**竞价文件**

**采购方式：线上竞价**

**项目名称：广东省肇庆监狱2025年网络安全保障服务项目（第二次）**

**广东省肇庆监狱**

**采联国际招标采购集团有限公司**

**二〇二五年七月**

第一章 竞价须知

1. 本项目通过云采链线上采购一体化平台（www.choicelink.cn）进行竞价，参与竞价的供应商必须登录平台进行注册，注册成功后方可参与项目竞价。
2. 语言要求

供应商提交的响应文件以及供应商与采购人或平台就有关项目的所有来往函电均应使用中文书写。供应商提交的文件或资料可以用另一种语言，但相应内容应附有中文翻译本，由翻译机构盖章或者翻译人员签名。两种语言不一致时以中文翻译本为准。

1. **在云采链平台参与项目竞价后放弃成交资格超过三次（含三次）的供应商连同该供应商同一法人名下所有公司将被列入平台黑名单，永久不得参与平台的项目竞价。**
2. 竞价须知
3. **竞价说明**
4. 参与竞价的供应商应承担所有与准备和参加竞价有关的费用，不论竞价的结果如何，采购人和代理机构均无义务和责任承担这些费用。
5. 参与竞价的供应商必须按竞价附件的格式填写，不得随意增加或删除表格内容。除单价、金额或项目要求填写的内容外，不得擅自改动竞价附件内容，否则将有可能影响成交结果，不推荐为成交候选人。
6. 参与竞价的供应商需对采购需求书的所有条款进行整体响应，采购需求书条款若有一条负偏离或不响应，不推荐为成交候选人。
7. 若成交供应商自身原因无法完成本项目，则采购人有权利保留追究责任。
8. 成交供应商因自身原因被取消成交资格，采购人可重新启动采购或按竞价公告规定顺延推选符合要求的供应商作为成交供应商。
9. 若本项目竞价采购失败，采购人将重新采购，届时采购人有权根据项目具体情况，决定重新采购项目的采购方式。
10. 成交供应商若无正当理由恶意放弃成交资格，采购人有权将拒绝其参加本项目重新组织的竞价采购活动。
11. 如采购人或代理机构在审核或复核参与竞价的供应商所提交的竞价资料时，供应商须无条件配合；期间若发现存在弄虚作假或相关的失信记录或违反国家法律法规等相关的不良情形，采购人可取消其成交资格并保留追究责任的权力。
12. 参与竞价的供应商向我司咨询的有关项目事项，一切以竞价文件规定和竞价公告规定以及本公司的书面答复为准，其他一切形式均为个人意见，不代表本公司的意见。
13. 参与竞价的供应商应认真阅读、并充分理解竞价文件的全部内容（包括所有的补充、修改内容重要事项、格式、条款、服务要求和技术规范、参数及要求等）。供应商没有按照竞价文件要求提交全部资料，或者参与竞价所上传的文件没有对竞价文件在各方面都作出实质性响应是供应商的风险，有可能导致其竞价被拒绝，或被认定为无效竞价。
14. 采购人有权拒绝接受任何不合格的货物或服务，由此产生的费用及相关后果均由成交供应商自行承担。
15. 供应商认为竞价结果损害其权益的，应按照云采链平台相关指引在规定的时间内向采购人或代理机构提交书面质疑，不提交的视为无异议，逾期提交将不予受理。
16. 本竞价公告和竞价文件的解释权归“云采链线上采购一体化平台”所有。
17. **竞价文件的澄清或修改**
18. 采购人或者采购代理机构可以对已发出的竞价文件进行必要的澄清或者修改。澄清或者修改的内容将在云采链平台上发布澄清（更正/变更）公告。
19. 无论澄清或者修改的内容是否影响竞价，平台将以短信形式通知所有的报名供应商；报名供应商应按要求履行相应的义务；如报名截止时间少于一个工作日的，采购人或者采购代理机构应当相应顺延报名的截止时间。
20. 采购人或者采购代理机构发出的澄清或修改（更正/变更）的内容为竞价文件的组成部分，并对供应商具有约束力。
21. **报名要求（参与竞价的供应商资质要求: 报名时需要提供以下盖章资料，并对上传的报名文件资料承担责任）**
22. 提供在中华人民共和国境内注册的法人或其他组织的营业执照或事业单位法人证书或社会团体法人登记证书复印件；如国家另有规定的，则从其规定（分公司参与竞价，须取得具有法人资格的总公司（总所）出具给分公司的授权书，并提供总公司（总所）和分公司的营业执照（执业许可证）复印件。已由总公司（总所）授权的，总公司（总所）取得的相关资质证书对分公司有效，法律法规或者行业另有规定的除外）；
23. 报名供应商须是：具有良好的商业信誉和健全的财务会计制度；有依法缴纳税收和社会保障资金的良好记录；具有履行合同所必需的设备和专业技术能力；参加采购活动前3年内在经营活动中没有重大违法记录的书面声明；具备法律、行政法规规定的其他条件；法定代表人或单位负责人与所参投的本项目其他供应商的法定代表人或单位负责人不为同一人且与其他供应商之间不存在直接控股、管理关系；本项目不接受转包分包且不接受联合体参与竞价（提供《供应商资格声明函》，格式见附件）；
24. 供应商完全响应本项目采购需求的条款、内容及要求的，提供采购需求书响应声明函**，格式详见附件。**
25. 供应商须提供1人担任项目经理，要求具有信息系统项目管理师证书，同时具备等保三级及以上项目经验。供应商需提供：①有效的信息系统项目管理师证书；等保三级及以上项目合同关键页（含该人员的名称、签订合同双方的单位名称、合同项目名称、合同概况、签订合同双方的落款盖章、签订日期的关键页）。
26. 供应商须提供至少1人专职工程师，要求具有信息安全工程师证书（或为CISP注册信息安全专业人员，或为CISAW信息安全保障人员），同时具备等保三级及以上项目经验。供应商须提供：①有效的信息安全工程师证书，或CISP注册信息安全专业人员有效的证明材料，或CISAW信息安全保障人员有效的证明材料；等保三级及以上项目合同关键页（含该人员的名称、签订合同双方的单位名称、合同项目名称、合同概况、签订合同双方的落款盖章、签订日期的关键页）。
27. 供应商须提供不少于2人现场测评人员，且现场人员具有“信息安全等级测评师”或“网络安全等级测评师证书”中级及以上认证证书，供应商须提供有效的公安部信息安全等级保护评估中心颁布的信息安全等级测评师证书（DJCP），或中关村信息安全测评联盟颁布的网络安全等级测评师证书。
28. **报价要求（报价时需要提供以下盖章资料，**并对上传的竞价文件资料承担责任**）**
29. 通过报名供应商应根据本公告要求，在规定的竞价时间内对采购项目进行报价，同时按本公告要求完整、真实、准确地填写并上传相应报价附件**（上传报价表）。**
30. **公告中的报价次数指报价期间供应商可进行的最多报价次数。如报价次数为2次，指供应商最多可进行2次报价。如供应商只进行1次报价，则以此次报价为准；如供应商因报价有误或其他原因需重新进行第2次报价，则以第2次报价为准，以此类推。**
31. **确定成交候选人**
32. 本项目以最低价成交的方式确定成交供应商。报价时间截止后，系统按报价（经价格核准后的价格）由低到高顺序排列，报价最低的为第一成交候选人，报价相同的，按报价时间在前的为第一成交候选人；报价次低的为第二成交候选人，以此类推。
33. **无效报价**
34. 参与竞价的供应商须提供本项目要求的资质文件，如果不按公告规定或竞价文件要求等相关规定提供符合要求的资质文件，将被视为无效报价。
35. 参与竞价的供应商须对本项目采购内容进行整体报价，任何只对其中一部分内容进行的报价都被视为无效报价。
36. 报价表以及有报价供应商落款的报价文件必须加盖报价供应商公章，否则视为无效报价。
37. 大写金额和小写金额不一致的，以大写金额为准；单价金额小数点或者百分比有明显错位的，以报价表的总价为准，并修改单价；总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；不接受总价优惠折扣形式的报价，供应商应将对项目的优惠直接在清单报价中体现出来。如果供应商不接受对其错误的更正，其报价将被视为无效报价。
38. **按有关法律、法规、规章属于报价无效的。**
39. **有下列情形之一的，视为串通竞价，其报价无效：**
40. 存在单位负责人为同一人或存在控股、管理关系的不同单位参与同一竞价项目；
41. 不同供应商的响应文件由同一单位或者个人编制；
42. 不同供应商委托同一单位或者个人办理竞价事宜；
43. **不同供应商使用同一IP地址参与竞价；**
44. 不同供应商的响应文件载明的项目管理成员或者联系人员为同一人；
45. 不同供应商的响应文件异常一致或者报价呈规律性差异；
46. 不同供应商的响应文件相互混淆；
47. 不同供应商的平台使用费从同一单位或者个人的账户转出。
48. **竞价活动失败**
49. 出现下列情况的，本项目竞价活动失败：
50. 有效报名供应商不足3家；
51. 有效报价供应商不足3家。

2.出现影响采购公正的违法、违规行为的。

3.因重大变故，采购任务取消的。

1. **使用费**

1.成交供应商须向平台服务商云采链线上采购一体化平台缴纳平台使用费，金额为成交金额的1.2%（四舍五入取整数）。

2.成交供应商无正当理由放弃成交资格的必须按竞价公告等相关规定缴纳相应的平台使用费。

3.如确实因不可抗力放弃成交资格的，应在不可抗力发生后三个工作日内予以通知采购代理机构并提供相关的证明；如逾期，采购代理机构不予退还平台使用费。

1. **联系方式**

1、采购人联系人及联系方式：  
广东省肇庆监狱业务咨询部门电话 0758-3173863。  
2、纪检监督部门：  
广东省肇庆监狱纪检监督部门电话 0758—3173809。

3、扫码关注微信公众号“云采链互联服务平台”，即可在线咨询相关事项。



**第二章 采购需求书**

**说明：**

1. **响应供应商须对本项目进行整体响应，任何只对其中一部分进行的响应都被视为无效响应。**
2. **项目一览表**

|  |  |  |  |
| --- | --- | --- | --- |
| **项目内容** | **数量** | **项目服务期限** | **最高限价** |
| 广东省肇庆监狱2025年网络安全保障服务项目（第二次） | 1项 | 1. 等保测评服务以合同签订之日起60天内完成测评服务，以提交报告给公安并收到回执为准。 2. 网络安全加固，网络安全应急响应等服务以2025年8月12日起，服务期限为一年。 | 人民币180000元 |

1. **项目名称**

项目名称：广东省肇庆监狱2025年网络安全保障服务项目（第二次）

1. **项目金额**

本项目最高限价为180000元*。*

项目合同总价包括了服务期间所有服务费用、设备费用、正常的税金、雇员费用、税费、不可预见费等完成本项目内容所需的一切费用及项目实施过程中应预见和不可预见费用等。成交人不得再向采购人收取任何费用。

1. **项目服务期限**
2. 等保测评服务以合同签订之日起60天内完成测评服务，以提交报告给公安并收到回执为准。
3. 网络安全加固，网络安全应急响应等服务以2025年8月12日起，服务期限为一年。
4. **项目内容**
5. **项目概述**

广东省肇庆监狱拟对已完成定级、备案的第三级信息系统（包括其所含各相关子系统（模块））开展网络安全等级保护测评、整改，网络安全设备升级，安全加固服务，网络安全培训及网络安全应急演练等相关工作。

1. **项目范围**

本项目服务范围包括：共计1个已完成定级、备案第三级信息系统（包括其所含各相关子系统（模块））；上述信息系统所涉及的网络、主机、安全设备、应用、数据、机房环境、管理制度等；监狱网络安全设备升级；安全加固服务。具体如下：

1. 信息系统及分布情况：1个第三级信息系统（包括其所含各相关子系统（模块））所涉及的基础软硬件环境等均部署于监狱中心机房。成交人需根据实施阶段对待测信息系统所涵盖的范围进行调整，采购人无需支付额外费用。
2. 网络情况：系统部署与政法内网，政法内网部分包括政法网出口、核心区、安全管理区、生产区（其中生产区包含应用区和数据库区）、存储区等网络区域，通过专线与上级单位互联，进行数据交互。
3. 监狱网络安全设备：天融信应用安全网关系统（IDP特征库、WEB过滤库、专业版快速扫描查杀防病毒库、应用识别特征库1年升级服务许可,适用于NU-31116产品(绑SN)），如果旧版本不能升级，需提供部署新版本。天融信Web应用安全防护系统（WAF产品特征库1年升级License,适用于TWF-52116产品(绑SN)），如果旧版本不能升级，需提供部署新版本。天融信安全管理系统V3(日志服务器系统），原许可型号TAEX\_S，许可类型396e0c65，升级版本，如果旧版本不能升级，需提供部署新版本，系统永久授权。
4. 安全加固服务：对单位终端、操作系统安全加固和优化，对机房网络设备安全加固和优化，包括主机（PC、办公终端）、网络设备和网络设施（交换机、路由器等）打补丁、升级、修补、加固和优化，协助处理应急网络安全事件并提供相关报告，对全狱终端系统、安全设备、网络进行漏洞扫描、修复，要求每月现场驻场处置不少于3个工作日。网络安全加固和优化过程需记录完整技术方法，形成经验教训登记册文档，移交给建设单位。
5. 网络安全应急响应服务：对建设单位网络安全事件进行现场应急处置；节假日提供网络安全检查及运维协助，如线上处理不了则必须当天到达现场处理；合同服务期内组织一次网络安全应急演练，形成网络安全应急演练记录表，记录完整技术方法，移交给建设单位。
6. 网络安全培训：组织一次本地网络安全知识培训，形成网络安全培训记录表，记录完整技术方法，移交给建设单位；提供不少于2人次CISP(或同等国家认证）线下培训课程服务与考试领证服务。
7. **项目内容清单**

|  |  |  |  |
| --- | --- | --- | --- |
| **序号** | **项目内容** | **内容详情** | **备注** |
| 1 | 信息系统等级保护测评服务 | 一个三级系统的等保测评 | 一年服务 |
| 2 | 信息系统等级保护整改优化 | 1. 对测评系统进行渗透测试、漏洞扫描并整优化以满足等保要求 2. 对管理制度审核、建设以满足等保要求 3. 对测评系统差距分析、风险评估并整改优化以满足等保要求 | 一年服务 |
| 3 | 安全加固服务 | 对全狱终端，服务器，业务系统，安全设备、网络进行漏洞扫描、修复（要求每月现场驻场处置时间不少于3个工作日） | 一年服务 |
| 4 | 网络安全设备病毒库，特征库升级服务，审计系统授权数升级服务 | 天融信应用安全网关系统（IDP特征库、WEB过滤库、专业版快速扫描查杀防病毒库、应用识别特征库升级服务许可,适用于NU-31116产品(绑SN)） | 一年服务 |
| 5 | 天融信Web应用安全防护系统（WAF产品特征库升级License,适用于TWF-52116产品(绑SN)） | 一年服务 |
| 6 | 天融信安全管理系统V3(日志服务器系统），原许可型号TAEX\_S，许可类型396e0c65，升级版本或提供全新版本。 | 永久授权 |
| 7 | 网络安全应急响应服务 | 1. 网络安全事件应急处置（现场） 2. 节假日提供网络安全检查及运维协助 3. 组织网络安全应急演练一次 | 一年服务 |
| 8 | 网络安全培训 | 1. 组织本地网络安全知识培训一次（具体培训时间由成交供应商与采购人进行协商确认） 2. 提供不少于2人次CISP(或同等国家认证）线下培训课程服务与考试领证服务 | 一年服务 |

1. **项目目标**

按照《信息安全技术网络安全等级保护基本要求》（GB/T22239-2019）标准要求对第三级信息系统开展等保测评工作，协助监狱完成各类问题的整改及验证工作，合格后出具等级保护测评等相关报告。更新监狱网络安全设备特征库、病毒库，更新日志服务器系统版本或提高全新版本。对监狱终端、服务器、网络设备提供漏洞扫描，修复，提供每月不少于3个工作日的现场驻场服务，协助处理网络安全漏洞及应急网络安全事件。

1. **测评标准**

依照我国网络安全等级保护法律法规和制度规范，开展等保测评工作。项目实施过程中应包括不限于以下法规和技术标准：

1. 《中华人民共和国网络安全法》
2. 《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）
3. 《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）
4. 《关于信息安全等级保护工作的实施意见》（公通字〔2004〕66 号）
5. 《信息安全等级保护管理办法》（公通字〔2007〕43 号）
6. 《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）
7. 《信息安全等级保护备案实施细则》（公信安〔2007〕1360 号）
8. 《计算机信息系统安全保护等级划分准则》（GB 17859—1999）
9. 《信息安全技术 网络安全等级保护测评要求》（GB/T 28448—2019）
10. 《信息安全技术 网络安全等级保护测评过程指南》（GB/T 28449—2018）
11. 《信息安全技术 网络安全等级保护基本要求》（GB/T 22239-2019）
12. 《信息安全技术 网络安全等级保护定级指南》（GB/T 22240-2020）
13. **服务要求**
14. **具体要求内容**

本项目采购的信息安全评测服务包括差距分析、风险评估、整改建议、等级保护测评和制度审核等，详细如下：

1. 信息系统差距分析活动

信息系统安全等级保护差距分析将根据《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 网络安全等级保护测评过程指南》（GB/T 28229-2018）等标准文件的要求，对已定级信息系统，进行系统现状调研，逐项进行合规性检测。其实质是采用基线安全分析的方法，明确当前信息系统与等级保护要求的不符合项及差距。

根据项目的总体要求及信息系统等级保护体系建设现状需要，对信息系统进行差距分析，从安全技术差距分析测评和安全管理差距分析测评两部分进行，对系统各项安全指标进行符合性评估，并标识系统不符合项，明确系统与国家安全等级保护相关标准要求的差距。

1. 信息系统整改咨询服务

信息系统安全建设整改咨询主要是依据差距分析报告，对被测信息系统面临的安全风险进行总结分析，对信息系统不符合信息系统等级保护建设基本要求的部分提供可行性整改建议或方案，从整体上把控内容，主要从技术和管理两方面进行整改，最终能够使被测信息系统在进行安全建设整改后可通过等级保护的测评。

成交人需要根据差距分析中出现的问题、差距分析中存在的差距点、渗透测试发现的信息系统脆弱性以及漏洞扫描结果等相关信息，结合系统实际情况，提供合理、切实可行的整改加固建议，并全程协助各单位进行整改工作，使各系统达到等级保护相应级别的要求。成交人据此完成《网络安全等级保护整改建议书》及其它资料的编撰和整理。

1. 信息系统等级保护测评服务

按照等级保护《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 网络安全等级保护基本要求》（GB/T22239-2019）对待测信息系统进行正式的信息安全等级保护测评及复测评，出具公安部门认可的网络安全等级测评报告。

信息系统安全等级测评主要检测和评估信息系统在安全技术、安全管理等方面是否符合已确定的安全等级三级的要求，对于尚未符合要求的信息系统，分析和评估其潜在威胁、薄弱环节以及现有安全防护措施，综合考虑信息系统的重要性和面临的安全威胁等因素，提出相应的整改建议，并根据初次等级保护测评工作中发现的问题进行整改，待整改工作结束后，进行等级保护复测确认，以确保信息系统的安全保护措施符合相应安全等级三级的基本要求，并提交符合国家等级保护测评三级要求的等级保护测评报告。

1. 管理制度审核

本项服务旨在依据国家信息安全管理相关要求，成交人为采购人开展安全建设及整改工作提供咨询指导。成交人依据有关国家标准，审核本项目执行过程中编制的网络安全等保相关制度，并提出修改意见。

1. 协助应检

成交人需配合采购人进行网络安全等保相关检查。具体内容如下：

检查前：需协助对应检系统开展自查，对自查发现的问题进行整改和完善；

检查中：指派专人参与的安全检查，并对检查过程中发现的问题进行记录；

检查后：协助完成网安检查过程中出现的安全问题的整改及编制整改报告。

1. 信息系统风险评估工作

成交人需依据风险评估工作的相关内容，对所有被评估对象进行检查、分析，使其满足项目最终验收要求。须严格按照相关制度和标准的要求，结合被评估单位的具体情况，确定科学严谨的现场实施方案，并完成《风险评估实施方案》的编写。风险评估方案的内容一般包括（但不仅限于）：团队组织：包括评估团队成员、组织结构、角色、责任等内容。工作计划：风险评估各阶段的工作计划，包括工作内容、工作形式、工作成果等内容。时间进度安排：项目实施的时间进度安排。

1. 渗透测试

成交人依据已经掌握的安全漏洞信息，模拟黑客的真实攻击方法对系统和网络进行非破坏性质的攻击性测试，并出具《信息系统渗透测试报告》。渗透测试内容应该主要包含外部测试、内部测试，黑盒测试和白盒测试，渗透测试范围应包含第三级系统及各相关子系统，所有的渗透测试行为需在采购人的书面明确授权和监督下进行。

1. 漏洞扫描

通过技术手段对第三级系统及各相关子系统进行漏洞扫描，发现可被利用的安全漏洞，并协助项目建设各相关单位进行漏洞修复。进行漏洞扫描后根据扫描结果出具《信息系统漏洞扫描报告》。

1. 安全基线核查

基于网络安全法要求以及监管合规要求进行网络安全法责任落实情况预查，为特殊时期的安全提供保障、落实国家政策、法律法规及监管单位的政策合规性的需求。预查内容包括：网络安全保障工作落实情况预查、网络安全信息系统预警及处理方案预查、网络安全管理制度建设与落实情况预查、其他（包含制度、数据、运维、边界、管理、新技术、新应用等）网络安全保护工作情况预查等。基于预查结果出具《信息系统安全配置策略符合性检查报告》、《信息系统安全策略自查报告》、《信息系统安全配置应急自查报告》。

1. 网络加固及现场驻场服务

对单位终端操作系统安全加固和优化，对机房网络设备安全加固和优化，包括主机（PC、办公终端）、网络设备和网络设施（交换机、路由器等）进行打补丁、升级、修补、加固和优化，协助处理应急网络安全事件并提供相关报告，对全狱终端系统，安全设备、网络进行漏洞扫描、修复，要求每月安排工程师现场驻场处置不少于3个工作日。

1. 监狱网络安全设备授权服务

天融信应用安全网关系统（IDP特征库、WEB过滤库、专业版快速扫描查杀防病毒库、应用识别特征库1年升级服务许可,适用于NU-31116产品(绑SN)），如果旧版本不能升级，需提供部署新版本。天融信Web应用安全防护系统（WAF产品特征库1年升级License,适用于TWF-52116产品(绑SN)），如果旧版本不能升级，需提供部署新版本。天融信安全管理系统V3(日志服务器系统），原许可型号TAEX\_S，许可类型396e0c65，升级版本，如果旧版本不能升级，需提供部署新版本，系统永久授权。

1. 网络安全培训服务

成交人为采购人提供1次本地网络安全培训，形成《网络安全培训会议纪要》。成交人为采购人提供不少于2人次CISP(或同等国家认证）线下培训课程服务与考试领证服务**，**培训费等相关费用由成交人承担。

1. 网络安全应急响应服务

成交人需成立项目网络安全应急响应服务团队，团队至少有一名项目经理与一名专职网络安全工程师组成，需提供7\*24技术支持服务，采购人出现网络安全事件需要应急处置时，成交人需30分钟内响应，2小时内安排项目专职工程师到采购人指定现场进行处置，同时节假日提供网络安全检查及运维协助，形成《网络安全事件应急处置统计表》。组织网络安全应急演练一次，形成《网络安全事件应急演练会议纪要》。

1. 其他要求

成交人在本项目实施期间应根据本项目实施阶段的国家网络安全等级保护相关要求进行以上工作，因国家网络安全等级保护测评标准变更引起的工作量变更，采购人无需支付额外费用。

1. **文档内容**

根据以上服务需求内容，成交人负责编制的文档应包括但不限于以下文档内容作为产出物：

1. 《网络安全设计方案》
2. 《网络安全等级保护差距分析报告》
3. 《信息系统风险评估报告》
4. 《信息系统渗透测试报告》
5. 《信息系统漏洞扫描报告》
6. 《网络安全等级保护整改建议书》
7. 《等级保护测评报告》
8. 《信息系统安全配置策略符合性检查报告》
9. 《信息系统安全策略自查报告》
10. 《信息系统安全配置应急自查报告》
11. 《肇庆监狱2025年网络安全加固技术方案记录表》
12. 《肇庆监狱2025年网络安全应急演练记录表》
13. 《肇庆监狱2025年网络安全培训记录表》

除上述13个已列明的文档产出物外，成交人应在本项目实施期间根据国家网络安全等级保护相关要求的变化，补充对应的文档产出物，采购人无需支付额外费用。

1. **实施要求**
2. **实施管理要求**
3. 成交人应成立项目管理组织，严格遵守采购人项目管控相关规章制度的要求。在项目实施的各个阶段，按照采购单位相关要求提交文档，并配合其工作。
4. 成交人应基于成熟的项目管理方法论，制订完善的项目管理制度、流程，合理划分项目管理的阶段，借助工程管理工具，在项目实施过程中对项目进行规范化管理，确保项目实施进度和实施质量。
5. 成交人应提供项目管理方案，至少覆盖进度管理、范围管理、风险管理、需求管理、质量管理、资源管理、时间管理、沟通管理等。
6. 成交人应根据项目管理的需要，提供和使用项目管理工具。如采购人要求使用的，必须使用采购人提供的项目管理工具。
7. 成交人提供项目管理工具的，应保证采购人免费使用该管理工具，如涉及版权纠纷，后果由成交人承担。
8. 成交人各阶段产出物采用特殊格式的，成交人需提供相应的打开、编译、运行、修改、打印等工具，并确保采购人无限制的使用；不受版权和知识产权限制，采购人不对工具额外付费。
9. 成交人应认真估算工作量，做好工作量冗余。终验前，成交人须无条件接受并按采购人要求完成各种项目变更，采购人不另行支付费用。
10. 成交人在项目实施过程中所需各种检测工具、项目管理工具等由成交人提供，其结果文档应不依赖于工具而具有可读性，采购人不对此额外付费。
11. **组织人员要求**

成交人负责提出项目实施的项目人员配置方案，主要要求如下：

1. 项目实施由成交人安排项目经理配合项目单位，负责项目管理、项目质量控制、项目进度控制、项目测试验收等工作，安排专职工程师配合负责系统测评，系统测试整改，网络安全应急服务等工作。
2. 成交人应提供至少1人担任项目经理，要求具有信息系统项目管理师证书，同时具备等保三级及以上项目经验，具有集成、实施项目的丰富经验和较强的沟通协调能力；具有预见和应对项目风险能力。自合同签订之日起至该项目相关系统等保测评全部完成前，项目经理需提供5\*8技术支持服务，进行安全建设咨询与指导工作等。
3. 成交人应提供至少1人专职工程师，要求具有信息安全工程师证书（或为CISP注册信息安全专业人员，或为CISAW信息安全保障人员），同时具备等保三级及以上项目经验，具有集成、实施项目的丰富经验和较强的沟通协调能力；自8月12日起，专职工程师需提供7\*24技术支持服务，日常的网络安全应急响应服务，每月不少于3个工作日的现场驻场服务等。
4. 成交人在本项目实施中，应选派工作责任心强、技术水平高、业务熟练、具备等级测评或风险评估实施经验的人员参加本项目的实施。人员总数建议不少于4人，其中测评人员现场不低于2人，且现场人员具有“信息安全等级测评师”或“网络安全等级测评师证书”中级及以上认证证书。
5. 成交人选派的项目组成员应以专职为主，专职人员在项目实施期间不得兼任与本项目无关的其他工作，专职人员比例应不低于 90％。
6. 成交人应在合同签订前提供项目经理与专职工程师名单，同时根据人员要求提供相应的证书或证明文件，在进入系统测评阶段需按要求提供现场测评实施人员名单由采购人确认后，才能进入测评阶段。采购人如认为成交人提供的项目组成员达不到要求，有权要求成交人更换，成交人必须负责在一周之内调换符合采购人要求的项目成员。成交人应按阶段提交项目参与人员名单，经采购人确认。成交人应保证项目组成员的稳定性，如特殊情况需要调整项目组成员的，应提前一个月书面通知采购人，并获得采购人的确认后才能安排调整。
7. 为确保项目顺利实施，项目实施队伍应保持适当的规模，项目组组织结构需分工合理、层次清晰，且分工要为适应项目实施需要。配备人员数量应满足项目需要，原则上每一现场实施人员不得少于1人，不允许职责交叉，不得因为人员离职影响项目的正常开展。
8. 项目经理、专职工程师，测评实施人员应满足项目需要，如果人员不能胜任，采购人有权要求成交人更换人员。成交人原则上不允许更换人员，若更换人员必须书面征得采购人同意，且更换的人员必须具有同等级别和实施经验，并且做好项目交接和资料回收工作；人员搭配应合理，并满足项目实施的要求。
9. **服务质量要求**
10. 成交人是本项目技术服务与质量保障的主要承担者和责任人。成交人必须能依据竞价书中各项需求提供及时、高效的技术保障与服务，协助采购人实现系统的长期稳定运行。技术与质量保障的范围包括本项目所涉及的所有服务。在项目规定的技术服务范围及期限内，不得另行收费。具体服务与质量保障要求如下：
11. 成交人方必须拥有完善的技术保障服务体系，能够为采购人提供统一快捷的技术保障服务。成交人必须向采购人免费提供电话、E-mail 技术支撑等方式。

现场实施过程中，在进行渗透检测或其他安全评估时务必做到对生产系统、业务连续性造成任何负面影响的风险实行规避策略。例如系统、应用异常，产生垃圾数据，数据紊乱等。整改过程中，应提供整改需求说明及整改内容，并协助完成整改。

1. 成交人参与项目的所有人员应严格遵守采购人的保密要求签订保密协议或保密承诺书, 并由成交人担保。成交人对于采购人提供的资料，以及本项目实施过程中所涉及的所有文档、数据、介质和相关信息保密，未经许可，不得以任何形式向第三方传播。保密期限不受本项目期限的限制，在本项目履行完毕后，保密信息接受方仍应承担保密义务。如因成交人一方的原因造成泄密，采购人将保留追究其法律责任的权利。
2. 知识转移的目标是成交人采取有效的方式、途径来保证采购人能顺利的接受本项目产生的各项电子版和纸质版文档交付物以及相关项目成果。在采购时，成交人需详细列出知识转移的方案和方式。成交人要规范和完善项目成果、交付物和中间成果的转交过程。成交人在按计划完成和提交项目成果等交付物的同时，这些文档均要以严格的档案管理规范集中组织并保存，提供电子、纸质等多种备查方式，向采购人相关人员开放项目文档，使得采购人可以随时查阅文档，了解和掌握项目中的各种知识。
3. 采购人对项目实施过程中所产生的所有成果（包括相关技术资料、文档等）享有所有权（永久使用权、复制权和修改权等）。除本项目工作所需外，未经采购人书面同意，成交人不得擅自使用、复制采购人的商标、标志、数据信息、文档及其他资料。
4. 成交人应保证在本项目中所有预装和为本项目安装的软件为在中国境内具有合法版权或使用权的正版软件且无质量瑕疵。成交人应保证其所提供的产品及服务不侵犯第三方的知识产权，否则，由此给采购人造成的一切损失由成交人承担。成交人为本项目提供的产品（设备及软件）均为终身授权产品，使用范围为本项目相关系统且无任何限制。
5. 成交人应对项目所涉及的各阶段工作文档的电子版和纸质版，按采购人质量、数量、提供方式、提供时间等要求进行整理，经采购人确认后提交采购人归档。
6. 在项目实施过程的各阶段，本项目相关技术人员适当参与，以工作中的配合关系和传帮带的工作模式进行知识与技能的转移。在此过程中，成交人须将信息安全等级测评和风险评估方法和经验等通过集中培训和文档提交等形式进行转移。
7. **服务期限要求**

签订合同后需60天内完成合同规定的三级系统通过网络安全等级保护第三级测评，网络安全加固，网络安全应急响应等服务保障时间为2025年8月12日起，服务期限为 12 个月。在本项目服务期内，必须严格按照合同要求完成相关工作，按时提交各阶段文档，协助完成验收工作。

1. **实施方案要求**

成交人必须在项目实施前提交详细的项目实施方案，具体包括技术方案、实施方案、知识转移方案等

1. **验收标准**

完成服务需求中所规定的各项内容，保障本项目所涵盖的网络系统全部通过网络安全等级保护第三级测评，完成一年的网络安全应急响应服务。以上工作完成后，按照采购人要求提交①等保测评报告，②过程文档（《网络安全设计方案》、《网络安全等级保护差距分析报告》、《信息系统风险评估报告》、《信息系统渗透测试报告》、 《信息系统漏洞扫描报告》、《网络安全等级保护整改建议书》、 《信息系统安全配置策略符合性检查报告》、 《信息系统安全策略自查报告》、 《信息系统安全配置应急自查报告》），③公安回执，④每月驻场运维人员考勤表，⑤每月网络安全漏洞修复统计表，⑥肇庆监狱2025年网络安全加固技术方案记录表，⑦肇庆监狱2025年网络安全应急演练记录表，⑧肇庆监狱2025年网络安全培训记录表，进行验收。

1. **合同签订期限**

成交供应商与采购人在本项目结果公告发布之日起15个工作日内签订合同。

1. **付款方式**

本项目计划分3 期支付，具体支付方式和时间如下：

1. 首期款：签订合同后 10 个工作日内，成交人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后启动首期款支付流程，占合同总金额的 30 %。
2. 进度款：合同签订后60天内完成合同规定的三级系统通过网络安全等级保护第三级测评后，成交人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后启动进度款支付流程，占合同总金额的 30 %。
3. 尾款：合同服务期限到期并通过验收后 10 个工作日内，成交人书面提出支付申请函及拟支付金额等额的符合采购人财务管理要求的相应发票，采购人确认后启动尾款支付流程，占合同总金额的 40 %。
4. 项目合同总价包括了服务期间所有服务费用、设备费用、正常的税金、雇员费用、税费、不可预见费等完成本项目内容所需的一切费用及项目实施过程中应预见和不可预见费用等。成交人不得再向采购人收取任何费用。
5. **违约责任与赔偿损失**
6. 成交人在合同签订前未按要求提供相应的项目成员名单，视为成交人违约，采购人有权拒签合同，要求成交人支付合同总价10%违约金，并且给采购人造成的经济损失由成交人承担赔偿责任。
7. 成交人未按合同要求的时间内完成项目清单内容，从逾期之日起每日按本项目合同总价5‰的数额向采购人支付违约金，期10天以上（含10天）的，采购人有权终止合同，要求成交人支付合同总价10%违约金，并且给采购人造成的经济损失由成交人承担赔偿责任。
8. 合同期内采购人和成交人双方无正当理由终止合同的，违约方须向守约方支付合同总额 20%的违约金。如因成交人违约导致合同解除的，成交人应返还采购人已支付的全部合同款项。违约金不足以弥补守约方所受损失的，守约方有权进一步追偿。若采购人解除合同后，成交人须在接到采购人解约通知之日起 10 天内退回采购人已支付合同价款。
9. 合同期内，如成交人出现2次或以上未按合同要求或时间完成服务的，视为成交人严重违约，采购人要求立即解除本项目合同，成交人应返还采购人已支付的全部款项，且采购人有权要求成交人按合同总额20%支付违约金。
10. **争议解决方式**

本项目合同发生争议，由双方协商或由政府采购监督管理部门调解解决，协商或调解不成时向有管辖权的人民法院提起诉讼。（本项目合同的诉讼管辖地为肇庆有管辖权的法院）（在诉讼期间，除有争议部分的事项外，合同其他部分仍应继续履行）。

1. **不可抗力**

任何一方由于不可抗力原因不能履行合同时，应在不可抗力事件结束后1日内向对方通报，以减轻可能给对方造成的损失，在取得有关机构的不可抗力证明或双方谅解确认后，允许延期履行或修订合同，并根据情况可部分或全部免于承担违约责任。

1. **保密**
2. 成交人必须采取措施对本项目合同实施过程中的技术资料保密，否则，由于成交人过错导致的上述资料泄密的，成交人必须承担一切责任。合同内容完成后，甲、乙双方均有责任对本项目合同的技术保密承担责任。
3. 未经采购人事先书面同意，成交人不得将由采购人为本项目合同提供的技术资料提供给与本项目合同无关的任何第三方，不得将其用于履行本项目合同之外的其它用途。即使向与履行本项目合同有关的人员提供，也应注意保密并限于履行合同所必需的范围。
4. 如果采购人有要求，成交人在完成合同后应将有关资料还给采购人。

第三章 报价附件

## 报 价 表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **项目内容** | **内容详情** | **采购人备注** | **报价（元）** | **供应商备注** |
| 1 | 信息系统等级保护测评服务 | 一个三级系统的等保测评 | 一年服务 |  |  |
| 2 | 信息系统等级保护整改优化 | 1. 对测评系统进行渗透测试、漏洞扫描并整优化以满足等保要求 2. 对管理制度审核、建设以满足等保要求 3. 对测评系统差距分析、风险评估并整改优化以满足等保要求 | 一年服务 |  |  |
| 3 | 安全加固服务 | 对全狱终端，服务器，业务系统，安全设备、网络进行漏洞扫描、修复（要求每月现场驻场处置时间不少于3个工作日） | 一年服务 |  |  |
| 4 | 网络安全设备病毒库，特征库升级服务，审计系统授权数升级服务 | 天融信应用安全网关系统（IDP特征库、WEB过滤库、专业版快速扫描查杀防病毒库、应用识别特征库升级服务许可,适用于NU-31116产品(绑SN)） | 一年服务 |  |  |
| 5 | 天融信Web应用安全防护系统（WAF产品特征库升级License,适用于TWF-52116产品(绑SN)） | 一年服务 |  |  |
| 6 | 天融信安全管理系统V3(日志服务器系统），原许可型号TAEX\_S，许可类型396e0c65，升级版本或提供全新版本。 | 永久授权 |  |  |
| 7 | 网络安全应急响应服务 | 1. 网络安全事件应急处置（现场） 2. 节假日提供网络安全检查及运维协助 3. 组织网络安全应急演练一次 | 一年服务 |  |  |
| 8 | 网络安全培训 | 1. 组织本地网络安全知识培训一次（具体培训时间由成交供应商与采购人进行协商确认） 2. 提供不少于2人次CISP(或同等国家认证）线下培训课程服务与考试领证服务 | 一年服务 |  |  |
| **合计（各项报价之和）：人民币 元** | | | | | |

**注：**

1. **供应商必须按报价表的格式填写，不得增加或删除表格内容。除品牌型号、单价、金额或项目要求填写的内容外，不得擅自改动报价表内容，否则将有可能影响成交结果，不推荐为成交候选人；**
2. **所有价格均系用人民币表示，单位为元，均为含税价；**
3. **大写金额和小写金额不一致的，以大写金额为准；单价金额小数点或者百分比有明显错位的，以报价表的总价为准，并修改单价；总价金额与按单价汇总金额不一致的，以单价金额计算结果为准；不接受总价优惠折扣形式的报价，供应商应将对项目的优惠直接在清单报价中体现出来。如果供应商不接受对其错误的更正，其报价将被视为无效报价；**
4. **平台上报价与报价表合计不一致的，以报价表合计（经价格核准后的价格）为准；**
5. **供应商报价表必须加盖公章，否则视作无效报价。**

供应商名称（单位盖公章）：

日期：

## 采购需求书响应声明函

**致：广东省肇庆监狱、采联国际招标采购集团有限公司**

关于贵单位、贵司发布**广东省肇庆监狱2025年网络安全保障服务项目（第二次）**的竞价公告，本公司（企业）愿意参加竞价活动，并作出如下声明：

本公司（企业）承诺在报名时已对于采购需求书中的各项条款、内容及要求给予充分考虑，明确承诺对于本项目的采购需求中的各项条款、内容及要求均为完全响应，不存在任意一条负偏离或不响应的情况。本公司（企业）清楚，若对于采购需求书各项条款存在任意一条负偏离或不响应的情况，不被推荐为成交候选人的要求。

本公司（企业）承诺在本次采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

**备注：**

1. 本声明函必须提供且内容不得擅自删改，否则视为响应无效。
2. 本声明函如有虚假或与事实不符的，作无效报价处理。

供应商名称（单位盖公章）：

日期：

## 供应商资格声明函

**致：广东省肇庆监狱、采联国际招标采购集团有限公司：**

关于贵单位、贵司发布**广东省肇庆监狱2025年网络安全保障服务项目（第二次）**的竞价公告，本公司（企业）愿意参加竞价活动，并作出如下声明：

一、本公司（企业）具备：

（一）具有独立承担民事责任的能力；

（二）具有良好的商业信誉和健全的财务会计制度；

（三）具有履行合同所必需的设备和专业技术能力；

（四）有依法缴纳税收和社会保障资金的良好记录；

（五）本单位（如前三年内有名称变更的，含变更前名称）参加采购活动前三年内，在经营活动中没有重大违法记录（重大违法记录是指因违法经营受到刑事处罚或责令停产停业、吊销许可证或者执照、较大数额罚款等行政处罚）；

（六）法律、行政法规规定的其他条件。

二、本公司（企业）的法定代表人或单位负责人与所参投的本项目其他供应商的法定代表人或单位负责人不为同一人且与其他供应商之间不存在直接控股、管理关系。

三、本公司（企业）在本项目中不转包分包且不联合竞价。

本公司（企业）承诺在本次采购活动中，如有违法、违规、弄虚作假行为，所造成的损失、不良后果及法律责任，一律由我公司（企业）承担。

特此声明！

**备注：**

1. 本声明函必须提供且内容不得擅自删改，否则视为响应无效。
2. 本声明函如有虚假或与事实不符的，作无效报价处理。

供应商名称（单位盖公章）：

日期：