的归纳、整理、提交，并提供完整的技术资料。 |
| 履约保证金 | 不收取 |
| 其他 |  |

其他商务需求

|  |  |  |  |
| --- | --- | --- | --- |
| 参数性质 | 编号 | 内容明细 | 内容说明 |
|  | 1 | 报价要求 | 1）本项目报价为广东省佛山市目的地交付验收价。 2）响应报价指供应商为完成本项目所收取的全部费用，包含但不限于以下费用： 【本项目内容深化、项目实施所需费用、相关授权及证书的购置、雇员费用、交通差旅费用、培训、验收（含专家验收所涉及的相关费用）、质保期服务、售后服务、各种税费、规费及合同实施过程中的不可预见费用等全部费用，如涉及软件许可使用或技术指导、人员培训的，还应包括软件许可费以及一切技术服务费、人员培训费，并应包含本次采购的采购代理费（成交服务费）】 。 3）供应商须考虑本项目在实施期间的一切可能产生的费用。 4）报价不得高于本项目的采购项目预算金额，否则视为无效报价，作无效响应处理。 5）报价合理性：根据《政府采购货物和服务招标投标管理办法》第六十条的规定：评标委员会认为供应商的报价明显低于其他通过符合性审查供应商的报价，有可 能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；供应商不能证明其报价合理性的，评标委员会应当将其作为无效响应处理。 |
|  | 2 | 付款要求 | 1）合同款项的支付方式：转账结算（银行转账）。 2）付款方：采购人；收款方：成交供应商。 3）开具发票：成交供应商收款时必须持有效发票。收款方、出具发票方、合同乙方均必须与成交供应商名称一致。 4）对于满足合同支付条件的，采购人原则上在收到发票后10个工作日内按照采购合同约定办理支付手续。采购人从中小企业采购货物、工程、服务，应当自货物、 工程、服务交付之日起30日内支付款项。 5）付款期间如因特殊情况需调整，由双方协商处理。 |
|  | 3 | 人员管理 | 1）本项目需设一个相对固定的项目团队，包含项目经理、技术负责人及项目团队人员。供应商应根据项目开展要求，提供信息系统安全、网络安全等信息化类相关的专业技术人员，以确保项目的顺利开展。 2）成交供应商在响应文件中承诺提供的项目团队人员必须按要求投入到本项目中，在合同期内不得擅自更换。成交供应商如因工作安排或其它原因，需要更换项目团队人员时，应事前向采购人书面提出书面申请，未经采购人同意，不得更换人员。 3）除须按采购人的要求对人员作出调整外，如成交供应商未经采购人书面同意擅自更换项目组人员，采购人有权终止合同，由此引致的经济损失，成交供应商须全额赔偿，采购人保留追究成交供应商相关责任的权利。 4）采购人有权以书面形式要求成交供应商更换不能按规定履行合同的人员。 5）即使是采购人要求或同意更换的人员，其代替人员的资质仍应得到采购人的认可，且其资历和经验均不低于被更换人员。由此而产生的费用由成交供应商承担。6）成交供应商对其雇员的人身安全负全部责任。 |
|  | 4 | 保密要求 | 遵守《中华人民共和国保密法》，成交供应商须遵守以下保密要求： 1）实施和维护人员在上岗前应签署保密协议书，并负责约束有关人员的保密工作。 2）实施人员应严格遵守有关法律法规和采购人内部规章制度，不得擅自翻阅、复制、传播所接触的资料或数据。 3）成交供应商现场工程师因维护服务而向采购人提供的数据资料属采购人所有，成交供应商负有保密的责任，成交供应商同意并承诺，对所有保密信息予以严格保密，未经采购人同意，不披露给任何其他人士或机构。 4）如成交供应商人员故意泄露采购人保密信息，成交供应商必须承担后果责任。 5）对蓄意破坏采购人系统或泄密事件的行为，一经查证，采购人有权中止合同，对蓄意破坏者交司法机关制裁和惩罚，成交供应商依法赔偿采购人的损失。 |
|  | 5 | 其他要求 | 1）成交供应商在项目实施过程中须接受采购人（包括采购人聘请的专家）和监理单位（如有）的管理和监督，采购人有权对项目的进度及工作内容等进行合理规划和分配。 2）项目实施过程中，成交供应商必须采用正版测评工具，如因版权问题导致实施计划延误，或受到来自第三方关于侵犯专利权及其他知识产权的法律指控时，成交供应商须承担由此而引起的一切责任和费用。 |
| 说明 |  打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标（响应）无效。 打“▲”号条款为重要参数（如有），若有部分“▲”条款未响应或不满足，将根据评审要求影响其得分，但不作为无效投标（响应）条款。 |

**2.技术标准与要求**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 品目名称 | 标的名称 | 单位 | 数量 | 分项预算单价（元） | 分项预算总价（元） | 所属行业 | 技术要求 |
| 1 | 其他服务 | 网络和数据安全防护服务 | 项 | 1.00 | 1,147,100.00 | 1,147,100.00 | 软件和信息技术服务业 | 详见附表一 |

**附表一：网络和数据安全防护服务**

|  |  |  |
| --- | --- | --- |
| 参数性质 | 序号 | 具体技术(参数)要求 |
|  | 1 | 一、项目背景本项目依据《广东省数字政府网络安全指数指标体系》、《广东省数字政府网络安全指数评估报告指导要求》和佛山市数字政府网络安全体系建设2022专项工作方案，通过网络安全管理、网络安全建设、网络安全运营和网络安全效果四个维度的建设，全面提升佛山市交通运输局网络安全保障能力，满足国家以及部、省相关网络安全监管要求。二、项目目标1.推进安全基础设施服务能力，提升网络安全防护能力。以构建公共安全运行监管服务能力、安全基础支撑为主要方向，以提升各部门网络基础环境及信息系统的安全防护能力为目标，建立持续改进、动态协作机制，构建网络安全态势感知、泛在互信、弹性扩展、智能运营的安全能力，充分考虑长远发展需求，运用先进的安全防护理念，推进安全基础设施改造升级，提升整体网络安全防护能力。2.完善安全保障体系建设，提升安全风险管控能力。结合“数字政府”新思路、新架构、新机制要求，以数据为核心资产，建设主动防御、智能安全、集监控预警、安全防护、审计响应多个安全功能于一身的动态的、闭环的安全功能框架，从安全技术、安全管理、安全运行、安全监管四个维度，融合人员、流程、制度、平台于一体，构建立体化的安全保障体系，进而实现对信息系统安全的可视、可管、可信。实现交通运输发展与网络安全保障的“双翼齐展、双轮齐转”。3.深化监测预警机制建设，提高事件协同处置能力。采用全域智能感知监测和行业协同监测预警通报机制结合的方式，提高网络安全事件协同处置能力。发展网络空间智能态势感知技术，通过静态动态分析、对比关联等方式进行网络安全数据分析和异常检测。加强与各监管部门联动，完善行业信息通报机制，提高跨部门、跨行业的网络安全应急响应、安全事件处置协作、安全预警响应能力。三、项目内容汇总

|  |  |  |
| --- | --- | --- |
| 序号 | 类别 | 服务内容 |
| 1 | 网络安全运营服务 | 基础网络安全防护和提升服务 |
| 2 | 业务系统专项安全服务 |
| 3 | 第三方服务 | 网络安全等级保护测评服务 |

四、详细技术要求**1.基础网络安全防护和提升服务**1.1服务概述基础网络安全防护和提升服务包括：一是全流量威胁管控服务。利用全流量检测设备发现攻击威胁作为线索，根据攻击线索关联到全流量取证设备进行溯源分析，可以确保有证可查，有源可溯，从而达到有效检测+取证溯源的目的。二是运维监控及分析管理服务。进一步强化佛山市交通运输局网络安全集中管控能力，确保单位内资产风险可控。三是边界防御能力升级服务。升级边界防护设备，提升网络边界设备性能，提升工作效率。四是全网一体化安全运营服务。优化监测能力，通过整合第三方检测能力，接入各方威胁情报，利用主动防御手段采集攻击者信息，加强防线发现和监测效果。五是国密证书服务。采用国密算法，提供数据加密传输，保障数据传输机密性、完整性。六是数据安全加密能力升级服务。实现业务系统全链条加密，提升业务系统的安全性，保障数据传输与存储机密性、完整性。1.2服务内容汇总

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 服务项目 | 服务目标及服务内容 | 服务期限 |
| 1 | 全流量追踪溯源服务 | 提供第2层到第7层的每个网络流量数据包的分类识别、记录，并对所有的网络数据建立索引，以确保能完整真实的还原网络安全事件的原始场景。 | 1年 |
| 2 | 威胁检测服务 | 可疑文件的进行动态检测，远控威胁具体行为分析。 | 1年 |
| 3 | 运维监控及分析管理服务 | 控制运维人员能运维哪些设备，执行哪些操作命令，避免运维人员非法或无意执行高危操作，并对运维人员的操作进行实时监控和事后审计。 | 1年 |
| 4 | 网络边界安全防护服务 | 1、新增边界防护服务工具，进一步提升网络安全边界安全防护能力。2、通过对老旧边界防护设备升级，实现边界防护能力的提升。 | 1年 |
| 5 | 全网一体化安全运营服务 | 通过现有及待建安全子系统的对接，分析全网资产及业务运行信息、脆弱性信息、攻击行为信息、风险信息、异常流量信息。 | 1年 |
| 6 | 国密证书服务 | 采用国密算法，提供数据加密传输，保障数据传输机密性、完整性。 | 1年 |
| 7 | 数据安全加密能力升级服务 | 实现业务系统全链条加密，提升业务系统的安全性，保障数据传输与存储机密性、完整性。 | 1年 |

1.3详细技术要求**1.3.1 全流量追踪溯源服务**为采购人提供建设追踪溯源安全服务，接入网络出口流量或者DNS日志，利用异常行为规则分析、人工智能等先进技术，全面监控网内的网络节点，定位黑客控制的关键主机，掌握被攻击事件。在关键位置进行持续检测，特别针对APT、未知威胁攻击事件，配合外部专业安全分析服务对失陷节点进行取证溯源分析，发现隐藏在内网的威胁源头。（1）原始数据存储与检索网络原始流量需要100%准确的存储和检索，这是完整真实的还原网络安全事件原始场景的基础。因此，全流量服务提供了如下关键技术：1）网络流量线速捕获与零碎片存储；2）高精度时间戳；3）高效索引；4）压缩与加密；5）历史流量回放。（2）元数据检索全流量威胁管控服务不仅可以提供完整的网络全流量捕获技术，还可以提供从DPI和流分析方法生成的会话日志，以及每条会话提取的大量元数据。在网络全流量捕获的同时，全流量系统将数千个元数据元素写入高度优化的数据库，以支持快速和高效的查询。**1.3.2 全流量威胁检测服务**威胁检测与溯源工作将利用威胁情报检测技术主动发现失陷机器与外部远控主机进行通信的行为，利用异常行为规则检测技术发现利用合法授权签名或工具等复杂隐蔽技术发起的恶意攻击行为，利用机器学习搭建智能训练模型对特定攻击进行检测发现训练，并且对于检测到的恶意文件进行云端沙箱进行分析判定。然后基于发现的威胁事件所提取的线索，利用先进的威胁情报知识图谱理念和分析技术，结合种类丰富的、具有国际领先性的专业大数据累积提供了一整套方便实用的智能追踪溯源工具，能够帮助佛山市交通运输局在攻击事件中，根据已知线索对攻击对手、其攻击手法、攻击途径、攻击资源和攻击位置后果等进行追踪溯源和拓展分析。**1.3.3** **运维监控及审计服务**（1）为采购人提供运维监控及分析管理服务，管控和审计运维人员操作，提升系统管理安全服务。（2）管理员可以使用集中管控能力提升服务工具控制运维人员能运维哪些设备，执行哪些操作命令，避免运维人员非法或无意执行高危操作，并对运维人员的操作进行实时监控和事后审计。（3）运维人员通过运维监控及分析管理服务工具做运维，不必记录设备的ip地址、用户名、口令等信息，也避免这些敏感信息的泄露，极大地方便了运维工作，提升运维效率。（4）运维监控及分析管理服务对整个运维过程从事前预防、事中控制和事后审计进行全程参与：1）事前预防：建立“自然人-资源-资源帐号”关系，实现统一认证和授权；2）事中控制：建立“自然人-操作-资源”关系，实现操作审计和控制；3）事后审计：建立“自然人-资源-审计日志”关系，实现事后溯源和责任界定。**1.3.4** **边界防御能力升级服务**边界防御能力提升服务是在现有的边界防护水平上扩充性能拓展、网络攻击监测、防病毒等模块服务，通过模块拓展方式，部署在Internet和内部网络之间，执行网络访问控制功能，防止外部用户对内网核心资源的非法访问，同时，也可以阻挡来自Internet的病毒、蠕虫、木马、间谍软件、恶意软件。无论使用何种Email服务器和客户端，只要使用的是标准的SMTP、POP3协议，边界防御能力提升服务工具可以对电子邮件中的病毒进行过滤，防止病毒通过邮件传播。边界防御能力提升服务工具还支持HTTP协议和FTP协议，对于Web浏览、下载、Web邮件及FTP文件传输过程中携带的病毒均可进行拦截。边界防御能力提升服务所采用的工具必须满足以下要求：（1）可以检测和阻断RedCode、Slammer、sober，Zotob、nimda等多种国内外流行的蠕虫病毒，并可通过会话数管理防御未知蠕虫病毒的攻击。（2）可检测和阻断Sub7、netbus、bandook、Doly、GateCrasher等多种国内外主流的后门程序。（3）可以检测和阻断灰鸽子、Storm、Duntek等国内外主流的木马。（4）可以检测和阻断IECodec、Spybuddy等国内外主流的间谍软件。（5）可以检测和阻断CGI、Unicode等间谍软件以及其他 Web攻击。（6）可以检测和阻断ARP攻击、UDPFlooding、SynFlooding 等网络层拒绝服务攻击，还可以处理CC，DNS Query Flooding等多种应用拒绝服务攻击。（7）对所有的攻击行为不但可以检测和阻断，同时支持审计、报警、限值带宽等防御手段。**1.3.5 全网一体化安全运营服务**（1）全网一体化安全运营服务可灵活的对接采购人网络中的安全设备或安全子系统，实现各类型多厂商安全监测防护资源的整合，通过现有及待建安全子系统的对接，相关服务工具可覆盖全网资产及业务运行信息、脆弱性信息、攻击行为信息、风险信息、异常流量信息，同时结合威胁情报订阅功能，在此基础上进行综合分析呈现，通过攻击链的描绘，形成包括被攻击对象和攻击源识别、脆弱性识别、攻击过程及影响分析、安全风险态势等在内的多视角全方位的全网一体化安全运营服务能力。（2）全网一体化安全运营服务是构建在现有的安全防护设施之上的平台服务，可以兼容整合采购人网络中现有的或待建设的各类安全设备、安全子系统或任何安全数据信息源，如防火墙、IDS、防病毒、WAF、APT、蜜罐系统以及威胁情报订阅信息等。基于任意安全设备及数据源的对接，全网一体化安全运营服务采用相关工具通过安全数据的融合分析及呈现实现态势感知能力，包括态势信息的集中采集获取、海量安全态势信息的大数据存储、面向态势感知的大数据集中分析以及态势感知的可视化呈现。（3）全网一体化安全运营服务的构成1）全网一体化安全运营服务是围绕采购人系统为被防护对象，收集影响业务安全的各维度要素信息，进而综合分析挖掘、可视化呈现，对影响业务安全的攻击、威胁、风险、运行等态势形成的持续、动态的感知响应。2）全网一体化安全运营服务是一个全面信息收集、融合处理感知安全状态及风险并进行态势可视化呈现的过程，该过程是动态持续的，通过连续的信息采集分析不断更新对目标网络安全态势的认知理解，掌握安全状态、了解发展规律、进行提前预警。3）全网一体化安全运营服务要处理的是海量多维的信息，要进行多方位的关联及发掘分析，要呈现的也是多对象、多维度、多视角的安全态势。鉴于此，全网一体化安全运营服务根据业务需求，将安全态势涉及的各类安全要素和监视角度进行了梳理归纳，形成了由八个维度组合构成的态势感知体系。这八个维度分别是资产态势、攻击态势、运行感知、脆弱性态势、风险态势、威胁态势、网站态势、流态势，融合这八个感知体系形成有面向综合态势监视的态势总览。4）通过该八个维度的感知，全网一体化安全运营服务可以为采购人呈现出一幅较为通用和完整的网络安全态势的全景图。并且在这八个维度的专项分析呈现和扩展外延中，采购人可以聚焦整合、按需搭配，形成适合自身业务需要和安全态势监控需要的态势感知系统。（4）遵从经典模型实践态势感知1）全网一体化安全运营服务的经典定义为：在大规模系统环境中，对能够引起系统状态发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。2）通过定义，得出由“态势要素获取”“态势理解”“态势预测”组成的三级模型。通过态势要素获取，获得必要的数据，然后通过数据分析进行态势观察理解，进而实现对未来短期时间内的态势预测。**1.3.6** **国密证书管理服务**（1）国密证书管理服务包括证书生成、签发和管理。通过使用符合国家密码管理局规定的国密算法，如SM2、SM3和SM4，并采用双证书的部署方式，提供更高级别的数据加密和数据完整性验证，以确保您的数据在传输过程中的安全性。（2）在注重数据保护的同时，也能保持与传统系统和设备的兼容性。逐步使用国密证书来提升数据保护水平，使得与各种环境进行安全通信更加便捷并确保与其进行安全通信。**1.3.7数据安全加密能力升级服务**（1）数据安全加密能力升级服务的目标是建立以国产密码为主要支撑的信息安全保障体系，实现本单位各系统关键业务信息的机密性、完整性保护，实现国产密码在单位各业务系统中的全面应用。（2）本服务基于国产密码体系，采用密码资源池平台以及密钥管理系统、云服务器密码机构建面向采购人应用系统的加密服务平台，在独立的密钥管理基础设施管控下，对各工作人员提供安全认证和数据二次加密服务，在加密网络传输的基础上，有效提升业务应用的安全性，解决采购人网络及应用系统的商用密码领域的缺失。对于移动终端设备，采用密码服务中间件，配合云密码资源平台，为移动端提供密码服务。（3）数据安全加密能力提升服务所采用的工具需要有以下要求：1）统一的密码管理将密码设备进行集中统一管理，实现对密码设备的多应用系统共享，大幅度减少密码设备的数量，设备采用热备份或负载均衡的模式，可进行在线的设备增加、删除和故障设备自动卸载，此外，可以对设备健康状态的实时监控。2）统一的应用API集成密码机的指令，提供统一的应用层开发接口，应用系统直接选用需要的功能进行简单封装，不需要单独开发API。3）安全的密钥管理特色将密钥使用和安全管理分离，密钥采用集中管理（产生、分发、使用、存放、销毁等），可动态配置密钥属性。4）多算法支持密码服务平台和密码机设备支持通用的国际算法（RSA、DES、MD5等）和国产密码算法（SM2、SM3、SM4），功能场景包括加解密数据、MAC计算和校验等。1.4 服务响应要求（1）技术支持服务1）维护期内通过各种方式为解决系统使用服务，设立客户支持中心，配备足够的专业技术人员解答提出的问题，提供7×24小时服务热线电话。2）维护期内在收到的电话、电子邮件、传真等方式的请求后。提供电话支持服务对在日常使用系统功能和一般性网络故障分析服务，以及在征求同意的前提下，可通过远程登陆的方式解决问题。电话支持和远程服务的类型和响应时间如下：网络故障分析小于1小时；系统功能使用小于1小时；系统软硬件故障小于2小时。（2）设备可用性保障服务当网络系统发生故障时，服务方在30分钟内响应支持，5小时内保障维护对象恢复正常运行。故障排除后3个工作日内向用户提交《故障处理报告》；故障排除10个工作日内提供维护对象故障彻底消除及优化方案，实施相关的系统升级、参数设置调整。（3）应急支持服务如遇节假日、敏感时期及突发特重大事件，需派相关人员免费去现场提供系统维护保障服务。1.5 服务成果《安全监测报告》（每月一份）《综合风险分析报告》（每季度一份）**2.业务系统专项安全服务**2.1 服务概述通过网络安全专项规划：渗透测试、安全整改与加固、应急演练、安全培训、安全运维等服务，实现事前、事中、事后全流程安全保障能力。2.2 服务内容

|  |  |
| --- | --- |
| 序号 | 服务项 |
| 1 | 渗透测试服务 |
| 2 | 安全整改与加固服务 |
| 3 | 应急演练 |
| 4 | 安全培训服务 |
| 5 | 安全运维服务 |

**2.2.1渗透测试服务**渗透测试是在采购人授权、监督和不影响目标系统正常运行的情况下，工程师采用手工方式和安全检测工具，模拟黑客的攻击方法对目标系统的技术弱点、缺陷或漏洞进行可控的非破坏性攻击测试，由安全专家模拟黑客入侵手段，检测常见安全问题和系统逻辑层面安全隐患，对业务系统进行漏洞测试及人工验证，验证当前安全机制在抵抗入侵时的有效性，最后提供渗透测试报告，使得采购人可以清晰知晓目标系统中存在的安全隐患。**2.2.2 安全整改与加固服务**针对渗透测试、安全检查或日常工作中发现的问题，修复也是重要的一环。不全面或不合理的处理问题，难以避免问题再次发生，可能还会带来新的风险。由专业技术人员利用专业技能和经验，结合采购人的安全现状，编写安全整改与加固方案，提出修复建议和措施，根据方案进行安全整改与加固，有效地解决发现的安全问题，提升信息系统的整体安全性。**2.2.3 应急演练**应急演练是构建我局网络数据安全体系的重要一环，在紧急情况下，时间往往是救援的关键。应急演练能够有效提高我局各个部门的应急响应速度，锻炼各岗位人员在突发网络安全数据事件发生时能够快速做出反应，采取有效措施，最大限度地减少损失。应急演练需包括仿真演练场景搭建、演练脚本编制及演练场景互动环节，通过在模拟环境中对各种突发事件的应对，可以发现和解决在真实事件中可能遇到的问题，不断磨合和完善我局的应急预案和应急管理机制，确保在实际危机中能够更加从容应对。**2.2.4 安全培训服务**随着信息化的不断发展，网络安全技术也不断在更新，《网络安全法》、《数据安全法》及《个人信息保护法》相继出台，采购人员工需要通过不断学习，更新网络安全知识。由专业技术人员进行安全培训，能够使采购人员工了解最新的安全漏洞和攻击技术，获取专业的指导和建议，并学习如何有效应对和预防安全事件。**2.2.5安全运维服务**采购人经过多年的信息化和信息安全建设，已经基本完成国家和行业网络安全保障要求，同时采购人通过积极推进信息安全保障体系建设，基本保障了重要信息系统的稳定运行。采购人已经从安全软硬件的建设阶段进入安全运行维护与保障阶段。由于信息安全技术不断更新，信息系统不断面临新的风险，目前在实际安全工作过程中采购人还是面临各种的管理问题。信息安全运维工作具有专业化、标准化等特点，需要专业的信息安全人员、工具和技术加以支撑。一方面，各种安全设备的不断部署，需要专业的安全人员进行维护；另一方面信息安全也是一个动态的过程，尤其在安全问题的及时发现和解决，事后的分析、以及在遇到突发、重大安全事故时，仅靠采购人自身的技术和管理人员，很难应对众多的安全问题。2.3 服务响应要求（1）技术支持服务1）维护期内通过各种方式为解决系统使用服务，设立客户支持中心，配备足够的专业技术人员解答提出的问题，提供7×24小时服务热线电话。2）维护期内在收到的电话、电子邮件、传真等方式的请求后。提供电话支持服务对在日常使用系统功能和一般性网络故障分析服务，以及在征求同意的前提下，可通过远程登陆的方式解决问题。电话支持和远程服务的类型和响应时间如下：网络故障分析小于1小时；系统功能使用小于1小时；系统软硬件故障小于2小时。（2）设备可用性保障服务当网络系统发生故障时，服务方在30分钟内响应支持，5小时内保障维护对象恢复正常运行。故障排除后3个工作日内向用户提交《故障处理报告》；故障排除10个工作日内提供维护对象故障彻底消除及优化方案，实施相关的系统升级、参数设置调整。（3）应急支持服务如遇节假日、敏感时期及突发特重大事件，需派相关人员免费去现场提供系统维护保障服务。2.4 服务成果（1）《渗透测试报告》（每年一份）（2）《安全整改与加固报告》（每年一份）（3）《应急演练方案》《应急演练报告》（每年一份）（4）《安全运维服务月报》（每季度一份）**注：上述“基础网络安全防护和提升服务”和“业务系统专项安全服务”两部分技术要求的补充要求：**（1）★合同签订后5个工作日内，成交供应商须按采购人要求编制本项目实施方案，内容包括但不限于全流量追踪溯源服务工具、全流量威胁检测服务工具、运维监控及分析管理服务工具、边界防御能力升级服务工具、全网一体化安全运营服务工具、漏洞扫描服务工具和基线检查服务工具等工具部署方案、应用方案以及应用计划等，确保提供的服务工具符合要求，无法满足需求的视为虚假响应，采购人将终止合同，由此引发的所有损失由成交供应商承担。**3.第三方服务（等保测评服务）**3.1 服务概述根据《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》的规定，和《关于转发国家网络安全等级保护工作协调小组办公室关于落实网络安全保护重点措施深入实施网络安全等级保护制度的指导意见的函》（佛公函〔2022〕177号）要求，为保障系统日常运行安全，按照GB/T2505 8-2010《信息安全技术信息系统安全等级保护实施指南》、GBT 22239-2019《信息安全技术网络安全等级保护基本要求》的规范要求，针对自身功能，制定出系统安全等级测评需求，通过该测评使系统具有更强的自主安全保护能力。综上所述，拟对采购人3个三级系统，3个二级系统进行等级保护测评工作，具体清单如下：

| **序号** | **信息系统名称** | **等级** | **是否在互联网区** |
| --- | --- | --- | --- |
| 1 | 佛山市城市道路建设和养护行业诚信管理平台（二期） | 三级 | 是 |
| 2 | 佛山市驾培招生网络报名平台(佛山学车公共服务平台) | 三级 | 是 |
| 3 | 佛山市驾培监管服务平台 | 三级 | 是 |
| 4 | 佛山市汽车维修电子健康档案信息服务平台 | 二级 | 是 |
| 5 | 佛山市城市道路工程农民工工资信息管理平台 | 二级 | 是 |
| 6 | 佛山市城乡道路客运成品油价格补助和新能源车辆运营补助里程统计报送系统 | 二级 | 是 |

3.2 服务要求（1）在安全测评工作中通过现场差距测评对系统出具差距测评报告，并针对在差距测评工作中发现的安全问题制定系统整改方案，按照系统整改方案对系统存在的安全漏洞进行整改，整改完成后进行验收测评，测评通过则出具验收测评报告。（2）等级保护测评内容主要包括以下方面：安全物理环境、安全通信网络、安全区域边界、安全计算环境和安全管理中心和安全管理制度等。3.3 服务成果包含但不限于：《等级保护测评报告》《备案材料》。五、单位技术能力及技术人员要求：1）供应商应具有网络安全等级保护的服务能力，具有信息系统集成等相关的能力，并且在服务过程中必须按采购人要求以及保密、涉密等相关标准做好信息保密工作，并能提供售后服务保障。2）供应商应根据项目实施内容，投入具有相关资历及信息化类（如系统分析、程序分析、信息安全、信息系统监理、网络安全测评、信息系统规划、数据处理分析、通信工程等）的专业技术人员到本项目中，已确保项目的顺利开展。   |
| ★ | 2 | 以下内容为带“★”号的技术要求的汇总：★合同签订后5个工作日内，成交供应商须按采购人要求编制本项目实施方案，内容包括但不限于全流量追踪溯源服务工具、全流量威胁检测服务工具、运维监控及分析管理服务工具、边界防御能力升级服务工具、全网一体化安全运营服务工具、漏洞扫描服务工具和基线检查服务工具等工具部署方案、应用方案以及应用计划等，确保提供的服务工具符合要求，无法满足需求的视为虚假响应，采购人将终止合同，由此引发的所有损失由成交供应商承担。 |
| 说明 |  打“★”号条款为实质性条款，若有任何一条负偏离或不满足则导致投标无效。 打“▲”号条款为重要技术参数，若有部分“▲”条款未响应或不满足，将导致其响应性评审加重扣分，但不作为无效投标条款。 |