2020年省戒毒局机关网络安全项目

竞争性磋商文件

项目编号：440000-202009-202001-0041

采　购　人：广东省戒毒管理局

采购代理机构：广东志正招标有限公司

2020年9月

温馨提示：供应商特别注意事项

一、 请供应商特别留意磋商文件上注明的首次响应文件提交截止时间，逾期送达的响应文件我司恕不接收。因此，请供应商适当提前到达会议室。**提交首次响应文件开始时间为响应文件提交截止时间前半小时。**

二、 磋商保证金用于保护本次磋商免受供应商的行为而引起的风险，为本次磋商的必要组成部分，建议供应商仔细阅读磋商文件中关于磋商保证金的描述。磋商保证金必须于**响应文件递交截止时间前到达账户**，以到达指定账户时间为准。因转账当天不一定能够达账，为避免因磋商保证金未达账而导致响应文件被拒绝，建议提前转账。以银行保函或《政府采购磋商担保函》形式交纳磋商保证金的，《银行保函》或《政府采购磋商担保函》复印件（加盖公章）放入响应文件的商务部分中，原件放入“保证金”信封中。

三、 请正确填写《首次报价一览表》，如含有包组的磋商项目需分开报价，报价要求详见磋商文件《首次报价一览表》。

四、 请仔细检查《资格声明函》、《报价函》、《法定代表人证明书》、《法定代表人授权书》、《首次报价一览表》、《首次报价详细报价表》、《实质性响应一览表》、《报价响应与磋商文件差异一览表》、等重要格式文件是否有按要求盖公章或签名或印鉴。

五、 建议将响应文件按目录格式顺序编制页码。

六、 分公司作为响应供应商参与磋商的，需提供具有法人资格的总公司的营业执照副本复印件及授权书。总公司可就本项目或此类项目在一定范围或时间内出具唯一的磋商授权书。法律法规或者行业另有规定的除外。

七、 **供应商请注意区分磋商保证金及采购代理服务费收款账号的区别**，务必将保证金按磋商文件的要求存入指定的保证金专用账户，采购代理服务费存入成交通知书中指定的服务费账户。切勿将款项转错账户，以免影响保证金缴纳、退还的时效。

（本提示内容非磋商文件的组成部分，仅为善意提醒。如有不一致，以磋商文件为准。）

附我司地图：


中公教育大厦
天工大厦
广东技术师范
大学(西校区)
广园快速路
农机物资
公司综合楼
龙怡路
银汇大厦
广州建设工程
交易中心
天润路
天诚广场
五山路
五山路口站
光大银行
华标广场
曜一城
天河北路
华师
E出口
华师
B出口
瑞安创逸写字楼
保利中宇广场
华师
师大后门站
天河区司法局
尚德大厦
广州市第一一三
中学(五山校区)
龙威商务大厦

目 录

竞争性磋商公告

2020年省戒毒局机关网络安全项目采购项目的潜在供应商应在广州市天河区龙怡路117号银汇大厦5楼或通过链接http://www.zztender.com/获取采购文件，并于2020年10月15日9点30分（北京时间）前提交申请文件。

一、项目基本情况

项目编号：440000-202009-202001-0041

项目名称：2020年省戒毒局机关网络安全项目

采购方式：竞争性磋商

预算金额：¥1,517,000.00

最高限价（如有）：¥1,517,000.00

采购需求：（包括但不限于标的的名称、数量、简要技术需求或服务要求等）

1、 标的名称：省戒毒局机关网络安全

2、 标的数量：一项

3、 简要技术需求或服务要求：2020年省戒毒局机关网络安全项目

4、 其他：/

合同履行期限：2年

本项目不接受联合体磋商。

二、申请人的资格要求：

1.满足《中华人民共和国政府采购法》第二十二条规定；

2.落实政府采购政策需满足的资格要求： 无

3.本项目的特定资格要求：

（1） 应具备《中华人民共和国政府采购法》第二十二条规定的条件，提供以下材料：

1）提供最新的供应商营业执照（或事业单位法人证书，或社会团体法人登记证书，或执业许可证）副本复印件；如供应商为自然人的需提供自然人身份证明；如国家另有规定的，则从其规定。若以不具有独立承担民事责任能力的分支机构磋商，须取得具有法人资格的总公司的授权书，并提供总公司营业执照副本复印件。

2)供应商应当具有良好的商业信誉和健全的财务会计制度,提供以下证明之一:①提供2018年年度（或2019年年度）年度审计报告或企业所得税年度汇算清缴报告（适用于在上一年度前成立的法人或其他组织）；② 2020年任一季度或任一月的财务报表，内容含盖资产负债表和利润表和现金流量表（适用在上一年度或本财务年度成立的法人或其他组织）；③基本户开户银行出具的资信证明，并提供开户许可证（适用于法人或其他组织）； ④中国人民银行出具的个人

信用报告（适用于自然人）。

3）具有履行合同所必需的设备和专业技术能力，提供资格声明函；

4）提供 2019 年（或 2020 年）任意一个月的依法缴纳税收的证明（如纳税凭证）复印件，如依法免税的，应提供相应文件证明其依法免税；（其中税种不能为社会保险基金）；供应商成立不满三个月的，可不提供缴纳税收的证明。

5）提供 2019 年（或 2020 年）任意一个月的依法缴纳社会保险的证明（如缴费凭证）复印件，如依法不需要缴纳社会保障资金的，应提供相应文件证明其依法不需要缴纳社会保障资金；供应商成立不满三个月的，可不提供缴纳社会保险的证明。

6）参加政府采购活动前三年内，在经营活动中没有重大违法记录，提供资格声明函；

（2） 未列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单的供应商（以提交首次响应文件当日采购代理机构在“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）的查询结果为准；处罚期限届满的除外。如“信用中国”网站查询结果显示“没有找到您搜索的企业”或“没有找到您搜索数据”，视为没有上述三类不良信用记录）。

（3） 不得参与同一采购项目竞争的供应商（提供资格声明函）

1）单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一包组磋商或者未划分包组的同一采购项目的政府采购活动。如同时参加，则评审时均作无效处理。

2）为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目的其他采购活动。

（4） 本项目不接受联合体参与磋商。

三、获取采购文件

时间：2020 年 9 月 28 日至 2020 年 10 月 12 日（*磋商文件的发售期限自开始之日起不得少于 5 个工作日*），每天上午 9:00 至 12:00，下午 14:30 至 17:30（北京时间，法定节假日除外 ）

地点：广州市天河区龙怡路 117 号银汇大厦 5 楼或通过链接 http://www.zztender.com/

方式：**现场领购或线上购买，售后不退。**线上购买采购文件的供应商，请于**上述“获取采购文件”中载明的期限前**登录广东志正招标有限公司官网“http://www.zztender.com/”中的“购买标书”入口进行线上操作并完成交费，详见官网“线上售标操作指引”。采购代理机构将按供应商提供的信息，发送电子采购文件并邮寄纸质采购文件。建议供应商选择线上购买方式，线上购买需另加邮购费人民币 60 元。（咨询电话 020-87554018，邓小姐）

售价（元）：300

四、响应文件提交

截止时间：2020 年 10 月 15 日 9 点 30 分（北京时间）*（从磋商文件开始发出之日起至供应商提交首次响应文件截止之日止不得少于 10 日；从谈判文件开始发出之日起至供应商提交首次响应文件截止之日止不得少于 3 个工作日；从询价通知书开始发出之日起至供应商提交响应文件截止之日止不得少于 3 个工作日）*

地点：广州市天河区龙怡路 117 号银汇大厦 5 楼广东志正招标有限公司会议室

五、开启（竞争性磋商方式必须填写）

时间： 2020 年 10 月 15 日 9 点 30 分（北京时间）

地点：广州市天河区龙怡路 117 号银汇大厦 5 楼广东志正招标有限公司会议室

六、公告期限

自本公告发布之日起 3 个工作日。

七、其他补充事宜

a) 本项目将优先确定符合相应资格条件的自主创新产品、节能产品、环保产品供应商参加磋商。

b) 服务详细内容、要求及执行标准：详见“用户需求”部分。

c) 需要落实的政府采购政策:《政府采购促进中小企业发展暂行办法》(财库[2011]181 号)、《关于政府采购支持监狱企业发展有关问题的通知》(财库[2014]68 号)、《三部门联合发布关于促进残疾人就业政府采购政策的通知》(财库〔2017〕141 号)、《关于环境标志产品政府采购实施的意见》(财库〔2006〕90 号、《节能产品政府采购实施意见》的通知（财库〔2004〕185 号)、《财政部 发展改革委 生态环境部 市场监管总局 关于调整优化节能产品、环境标志产品政府采购执行机制的通知》(财库〔2019〕9 号）等。

d) 本项目采购本国产品/服务。

e) 本项目属于政府采购项目。

f) 监管部门：广东省财政厅政府采购监管处。

g) 内部纪律监督电话：020-87554258

八、凡对本次采购提出询问，请按以下方式联系。

1.采购人信息

名称：广东省戒毒管理局

地址：广州市越秀区黄华路 4-1 号

联系方式： 020-83873705

2.采购代理机构信息

名称：广东志正招标有限公司

地址：广东省广州市天河区龙怡路 117 号 501、503、504、505、506 房

联系方式：020-87554018　87554038

3.项目联系方式

项目联系人：林小姐

电话：020- 87554038

发布人：广东志正招标有限公司

发布时间：2020 年 9 月 27 日

第一部分 磋商须知

磋商须知前附表

序号	项目	内容
1	采购人名称	广东省戒毒管理局。
2	最高限价及资金来源	★本项目最高限价：★预算金额：人民币 151.7 万元； 资金来源：财政性资金。
3	答疑及踏勘现场等	本项目不举行集中答疑会。 本项目不举行现场考察。
4	★磋商有效期	自提交首次响应文件截止之日起 90 日。
5	磋商保证金	**★金额小写：10000 元整** ★提交形式：支票、汇票、本票或金融机构、担保机构出具的保函、网上银行转账等非现金形式。磋商保证金与磋商响应文件一同递交，必须于**响应文件递交截止时间前**到达指定账户，以到达指定账户的时间为准。
		保证金账号： 收款单位：广东志正招标有限公司； 开户银行：广州银行龙口西支行； 账号：800201177509011； 保证金相关事宜联系人：郑小姐 联系电话：020-87554268； 网上银行转账的，请各供应商将磋商保证金存进以上广东志正招标有限公司指定银行账户，并在提交磋商响应文件时，提交银行电子回单加盖单位公章，同时在银行转账单据上标注项目编号：440000-202009-202001-0041 。 以《银行保函》或《政府采购磋商担保函》形式交纳保证金的，《银行保函》/《政府采购磋商担保函》复印件（加盖公章）放入响应文件的商务部分中，原件放入“磋商保证金”信封中。
6	响应文件份数	正本壹份、副本叁份和不作任何加密的电子标书壹份。
		正本和电子标书一起封装，副本一起封装，建议封套盖章并标明项目名称、项目编号、供应商名称及“正本”、“副本”等字样。 保证金退还说明（原件）、保证金银行转账电子回单/《银行保函》**(原件)**/《政府采购磋商担保函》**(原件)**一起封装，封套标明项目编号、供应商名称及“磋商保证金”等字样。
7	演示与述标	无。
8	样品要求	无。
9	磋商小组组成	本项目评审工作由依法组建的磋商小组负责完成，磋商小组由 3 人组成。

10	评审方法	经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分。 综合评分法，是指响应文件满足磋商文件全部实质性要求且按评审因素的量化指标评审得分最高的供应商为成交候选供应商的评审方法。
11	成交候选人的推荐	磋商小组根据综合评分情况，编写书面的评审报告，按综合得分高低次序排出名次，并推荐综合得分排名第一的供应商为第一成交候选人，排名第二的供应商为第二成交候选人，排名第三的供应商为第三成交候选人。 综合得分相同的，按照最后报价由低到高的顺序推荐。综合得分且最后报价相同的，按照技术指标优劣顺序推荐。综合得分相同、评审价和技术评分均相同的，名次由磋商小组抽签确定。法律法规有明确规定的，以法律法规规定为准。
12	采购代理服务费	成交供应商按以下标准和规定向采购代理机构缴纳采购代理服务费： （1）以项目成交总金额作为采购代理服务费的计算基数； （2）采购代理服务费采用差额定率累进法进行计算，按照以下标准计取： 100万元以下的部分，按照1.5%计取； 100-500万元的部分，按照0.8%计取； 500-1000万元的部分，按照 0.45%计取； 1000-5000万元的部分，按照 0.25%计取。
		采购代理服务费由供应商支付的，成交供应商应在《付款通知书》发出五个工作日内一次性将采购代理服务费存入采购代理机构指定账户，凭已盖银行收款章的进账单、成交供应商开具的介绍信及身份证原件到采购代理机构领取《成交通知书》。 收款单位：广东志正招标有限公司 开户银行：中国光大银行广州分行 银行账号：083861120100304174807（交纳采购代理服务费账号，非保证金专用账户） 注明项目编号。
13	履约保证金	合同金额的 5%
14	供应商信用	采购代理机构在磋商当日通过“信用中国”网站（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）查询供应商信用记录。 对列入失信被执行人、重大税收违法案件当事人名单、政府采购严重违法失信行为记录名单及其他不符合《中华人民共和国政府采购法》第二十二条规定条件的供应商，拒绝其参与政府采购活动。（处罚期限届满的除外，如“信用中国”网站查询结果显示“没有找到您搜索的企业”或“没有找到您搜索数据”，视为没有上述三类不良信用记录） 采购代理机构将信用信息查询记录和证据打印留存，信用信息查询记录及相关证据与其他采购文件一并保存。
15	★其他	**本项目不接受备选方案，不接受有任何选择或具有附加条件的报价，磋商响应文件的报价只允许唯一方案报价。否则，磋商小组将对其作无效处理。**

16	新型冠状病毒感染肺炎疫情防控期间的便利化措施**（本采购文件其他条款与本条不一致的，以本条为准）**	**响应文件的递交与开标** 1. 疫情防控期间，各响应供应商可以通过“中国邮政”、“EMS”、“顺丰快递”等快递方式，按照采购文件要求在规定的响应截止时间前将《响应文件》及相关样品（如有）送达到开标地点，快递单上应清晰写明如下信息： 1）收件地址：广州市天河区龙怡路 117 号银汇大厦 5 楼 2）收件人：广东志正招标有限公司前台 3）注明采购项目编号 如需现场安装或调试的样品，不接受邮寄送达的方式。 需现场陈述的项目，请供应商派代表参与。 2. 通过快递方式递交《响应文件》及相关样品（如有）的，递交时间为送达我司由我司前台人员签收的时间，请响应供应商预留邮寄所需的时间。建议响应供应商在邮递之后，主动在响应截止时间前及时与我司联系，核实响应文件是否在规定的时间内送达。 3. 通过快递方式递交《响应文件》及相关样品（如有）的，寄错地址、逾期送达、未按照采购文件要求密封或者邮寄过程导致包装密封出现破损的，我司将拒绝接收，由响应供应商自行承担相应责任与后果，我司不承担责任。 4. 响应供应商未参加现场开标的，视同认可开标结果。 **中标（成交）通知书与发票送达** 疫情防控期间，我司暂停中标（成交）通知书、服务费（标书款）发票现场领取，中标（成交）通知书、我司将通过快递方式送达给中标（成交）人，服务费（标书款）发票以邮件方式发送电子发票。 **采购合同送达** 疫情防控期间，我司提倡中标（成交）人优先采用邮寄方式将签订的合同及时送达我司。 1）收件地址：广州市天河区龙怡路 117 号银汇大厦 5 楼 2）收件人：广东志正招标有限公司前台 3）注明采购项目编号

供应商必须认真阅读以下内容，以免造成响应失败。

（一）总　则

1. 适用范围

1.1 依据《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《政府采购非招标采购方式管理办法》、《政府采购竞争性磋商采购方式管理暂行办法》及广东省政府采购有关规定制定本须知。

1.2 本项目的采购人、采购代理机构、供应商及各方当事人适用本须知。

2. 项目说明

2.1 资金性质、资金来源，详见磋商须知前附表第2项。

2.2 最高限价，详见磋商须知前附表第2项。

2.3 磋商内容

（详细内容请参阅磋商文件中的相关内容）

3. 概念释义

3.1 监管部门：指同级或以上人民政府财政部门。

3.2 采购人：指依法进行政府采购的国家机关、事业单位和团体组织，详见磋商须知前附表第1项。在采购阶段称为采购人，在合同阶段称为甲方或买方。为便于磋商文件及附件直接转化为合同条款，在磋商文件中有时称采购人为买方、甲方或业主。

3.3 采购代理机构：依法设立、从事采购代理业务并提供相关服务的社会中介组织-广东志正招标有限公司。

3.4 磋商小组：磋商小组是依法组建专门负责本次评审工作的临时性机构。

3.5 响应供应商：符合资格要求，响应磋商、参加磋商竞争的依法成立的法人或其他组织。

3.6 成交供应商：经合法磋商程序评选出来并经采购人确认的获得本项目成交资格的供应商。

3.7 日期：指公历日。

3.8 时间：指北京时间。

4. 合格的供应商

4.1 ★对供应商的要求：**详见竞争性磋商公告中“供应商资格”部分。**

4.2 ★供应商需由法定代表人（负责人）或其委托代理人（具有法定代表人签署的授权书）**携带身份证明原件**参加磋商，在评审过程中随时接受磋商小组就响应文件的内容提出的质询，并予以解答。

5. 合格的货物和服务

5.1 供应商提供的所有货物和服务，必须是合法生产、合法来源，符合国家有关标准要求，并满足磋商文件规定的规格、参数、质量、价格、有效期、售后服务及供应商须承担的运输、安装、技术支持、培训和磋商文件规定的其它伴随服务等要求。

5.2 采购人有权拒绝接受任何不合格的货物和服务，由此产生的费用及相关后果均由供应商自

行承担。

5.3 政府采购若需采购进口产品的，依据《政府采购进口产品管理办法》执行。

5.4 进口产品是指通过中国海关报关验放进入中国境内且产自关境外的产品。

6. 磋商文件中，凡标有“★”的地方，供应商要特别加以注意，必须对此作出一一响应。若有一项带“★”的指标未响应或不满足，将对其响应文件作无效处理。（注：若磋商小组在磋商过程中对磋商文件作出了实质性变动，本条中的磋商文件指变动后的磋商文件）

7. 关于分支机构

7.1 分公司作为响应供应商的，需提供具有法人资格的总公司的营业执照副本复印件及授权书。总公司可就本项目或此类项目在一定范围或时间内出具唯一的磋商授权书。已由总公司授权的，总公司取得的相关资质证书对分公司有效，但总公司及总公司下属其他分公司的人员及业绩不作为响应供应商的人员或业绩；若磋商文件另有详细规定的遵从其规定。

7.2 总公司作为供应商参与，但授权分公司进行磋商活动的，需由总公司对分公司出具唯一的授权授章书进行磋商。

7.3 法律法规或者行业另有规定的，法人的分支机构参与磋商不受前两款的约束。

8. 关于联合体磋商

若竞争性磋商公告允许联合体磋商的，则必须满足：

8.1 两个以上供应商可以组成一个联合体参与磋商，以一个供应商的身份参与。

8.2 联合体各方均应当符合《政府采购法》第二十二条第一款规定的条件，根据采购项目的特殊要求规定供应商特定条件的，联合体各方中至少应有一方符合采购人规定的特定条件。

8.3 联合体磋商的，必须提供各方签订的共同磋商协议，明确约定各方承担的工作和相应的责任。联合体各方签订共同磋商协议后，不得再以自己名义单独在同一项目中磋商，也不得组成新的联合体参加同一项目磋商；

8.4 联合体磋商的，可以由联合体中的一方或者共同提交磋商保证金，以一方名义提交磋商保证金的，对联合体各方均具有约束力。

8.5 联合体获得成交资格的，联合体各方应当共同与采购人签订合同。

8.6 同一专业的单位组成的联合体，按照同一项资质等级较低的单位确定资质等级。

8.7 两个以上的自然人、法人或者其他组织组成一个联合体，以一个供应商的身份共同参加政府采购活动的，采购人或者采购代理机构对所有联合体成员进行信用记录查询，联合体成员存在不良信用记录的，视同联合体存在不良信用记录。

9. 不得参与同一采购项目竞争的供应商

单位负责人为同一人或者存在直接控股、管理关系的不同供应商，不得参加同一包组投标或者未划分包组的同一招标项目的政府采购活动。如同时参加，则评审时均作无效投标处理。

为采购项目提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再

参加该采购项目的其他采购活动。

10. 关于中型、小型、微型企业参与磋商

10.1 根据财政部、工业和信息化部印发的《政府采购促进中小企业发展暂行办法》（财库[2011]181 号）的规定，对小型和微型企业产品的价格给予 6%-10%的扣除，用扣除后的价格参与评审；报价产品中仅有部分小型和微型企业产品的，则按所报小型和微型企业产品的价格予以扣除。

10.2 《政府采购促进中小企业发展暂行办法》所称中小企业（含中型、小型、微型企业，下同）应当同时符合以下条件：

（1） 符合中小企业划分标准；

（2） 提供本企业制造的货物、承担的工程或者服务，或者提供其他中小企业制造的货物。本项所称货物不包括使用大型企业注册商标的货物。

10.3 《政府采购促进中小企业发展暂行办法》所称中小企业划分标准，是指国务院有关部门根据企业从业人员、营业收入、资产总额等指标制定的中小企业划型标准。

10.4 小型、微型企业提供中型企业制造的货物的，视同为中型企业。

10.5 中小微企业参与磋商应提供《中小微企业声明函》。根据财库〔2014〕68 号《财政部 司法部关于政府采购支持监狱企业发展有关问题的通知》，监狱企业视同小微企业。监狱企业是指由司法部认定的为罪犯、戒毒人员提供生产项目和劳动对象，且全部产权属于司法部监狱管理局、戒毒管理局、直属煤矿管理局，各省、自治区、直辖市监狱管理局、戒毒管理局，各地(设区的市)监狱、强制隔离戒毒所、戒毒康复所，以及新疆生产建设兵团监狱管理局、戒毒管理局的企业。监狱企业参与磋商提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件，不再提供《中小微企业声明函》。

10.6 根据财库〔2017〕141 号《三部门联合发布关于促进残疾人就业政府采购政策的通知》，符合条件的残疾人福利性单位在参加政府采购活动时，应当提供《残疾人福利性单位声明函》，并对声明的真实性负责。残疾人福利性单位视同小型、微型企业，享受评审中价格扣除的政府采购政策。成交供应商为残疾人福利性单位的，采购人或者其委托的采购代理机构应当随成交结果同时公告其《残疾人福利性单位声明函》，接受社会监督。

11. 关于节能产品、环境标志产品

国家行业主管部门对政府采购节能产品、环境标志产品实施品目清单管理。

12. 磋商文件的解释权

本磋商文件的解释权归“广东志正招标有限公司”所有。

（二）磋商文件

13. 磋商文件构成

要求提供的服务、磋商过程和合同条件在磋商文件中均有说明。磋商文件包括：

- 竞争性磋商公告；
- 磋商须知；
- 用户需求；
- 合同草案；
- 响应文件格式；
- 磋商过程中发生的澄清、修改和补充文件（如有）。

14. 供应商应认真阅读、并充分理解磋商文件的全部内容（包括所有的补充、修改内容、重要事项、格式、条款和技术规范、参数及要求等）。供应商没有按照磋商文件要求提交全部资料，或者响应文件没有对磋商文件在各方面都作出实质性响应是供应商的风险，有可能导致其磋商响应被拒绝，或被确定为响应无效。

15. 磋商文件的澄清和修改

15.1 提交首次响应文件截止之日前，采购人、采购代理机构可以对已发出的磋商文件进行必要的澄清或者修改，澄清或者修改的内容作为磋商文件的组成部分。澄清或者修改的内容可能影响响应文件编制的，采购人、采购代理机构应当在提交首次响应文件截止时间至少 5 日前，以书面形式通知所有获取磋商文件的供应商；不足 5 日的，采购人、采购代理机构应当顺延提交首次响应文件截止时间。潜在供应商在收到上述通知后，应立即以书面形式向采购代理机构确认。如在 24 小时之内无书面回复则视为同意澄清或者修改的内容，并有责任履行相应的义务。

15.2 对磋商文件中描述有歧义或前后不一致的地方，磋商小组有权进行评判，但对同一条款的评判应适用于每个供应商。

16. 答疑会或现场考察

详见磋商须知前附表第 3 项。

（三）响应文件的编制

17. 响应文件的构成

供应商编写的响应文件应包括资格证明文件、商务文件和技术文件，编排顺序参见响应文件格式。资格证明文件、商务文件部分指供应商提交的证明其有资格参加磋商和成交后有能力履行合同的文件。技术方案说明部分是能够证明供应商提供的货物及服务符合磋商文件规定的文件。供应商应按规定提交资格证明文件、商务文件部分和技术文件。

18. 磋商费用

供应商应承担所有与编写和提交响应文件有关的费用，不论磋商的结果如何，采购代理机构、采购人在任何情况下均无义务和责任承担这些费用。

19. 报价函

供应商应完整地填写磋商文件格式中规定的报价函。

20. 报价说明

20.1 供应商应以人民币报价。

20.2 供应商应按磋商文件格式要求填写报价明细表。

20.3 供应商所报的价格在合同执行期间是固定不变的，不得以任何理由予以变更。报价不是固定价的，将作为非响应性报价而予以拒绝。

20.4 供应商所报的最后价格应为所投项目的最终报价，包含一切税费；供应商应自行增加正常运行及使用所必需但磋商文件没有包含的所有部件、工具、版权、专利等一切费用，如果供应商在成交并签署合同后，在项目实施等工作中出现任何遗漏，均由成交供应商提供，买方将不再支付任何费用。

21. 响应文件的编写原则

21.1 磋商语言：响应文件、供应商与采购代理机构就磋商交换的文件和来往信件，应以中文书写。供应商提供的支持文件、技术资料和印刷的文献可以用其他语言，但相应实质性内容须附有中文翻译本，并以中文为准。

21.2 计量单位：除在磋商文件的技术规格中另有规定外，计量单位应使用中华人民共和国法定计量单位(国际单位制和国家选定的其他计量单位)。

21.3 供应商应保证所提供的所有资料的真实性、准确性、完整性。

21.4 供应商应当对响应文件进行装订，对未经装订的响应文件可能发生的文件散落或缺损，由此造成的后果和责任由供应商承担。若项目含有多个包组，且供应商参与对多个包组磋商的，建议其响应文件的编制按每个包组的要求分别装订和封装。

21.5 供应商在采购过程中提供不真实的材料，无论其材料是否重要，采购人均有权拒绝，并取消供应商的成交资格，供应商需承担相应的后果及法律责任。

21.6 本项目概不接受电报、电话、电子邮件或传真形式提交的响应文件。

22. 证明供应商合格的资格文件

22.1 供应商应提交证明其有资格参加磋商和被确定为成交供应商后有能力履行合同的文件，以及证明其提供的合同项下，服务的合格性符合磋商文件规定的文件，并作为响应文件的一部分。如果供应商为联合体，应提交联合体各方的资格证明文件、共同磋商协议并注明主体方及各方拟承担的工作和责任。否则，将导致其磋商响应无效。

23. 关于保证金

23.1 保证金为响应文件的组成部分，应在有关单据上注明项目编号。

23.2 保证金用于保护本次磋商免受供应商的行为而引起的风险。

23.3 供应商须按磋商文件中的磋商须知前附表第 5 项规定向采购代理机构交纳保证金。

23.4 磋商保证金以支票、汇票、本票或金融机构、担保机构出具的保函、网上银行转账等非现金形式提交。

23.5 以银行转账方式提交的，请供应商按磋商须知前附表第 5 项将磋商保证金存进广东志正招

标有限公司指定账户。

24.5.1 采用银行保函提交的：

① 采用磋商文件提供的格式或采购人接受的其他格式；

② 由中华人民共和国境内的银行出具的银行保函；

③ 有效期超过磋商有效期 30 天。

24.5.2 采用政府采购磋商担保函提交的：

① 采用磋商文件提供的格式或采购人接受的其他格式；

② 由专业担保机构出具的政府采购磋商担保函；

③ 有效期超过磋商有效期 30 天。

24.5.3 以银行保函（或《政府采购磋商担保函》）形式交纳保证金的，银行保函（或《政府采购磋商担保函》）复印件（加盖公章）放入响应文件的商务部分中，原件放入“保证金”信封中。

23.6 未按规定提交保证金或《政府采购磋商担保函》的响应文件，将被视为无效文件。

23.7 未成交的供应商的保证金，在该采购项目的结果通知书发出后按《保证金退还说明》的要求在五个工作日内无息全额退回。

23.8 成交供应商的保证金，在成交供应商与采购人签订采购合同并将合同原件交采购代理机构备案后按《保证金退还说明》的要求在五个工作日内无息全额退回。

23.9 在下列情况下保证金将不予退还：

① 供应商在提交响应文件截止时间后撤回响应文件的；

② 供应商在响应文件中提供虚假材料的；

③ 除因不可抗力或磋商文件认可的情形以外，成交供应商不与采购人签订合同的；

④ 供应商与采购人、其他供应商或者采购代理机构恶意串通的；

⑤ 法律法规规定的其他情形。

24. 磋商有效期

24.1 **响应文件在磋商须知前附表第 4 项规定的磋商有效期内有效。磋商有效期比规定期限短的将被视为无效响应文件。**

24.2 特殊情况下，在原磋商有效期截止之前，采购代理机构可要求供应商延长磋商有效期。这种要求与答复均应以书面形式提交。供应商可拒绝政府采购代理机构的这种要求，其磋商保证金将被无息退还，但其磋商在原磋商有效期期满后将不再有效。同意延长磋商有效期的供应商将不会被要求和允许修正其磋商，而只会被要求相应地延长其磋商保证金的有效期。在这种情况下，本须知有关磋商保证金的退还和不予退还的规定将在延长了的有效期内继续有效。

25. 响应文件的式样和签署

25.1 供应商应按磋商须知前附表第 6 项准备响应文件正本、副本和电子文档标书（刻录光盘或

U盘），电子标书的文件格式要求用MS WORD/EXCEL简体中文版，电子标书封面注明响应供应商名称和项目编号，每份响应文件须清楚地标明“正本”或“副本”。一旦正本和副本不符，以正本为准。

25.2 供应商应将按照响应文件格式的目录要求顺序装订成册。响应文件应装订牢固不可拆卸（如：胶订），如因装订不牢固导致的任何损失由供应商承担。

25.3 响应文件除签字或印鉴外必须是印刷形式，一般不许有加行、涂抹或改写；如有加行、涂抹或改写，必须由供应商法定代表人或其授权代表在修改处签名或印鉴或加盖供应商公章。

25.4 响应文件正本须打印并由供应商的法定代表人或其委托代理人（具有法定代表人签署的授权书）在响应文件上要求的地方签字或印鉴，副本可通过正本复印。

（四）响应文件的提交

26. 响应文件的标记

26.1 正本和电子响应文件一起封装，副本一起封装，封套盖章并标明项目名称、项目编号、供应商名称及“正本/副本”等字样。

26.2 保证金退还说明（原件）、保证金银行转账电子回单/保证金担保函原件一起封装，封套标明项目编号、供应商名称及“磋商保证金”等字样。

26.3 封套上应注明：

收件人：广东志正招标有限公司

项目名称：

项目编号:

供应商名称：

供应商地址：

在规定响应文件提交截止时间之前不得启封

26.4 **如因密封不严导致投标文件非人为因素过早启封的，采购代理机构概不负责，并将该文件退还给投标人。**

26.5 逾期送达或者未密封的响应文件，采购人、采购代理机构应当拒收。密封有瑕疵，但不足以造成响应文件可从外包装内散出而导致响应文件内容泄密的，不被认定为未密封。

27. 迟交的响应文件

27.1 **采购代理机构将拒绝并原封退回在其规定的响应文件提交截止时间后收到的任何响应文件。**

27.2 如果推迟响应文件提交截止时间，采购代理机构、采购人和供应商受响应文件提交截止时间制约的所有权利和义务均应相应延长至新的截止时间。

28. 响应文件的修改和撤回

供应商在响应文件提交截止期前，可以对所提交的响应文件进行补充、修改或者撤回，并书

面通知采购代理机构。补充、修改的内容应当按磋商文件要求签署、盖章，并作为响应文件的组成部分。

（五）关于评审

29. 磋商小组

29.1 本次磋商按照磋商须知前附表第 9 项规定依法组建磋商小组，（达到公开招标数额的项目磋商小组成员为五人以上单数）。

29.2 磋商小组所有成员集中对响应文件进行审查，与每个供应商分别进行先商务技术条件后价格的磋商，本次磋商采用一轮磋商，两次报价形式进行。磋商小组也可视实际情况确定磋商轮次及报价次数，并提交评审报告及推荐成交供应商。

29.3 磋商小组名单在磋商结果确定前严格保密。磋商专家（不含采购人代表）有下列情形之一的，受到邀请应主动提出回避，采购当事人也可以要求该磋商专家回避：

① 本人、配偶或直系亲属 3 年内曾在参加该采购项目的供应商中任职（包括一般工作）或担任顾问、董事、监事或与参加该采购项目的供应商发生过法律纠纷；

② 参加采购活动前 3 年内是供应商的控股股东或者实际控制人；

③ 与供应商的法定代表人或者负责人有夫妻、直系血亲、三代以内旁系血亲或者近姻亲关系；

④ 任职单位与采购人或参加该采购项目供应商存在行政隶属关系；

⑤ 曾经参加过该采购项目的进口产品或磋商文件、采购需求、采购方式的论证和咨询服务工作；

⑥ 为参加该采购项目供应商的上级主管部门、控股或参股单位的工作人员，或与该供应商存在其他经济利益关系；

⑦ 磋商小组成员之间具有配偶、近亲属关系；

⑧ 法律、法规、规章规定应当回避以及其他可能影响公正评审的。

30. 磋商的原则

30.1 磋商小组将依据采购的有关规定，遵循“公开、公平、公正、科学、择优”的原则进行磋商和评审工作。磋商小组将按照规定只对通过资格、符合性评审的响应文件进行最终评审和比较。如各评委结论不一致时，磋商小组的结论以少数服从多数原则确定。

30.2 在磋商中，磋商的任何一方不得透露与磋商有关的其他供应商的技术资料、价格和其他信息。磋商小组和参与磋商的有关工作人员不得透露对响应文件的评审和比较以及与磋商有关的其他情况。

30.3 对磋商文件中描述有歧义或前后不一致的地方，磋商小组有权进行评判，但对同一条款的评判应适用于每个供应商。

31. 响应文件差异修正准则

响应文件出现差异时，磋商小组按以下修正原则及顺序对响应文件的差异进行修正：

① 报价一览表与分项明细表或其它相关报价表报价不一致的，均以报价一览表为准；

② 大写金额和小写金额不一致的，以大写金额为准；

③ 分项报价表中的单价与对应的合计价不相符的，以单价为准，修正对应的该项合计价；

④ 单价金额小数点有明显错位的，应以总价为准，并修改单价；

⑤ 响应文件描述内容与原始材料引述内容不一致的，以原始材料内容为准；

⑥ 对不同文字文本响应文件的解释发生异议的，以中文文本为准；

⑦ 对出现以上情况或因明显笔误而需修正任何内容时，均以磋商小组审定通过方为有效；

⑧ 对采购项目的关键、主要内容，报价供应商报价漏项的，作非实质性响应处理；

⑨ 磋商小组认定为表述不清晰或无法确定的报价均不予修正。

32. 响应文件的澄清

32.1 对响应文件中含义不明确、同类问题表述不一致或者有明显文字和计算错误的内容，磋商小组可以书面形式要求供应商作出必要的澄清、说明或者纠正。

32.2 供应商的澄清、说明或者补正应当采用书面形式，并不得超出响应文件的范围或者改变响应文件的实质性内容。供应商的澄清、说明或者更正应当由法定代表人或其授权代表签字或印鉴或者加盖公章。由授权代表签字或印鉴的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字或印鉴并附身份证明。

32.3 磋商小组均应当阅读供应商的澄清，但应独立参考澄清对响应文件进行评审，整个澄清的过程不得存在排斥供应商的现象。

32.4 除上述规定的情形之外，磋商小组在评审过程中，不得接收来自评审现场以外的任何形式的文件资料。

33. 参与磋商的供应商数量要求

33.1 磋商文件能够详细列明采购标的的技术、服务要求的，磋商结束后，磋商小组应当要求所有通过了资格、符合性评审，继续参加磋商的供应商在规定时间内提交最后报价及有关承诺，提交最后报价的供应商不得少于 3 家，采用竞争性磋商采购方式采购的政府购买服务项目（含政府和社会资本合作项目）除外。

33.2 磋商文件不能详细列明采购标的的技术、服务要求的，需经磋商由供应商提供最终设计方案或解决方案的，磋商结束后，磋商小组应当按照少数服从多数的原则投票推荐 3 家以上供应商的设计方案或者解决方案，并要求其在规定时间内提交最后报价。采用竞争性磋商采购方式采购的政府购买服务项目（含政府和社会资本合作项目）除外。

33.3 供应商在提交最后报价之前可以根据磋商情况退出磋商（不影响保证金退还），提交最后报价的供应商不得少于 3 家，采用竞争性磋商采购方式采购的政府购买服务项目（含政府和社会资本合作项目）除外。

33.4 市场竞争不充分的科研项目，以及需要扶持的科技成果转化项目，当提交最后报价的供应商为 2 家时，磋商小组可以继续进行评审活动或宣布项目采购失败。

33.5 采用竞争性磋商采购方式采购的政府购买服务项目（含政府和社会资本合作项目），在采购过程中符合要求的供应商（社会资本）只有 2 家的，竞争性磋商采购活动可以继续进行。采购过程中符合要求的供应商（社会资本）只有 1 家的，采购人（项目实施机构）或者采购代理机构应当终止竞争性磋商采购活动，发布项目终止公告并说明原因，重新开展采购活动。

34. 评审办法

本项目评审办法详见本磋商文件第四部分。

（六）关于成交供应商

35. 成交供应商的确定

采购代理机构自评审结束之日起 2 个工作日内将评审报告和推荐成交意见送交采购人。采购人自收到评审报告之日起 5 个工作日内在评审报告推荐的成交候选人中按顺序确定成交供应商，也可以事先授权磋商小组直接确定成交供应商。

36. 磋商结果公告

经采购人确认后，采购代理机构在 2 个工作日内将成交公告在竞争性磋商公告规定的媒体上进行发布，并向成交供应商发出《成交通知书》，向未成交供应商发出《成交结果通知书》，《成交通知书》对成交供应商和采购人具有同等法律效力。

（七）采购代理服务费

37. 采购代理服务费

本次采购代理服务费按磋商须知前附表第 12 项规定收取。

（八）授予合同

38. 合同的订立

38.1 采购人自成交通知书发出之日起三十日内，按磋商文件要求和成交供应商响应文件及承诺与成交供应商签订合同，但不得偏离磋商文件和成交供应商响应文件的范围和实质性内容。

38.2 成交供应商在收到《成交通知书》后，应按照《成交通知书》指定的时间、地点，派遣其授权代表前往与采购人签署合同，并向**采购代理机构提交一份合同原件备案**。

39. 合同的履行

39.1 成交候选人采购人若遇排名第一的供应商放弃成交资格、不按要求与采购人签订采购合同、因不可抗拒力不能履行采购合同、不按磋商文件要求提交履约保证金，或者被查实存在影响成交结果的违法行为等情况，不符合成交条件的，采购人可按顺序确定综合得分排名第二的成交候选人为成交供应商，以此类推，或者重新组织采购。

39.2 采购合同订立后，合同各方不得擅自变更、中止或者终止合同。采购合同需要变更的，采购人应将有关合同变更内容，以书面形式报监督管理部门备案；因特殊情况需要中止或终止合同的，采购人应将中止或终止合同的理由以及相应措施，以书面形式报监督管理部门备案。

39.3 除不可抗力等因素外，成交通知书发出后，采购人改变成交结果，或者成交供应商拒绝签订政府采购合同的，应当承担相应的法律责任。

（九）关于询问、质疑

1 询问

1.1 响应供应商对政府采购活动事项（磋商文件、采购过程和成交结果）有疑问的，可以向采购人或采购代理机构提出询问，采购人或采购代理机构将作出答复。询问可以口头方式提出，也可以书面方式提出。

1.2 如采用书面方式提出询问：

供应商为自然人的，应当由本人签字或印鉴；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或印鉴，并加盖公章。

供应商递交询问函时，非法定代表人（供应商为法人时）或主要负责人（供应商为其他组织时 ）亲自办理的需提供授权委托书（应载明授权代表的姓名或者名称、代理事项、具体权限、期限和相关事项）及授权代表身份证复印件。

2 质疑

2.1 质疑期限

供应商认为磋商文件的内容损害其权益的，应在收到磋商文件之日或者磋商文件公告期届满之日起七个工作日内。（注：供应商购买磋商文件之日早于磋商文件公告期限届满之日的，则以供应商购买磋商文件之日为质疑时效期间的起算日期；否则，以磋商文件公告期限届满之日为质疑时效期间的起算日期）

供应商认为采购过程损害其权益的，应在各采购程序环节结束之日起七个工作日内。

供应商认为成交结果损害其权益的，应在成交结果公告期限届满之日起七个工作日内。

2.2 提交要求

以书面形式向采购人或者采购代理机构一次性提出针对同一采购程序环节的质疑。

以联合体形式参加政府采购活动的，其质疑应当由组成联合体的所有供应商共同提出。

2.3 质疑函内容

质疑函应包括供应商的姓名或者名称、地址、邮编、联系人及联系电话、质疑项目的名称及编号、具体且明确的质疑事项和与质疑事项相关的请求、事实依据、必要的法律依据、提出质疑的日期（详见财政部国库司发布的《政府采购供应商质疑函范本》。如有提供相关证据的，应填写《证据目录清单》，与质疑函一并提交）。供应商为自然

人的，应当由本人签字或印鉴；供应商为法人或者其他组织的，应当由法定代表人、主要负责人，或者其授权代表签字或印鉴，并加盖公章。

证据目录清单

序号	证据名称	证据来源	证明对象
	……		

供应商递交质疑函时，非法定代表人（供应商为法人时）或主要负责人（供应商为其他组织时 ）亲自办理的，需提供授权委托书（应载明授权代表的姓名或者名称、代理事项、具体权限、期限和相关事项）及授权代表身份证复印件。

2.4 供应商捏造事实、提供虚假材料或者以非法手段取得证明材料不能作为质疑的证明材料。

2.5 采购人或者采购代理机构在收到供应商的书面质疑后 7 个工作日内作出答复，并以书面形式通知质疑供应商和其他有关供应商，但答复内容不涉及商业秘密。

2.6 以邮寄、快递方式递交的，质疑提起日期应当以邮寄件上的戳记日期、邮政快递件上的戳记日期或非邮政快递件上的签注之日起计算，收到日期则以采购代理机构收到质疑函原件之日计算。

2.7 质疑联系方式

受理部门：广东志正招标有限公司内控部

地址：广州市天河区龙怡路 117 号银汇大厦 5 楼

电话：020-87554018

邮箱：tender@gd.gov.cn（用于接收质疑、询问）

（十）关于投诉

1 投诉形式

质疑供应商对采购人、采购代理机构的质疑答复不满意，或者采购人、采购代理机构未在规定期限内作出答复的,可以在答复期满后 15 个工作日内向采购人的同级政府采购监督管理部门提起投诉。投诉时，应以书面形式。

第二部分 用户需求

说明：

1. 供应商须对本项目为单位的货物及服务进行整体响应，任何只对其中一部分内容进行的响应都被视为响应无效。

1 总体要求

1.1 说明

1.《用户需求》中标注有“★”号的条款必须实质性响应，负偏离（不满足要求）将导致投标无效。“▲”号条款为评审打分重要条款,每个“▲”号为一个指标要求。如无特别说明，上述条款要求提交承诺作为响应材料。

2.投标文件的响应内容均真实有效，且按原厂商产品参数和服务标准进行响应，否则将被视为无法实质性响应采购文件而作废标处理；需求中安全产品技术要求清单所示服务数量为最低交付标准，提供安全驻场服务的厂商需要按照省戒毒管理局的要求提供该清单指定服务数量之外的安全相关服务次数；对于总体性能达不到客户要求的情况下，如需增加设备资源，则相关成本由供应商承担；供应商如在投标时承诺满足，但中标后发现有虚假响应，即事实上不能满足的，采购人将报政府采购监管部门依法处理。

1.2 项目概述

1.项目名称：2020 年省戒毒局机关网络安全项目。

2.最高限价：人民币 151.7 万元，投标报价超出预算金额将作无效投标处理。总报价均应已包含国家规定的所有税费。

3. 供应商需提供质保期后的服务方式、范围及收费标准，以做参考。

4.项目周期：本次项目中安全运营驻场服务周期为 2 年；终端安全管理系统的部署时间不多于 30 天，质保期 3 年。

5.本项目包括安全驻场服务、安全培训服务和终端安全管理系统建设三个方面。驻场地点主要在局机关，特殊情况需要到基层戒毒单位。服务范围涉及广东省戒毒管理局（政法专网、工作专网、电子政务外网等非涉密网）以及省属单位内已有网络、所有信息化设施包括不限于计算机终端、服务器、网络设备、安全设备、存储设备等及非涉密政务系统、数据库和中间件等；安全培训服务涉及局机关及全省戒毒单位；终端安全管理系统将在广东省戒毒管理局机关（一级部署）和 11 个省直单位（二级部署）进行安装调试部署，通过服务加产品集成的方式构建基础的网络安全防御体系。

6.投标产品必须达到等保二级要求；软件安装调试后必须稳定运行，软件累计出现三次同类问题或不能满足业务需求，且不能查明原因或给出的理由不能让采购人接受的，省戒毒管理局有权要求供应商更换性能更好的产品，因此产生的一切费用由供应商承担。

1.3 项目建设背景

2017 年 6 月 1 日，我国第一部网络安全法《中华人民共和国网络安全法》正式实施，我国网络安全管理迈入法治新阶段，网络空间法治体系建设加速开展。网络安全法中对网络安全应急演练工作明确指出：“关键信息基础设施的运营者应制定网络安全事件应急预案，并定期进行演练”，“国家网信部门应当统筹协调有关部门应定期组织关键信息基础设施的运营者进行网络安全应急演练，提高应对网络安全事件的水平和协同配合能力”，“负责关键信息基础设施安全保护工作的部门应当制定本行业、本领域的网络安全事件应急预案，并定期组织演练”要求关键信息基础设施的运营者、国家网信部门等应定期组织开展应急演练工作。

2018 年全国网络安全和信息化工作会议于 4 月 20 日至 21 日在北京召开，习总书记出席会议并发表重要讲话，强调“没有网络安全就没有国家安全，就没有经济社会稳定运行，广大人民群众利益也难以得到保障。要树立正确的网络安全观，加强信息基础设施网络安全防护，加强网络安全信息统筹机制、手段、平台建设，加强网络安全事件应急指挥能力建设，积极发展网络安全产业，做到关口前移，防患于未然。要落实关键信息基础设施防护责任，行业、企业作为关键信息基础设施运营者承担主体防护责任，主管部门履行好监管责任”。

2019 年 5 月 13 日，国家市场监督管理总局召开新闻发布会，网络安全等级保护制度 2.0 国家标准(下称“等保 2.0”)正式发布，并将于 2019 年 12 月 1 日正式实施。等保 2.0 在等保 1.0 的基础上，注重全方位主动防御、动态防御、整体防控和精准防护，实现了对云计算、大数据、物联网、移动互联和工业控制信息系统等保护对象全覆盖；等保 2.0 标准依然采用“一个中心、三重防护”的理念，从等保 1.0 标准被动防御的安全体系向事前预防、事中响应、事后审计的动态保障体系转变。

由此可见，安全运营将是政府企事业单位做好网络安全工作的重要抓手，《网络安全法》、《网络安全等级保护基本要求 2.0》中，都已明确提出了安全监测处置的要求，这是安全运营的重要环节。尤其在等保 2.0 中要求的安全管理中心，更是说明安全运营管理是明确的合规要求。

1.4 项目建设依据

- 《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》（国务院 147 号令）
- 《国家网络空间安全战略》（中共中央网信办）
- 《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 网络安全等级保护安全设计技术要求》（GB/T25070-2019）
- 《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 网络安全等级保护测评过程指南》（GB/T 28449-2018）
- 《信息安全技术 网络安全等级保护安全管理中心技术要求》（GB/T 36958-2018）
- 《网络与信息安全风险评估服务能力评估方法》（YD/T 2252-2011）

- 《信息安全技术 信息安全风险评估规范》（GB/T 20984-2007）
- 《信息安全技术 信息安全风险评估实施指南》（GB/T 31509-2015）
- 《信息安全技术 信息系统通用安全技术要求》（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 20272-2006）
- 《信息安全技术 数据库管理系统安全技术要求》（GB/T 20273-2006）
- 《信息安全技术 服务器技术要求》（GB/T 21028-2007）
- 《信息安全技术 信息系统安全管理要求》（GB/T 20269-2006）
- 《信息安全技术 信息系统安全工程管理要求》（GB/T 20282-2006）
- 《信息保障技术框架》（IATF）
- 《信息技术 安全技术 信息安全管理体系 要求》（GB/T 22080-2016）
- 《信息安全技术 信息系统密码应用基本要求》（GM/T 0054-2018）

1.5 项目建设总体目标

本项目按照国家和司法部的有关规定和标准规范要求，遵照 等保 2.0 标准，坚持管理和技术并重的原则，在省戒毒管理局建立一套标准化的网络安全运营管理体系，以省局机关为中心，在局机关和省直基层场所分级部署终端安全管理平台，在局机关综合采取驻场值守、日常巡检、应急响应处置、技术指导等方式和流程，对局机关及省直基层场所进行统一的、标准的、可量化的基础网络安全管控、防范，以科学合理的方法实现最短时间内协调设备资源、人力资源、管理资源，对省戒毒管理局网络安全事件进行有效处置，指导、协助全省戒毒基层单位开展网络安全管理工作，保障 省戒毒管理局的网络空间安全、稳定，相关系统持续、有序、安全运转。本次项目将达成以下目标：

1.建立标准化的网络安全运营管理体系：从管理制度建立、管理机构设立、人员安全、应用系统建设、系统运维管理、运行管理机制等维度，建立一套标准化的网络安全运营管理体系，建设“事前全面预防、事中积极防御、事后快速检测”的安全防御体系，指导局机关、基层场所及时有效地排查、防范网络安全风险隐患，全面提升省戒毒管理局的网络安全防护水平。

2.健全完善的网络安全管理制度：建立健全省戒毒管理局的网络安全工作的纲领性文件，在网络安全方针策略的指导下,制定各项网络安全管理和技术制度、办法和准则,规范和指导局机关各业务处室、基层场所网络安全管理工作。

3.建设专业的网络安全管理队伍：由信息安全领导小组进行决策、监督及管理，设置安全管理员、安全审计员、系统管理员、网络管理员、数据库管理员、机房管理员等负责执行，定期开展安全专项培训工作，提高安全队伍的专业能力。

4.打造快速的网络安全 运维团队：通过现场运维和应急响应的方式，提升日常网络安全和突发安全事件的处理能力，打造一个全天候、高水平、反应快的运维团队。

5.加强突发事件的应急处置能力：提升省戒毒管理局安全管理人员和驻场安全工程师对网络安全突发事件的实时检测、分析和应急处置能力和协作配合能力，大力提升省戒毒管理局网络安全意识。

2 需求分析

2.1 安全服务需求

2.1.1 现场驻场服务需求

本次项目涉及的现场驻场服务需根据省戒毒管理局要求，提供现场驻场人员 2 人（高级驻场工程师以及中级驻场工程师各 1 人），现场驻场服务周期 2 年。负责安全服务的组织、管理、咨询、日常事务性等工作，提供 5x8 小时驻场服务现场值班、技术支持、安全事件应急处置、日常巡检、特别对 ODAY 漏洞类的情报收集分析等驻场服务，对常见网络攻击及防范措施有一定见解，如 Injection、XSS、CSRF、DDOS，具有现场应急处置、漏洞分析、漏洞（修复）验证、安全加固、日志分析等能力，要求是计算机相关专业，本科或以上学位，具有 2 年或以上、安全服务等工作经验，熟悉网络相关技术，并考取 CISP 证书的安全服务工程师。其中高级驻场工程师至少具备 1 年及以上渗透测试工作经验，需具备参加省级或以上的护网行动的经验，参加过大型企业和政府部门的安全运维，熟悉各种安全检测工具的使用，及时响应用户的需求，有良好的写作能力和表达沟通能力，负责对局科技部门技术人员进行具体技术指导。中标商需提供驻点人员在其公司任职的相关证明材料，提供人员管理及配备方案，确保人员的稳定。如更换服务人员，须由省戒毒管理局同意并签字确认。

每位驻场工程师均有能力独立完成以下工作内容：

1.负责信息安全日常运维工作。

2.信息安全风险评估工作。

3.信息安全加固工作。

4.负责用户安全制度编制与修订工作。

5.信息安全应急工作。

6.漏洞扫描工作

2 名驻场安全工程师均须提供工作日 5x8 小时的驻场服务、周末及节假日 7x24 小时值班以及在戒毒管理局要求的期间内提供 7x24 小时值班服务。

值班服务主要工作内容包括但不限于：按照省戒毒管理局的要求统筹开展戒毒管理局各项网络安全工作，为基层单位特别是省直戒毒单位提供网络安全应急技术指导和支撑服务，工作日时

间 8:30-17:30 提供 5x8 小时的驻场服务，周六日、重大节假日以及戒毒管理局要求的重要保障期间内提供 7x24 小时驻场服务、7x24 小时的响应服务、安全制度制定、安全事件处置、日常安全巡检、日常安全扫描、安全问题整改落实、安全服务咨询等。其中周六日、重大节假日以及戒毒管理局要求的重要保障期间内提供 7x24 小时驻场服务，安全服务供应商需统筹安排其中 1 名驻场安全工程师现场值班轮班，下一个月的值班表每月 20 日前报省戒毒管理局。重大节假日以及戒毒管理局要求的重要保障期间内，除现场驻场的 2 名安全工程师外，可增加二线专家参与现场值班轮班，值班表需提前 5 个工作日报省戒毒管理局报备。

驻场人员服务工作内容包括但不限于：在风险评估服务、安全加固服务、安全应急服务、漏洞扫描服务、应用系统渗透测试、安全攻防演练服务、安全重保服务等安全运营驻场服务需求及采购清单中提到的内容，因人手、技术能力或资质要求无法保障，提供安全驻场服务的厂商必须按照实际情况及省戒毒管理局的要求及时安排二线专家团队或专业安全公司进行技术保障，因安排不及时或处置不当造成的不良影响甚至损失的，省戒毒管理局有权依法追究提供安全驻场服务的厂商的责任。上述服务因实际需要增加的人手、二线团队或专业公司服务的所有费用均包含在投标总价中，不得另行收取费用。

详细要求如下：

为省戒毒管理局机关（政法专网、电子政务外网、工作专网等非密网）提供安全管理检查和现场安全值守工作，并指导下属单位的安全工作，协助局机关落实相关安全政策以及相关要求。根据国家部委、省委省政府、省政数局以及司法厅等定期安全评估，不定期系统安全审计，定期的安全事件审计及响应处理，不定期的重大节假日或活动的安全应急服务，同时根据广东省有关部门制定的安全检查内容及方法，通过在日常运维中将安全的整个运维流程融入到日常的工作中，及时掌握业务应用系统安全状况和面临的威胁，认真查找隐患，完善安全措施，减少安全风险，提高应急处置能力，确保系统持续安全稳定运行。全面推进安全客户端统一集中管理；进一步合理优化划分安全域，进一步完善统计信息安全监控、审计机制和安全运维。对本单位内外网（政法专网、电子政务外网、工作专网等非密网）、办公系统等进行安全分析、风险评估和安全监控；对本单位突发事件分析处置，并制定有效策略进行防范；负责处理安全事件，按需应急响应并设计规避风险方案；跟踪和分析各类安全问题和安全事件，支持各系统日常安全工作，引导各系统相关负责人修复安全问题；

驻场安全工程师在服务期间需要完成省戒毒管理局机关科技部门交办的其他安全工作任务，根据工作需要对基层场所特别是省直戒毒单位进行相关的网络安全分析、漏洞扫描、风险评估等工作，及时为基层单位提供网络安全应急技术指导和支撑服务。因特殊情况需要，如需驻场安全工程师赶赴基层场所特别是省直戒毒单位提供现场技术支援的，由省戒毒管理局统一安排车辆，提供安全服务的公司不得以任何形式向省戒毒管理局收取任何费用。

供应商需指定一名项目经理，负责本服务项目的统一管理和协调。项目经理应在以下领域拥有丰富的项目经验：

1.安全咨询领域

2.网络架构领域

3.系统架构领域

4.服务管理领域

5.安全检测领域

拟投入的项目经理需熟悉 ISO27001、COBIT、ITIL/ISO20000 等标准或最佳实践，要求在信息安全领域拥有 5 年以上工作经验，具备 3 次以上担任类似信息安全咨询规划、信息安全审计、等级保护等项目经理经验。

项目经理具备相关信息安全专业资格证书。

2.1.2 安全运营体系建设需求

1.协助省戒毒管理局建立健全网络安全管理组织，根据省戒毒管理局的实际情况，健全完善网络安全管理组织架构，明确组织各个层级的职责分工。

2.健全完善网络安全的管理制度和管理机制，建立针对网络安全的考核指标，定期组织针对网络安全意识、网络安全技能等的培训，协助省戒毒管理局开展网络安全检查，确保网络安全可控。

3.网络安全开发生命周期各项控制措施的落地，完善软件安全开发生命周期在需求分析、软件设计、编码开发、测试部署、上线运行、系统下线等各个阶段的管理流程和技术管控措施，确保系统安全技术措施的同步规划、同步建设、同步使用。

供应商需向省戒毒管理局提供网络安全开发生命周期落地的技术工具，费用包含在投标报价中。

2.1.3 风险评估服务需求

供应商需提供专业的服务团队在现场驻场服务期（2 年）内按照客户要求或按需对省戒毒管理局的信息系统和 IT 基础设施进行安全风险评估，并出具评估报告。风险评估包括风险评估范围、识别重要资产、识别脆弱性和威胁、现有安全控制措施、应用系统漏洞扫描、分析和计算风险状况、并出具风险评估报告。风险评估要识别戒毒管理局的信息资产、业务信息、面临威胁和自身脆弱性，对安全风险进行全面分析，为建立省直单位政务信息系统安全运营体系提供依据;识别戒毒管理局安全运维需求，为制定安全运维方案提供依据；识别戒毒管理局系统迁移上云的安全需求，为系统迁移上云提供安全保障。

针对现有的资产进行资产核查。包含内部主机、数据库、中间件、核心网络设备全量资产进行识别、梳理。通过多种工具与人工结合排查已知与未知资产并落实相关责任人后，出具资产清单，包括但不限于硬件配置信息、ip、操作系统版本、属主等。

对新增上线系统进行漏洞扫描，web 扫描，基线检查等服务后，出具新增上线检查评估报告。在服务期间内，对新上线系统进行安全检测，该服务的对象是应用系统，包括物理环境、网络设备、操作系统、应用软件、数据等,服务通过从系统漏洞、配置核查、安全管理风险、内在风险等方面进行全面检测。新系统上线检查服务的实施时间应在应用系统完成编码与测试阶段，部署至生产环境后，正式发布前。

每月定期编制资产清单。

供应商需承诺服务期内按照客户要求或按需提供风险评估服务，并出具风险评估报告。

2.1.4 安全加固服务需求

定期（出现重大安全补丁发布要两个工作日内更新）；对局机关所有系统主机、服务器等设备安全加固，包括针对各种设备、多种操作系统、多项应用打补丁、停止不必要的服务、升级或更换程序、除去后门程序、修改配置及权限以及针对复杂问题的专门解决方案等服务，并对省直单位提供安全加固提醒或指导服务。须使用正版或具有自主产权的工具进行服务。

1.主机安全加固

根据省戒毒管理局实际情况和业务使用情况，针对操作系统、数据库、中间件等组件进行安全加固。操作系统安全加固包括账户安全、密码安全、主机防病毒安全、日志审计安全、访问控制安全、安全防护安全；数据库安全加固包括账户安全、密码安全、日志审计安全、访问控制安全；中间件安全加固包括账户安全、密码安全、日志审计安全、访问控制安全。

2.网络设备加固

根据省戒毒管理局实际情况和设备使用情况，针对网络设备安全配置进行安全加固，安全配置加固包括密码安全、账户安全、日志审计安全、运维管理安全、访问控制安全。

3.安全设备加固

根据省戒毒管理局实际情况和设备使用情况，针对安全设备安全配置和网络架构等进行安全加固，安全配置加固密码安全、账户安全、日志审计安全、运维管理安全、访问控制安全；网络架构安全加固包括访问控制安全、安全防护安全、加固安全。

在服务期间内，对戒毒所现有服务器、数据库、中间件进行系统加固。协助进行安全加固检查主要从加固修补系统漏洞、系统帐户权限强化，加强服务器日志审核，过滤危险服务，屏蔽不必要的端口服务，优化注册表等方面来进行，并出具安全加固意见报告。

对每季度的主机漏洞扫描的漏洞进行定级，出具漏洞整改建议及方案，协助相关方进行漏洞跟踪及修复。

对每季度的 WEB 漏洞扫描的漏洞进行定级，出具漏洞整改建议及方案，协助相关方进行漏洞跟踪及修复。

供应商需承诺服务期内按照客户要求和需要进行全面的安全加固服务，并出具安全加固报告。

2.1.5 安全应急服务需求

应急响应，是当省戒毒管理局系统遭受病毒传播、网络攻击、黑客入侵，安全事件从而导致信息业务中断、系统宕机、网络瘫痪，数据丢失、企业声誉受损，并对组织和业务运行产生直接或间接的负面影响时，由安全专家提供的入侵原因分析、业务损失评估、系统恢复加固、以及黑客溯源取证的安全服务，减少因黑客入侵带来的损失。

在日常运维过程中，需要及时了解零日漏洞、业界新发现的高危安全漏洞、突发安全事件的影响，根据网络网络设备、网站与信息系统资产指纹库，进行预警，提出遏制和缓解措施。发生紧急安全事件或特殊安全保障任务期间，驻场人力不足情况下，服务商需增派专业人员应急处置。

在日常运维过程中，遇到无法解决的以下事件：主机系统或网络与安全有关的紧急事件、网络入侵、拒绝服务攻击、网络病毒传播爆发等，在现场驻场人员不具备应急处理的情况下，二线专家团队派出专业的信息安全工程师，1 小时内快速响应现场解决安全问题；应急响应的流程必须包含以下内容：故障诊断、故障修复、系统清理和系统防护；

每次服务完成后，现场驻场人员必须提交完整的《X 事件分析报告》，详细说明事件原因、经过和处理方式等，而且对以后整改的方向提供适当的解决方案。

供应商需提供 7x24 小时的应急技术支持服务，若遇到突发的安全问题，如：发生网络入侵事件、大规模病毒爆发、遭受拒绝服务攻击等，无法及时对该事件进行处理或解决时，在收到省戒毒管理局应急响应服务信息后，二线专家团队在 1 小时内赶到现场，协助查明安全事件原因，确定安全事件的威胁和破坏的严重程度，解决出现问题；对于省直单位以及各地市戒毒所的安全事件，供应商 需能 提供指导以及远程协助，必要时需要现场进行技术支持。

2.1.6 漏洞扫描服务需求

省戒毒管理局运行的服务器、终端、网络设备、安全设备、网站及应用系统，可能存在硬件、软件、协议的具体实现或系统安全策略上的缺陷，这些缺陷可能被攻击者所利用从而产生不利影响，这些缺陷就是安全漏洞。

通过安全扫描评估，可以及时发现信息系统中存在的安全漏洞，通过对 Windows、Linux 服务器及安全设备漏洞的整改，可以及时地消除安全漏洞可能带来的安全风险。须使用正版或具有自主产权的工具进行服务。

供应商需承诺服务期内按照客户要求和需要进行针对所有业务系统的漏洞扫描服务，并出具整改建议报告。

2.1.7 渗透测试服务需求

渗透测试是由具备高技能和高素质的安全服务人员发起、并模拟常见黑客所使用的攻击手段对目标系统进行模拟入侵，找出系统中未知的脆弱点。渗透测试服务的目的在于充分挖掘和暴露系统

的弱点，向用户提供安全整改建议。

模拟黑客的攻击思路对戒毒管理局进行各种入侵攻击测试，渗透测试执行期间，渗透测试工程师会以模拟黑客常用的攻击手段，尝试入侵授权范围内的 WEB 应用、操作系统、网络设备，找出各种潜在的安全漏洞，以验证戒毒管理局的设备与资料是否可被破坏或窃取。

渗透测试结束后，渗透测试工程师会列出渗透测试过程中使用的攻击手法与步骤，并针对漏洞提供可靠的修复建议，让戒毒管理局能够降低遭受入侵的风险。

渗透测试范围包括局机关所有信息化基础设施、服务器、操作系统、网络设备以及非涉密信息系统等。须使用正版或具有自主产权的工具进行服务。

供应商需承诺服务期内按照客户要求和需要进行渗透测试服务（省局或直属单位），并出具渗透测试整改建议报告。

2.1.8 安全攻防演练服务需求

驻场服务周期内为戒毒管理局提供至少两次安全攻防演练服务，制定应对不同安全事件的应急预案，确定不同安全事件的应急处理流程、系统恢复流程；明确各有关部门的职责，健全省戒毒管理局网络与信息安全运行应急工作机制；通过演练检验系统安全应急预案的科学性、可操作性，验证应急响应小组和技术人员应对网络和信息安全突发事件的组织指挥能力和应急处置能力。确保发生安全事故时响应工作及时、有效，能最大限度减轻网络与信息安全突发事件造成的损失。

通过模拟真实的网络攻防场景，从实战环境中提升安全人员的安全技能和防护水平。在了解单位实际安全状况的基础上，针对单位重要核心业务，模拟多种生动逼真的红蓝对抗（网络攻防）场景，使业务人员了解常见网络攻击过程与实际防护，培养和提升戒毒管理局安全人员的安全意识。红蓝对抗可以揭示信息系统的漏洞与安全脆弱性，促进信息系统和信息安全管理制度的不断完善，从而更好地保护戒毒管理局的数据信息安全。并最终交付安全攻防演练报告，总结省戒毒管理局安全工作短板。供应商须提供攻防演练所需环境以及设备等，并使用正版或具有自主产权的工具进行服务。

攻防演练服务主要包含下列服务内容：

1.攻防演练环境的设计及搭建，根据演练内容，目标主机、应用环境、网络环境的安装、配置以及部署；

2.演练前的培训以及演练安排包括：演练前的基本技能培训、攻防双方的使命及注意事项。如胜利点制定、手段限制等、关键事件的引入。如利于某一方的事件导入、角色互换等、演练过程中攻防环境的维护及监控、演练结束时的结果裁定。

供应商需承诺服务期内按照客户要求和需要举行攻防演练（至少两次），并提供攻防演练所需环境以及设备等资源。

2.1.9 安全重保服务需求

为戒毒管理局提供重要时期的系统重点监控、预警、防护服务。帮助戒毒管理局在系统遭到攻击时能够做出及时反映，启动应急。将攻击的危害程度降到最低。

在国庆、两会、春节、重要节假日（如清明、五一、中秋、端午等）、重要会议、极重要业务服务时间段以及局机关要求的期间开展安全职守服务，对重要业务系统特别是门户网站的完整性进行安全检查；分析网络安全设备的日志以发现重要的安全事件，对重要安全事件协调相关人员开展应急响应工作；分析设备性能在重要时间内的运行情况，判断设备性能的最大负荷等等。

供应商需随时响应省戒毒管理局需求，若遇到突发的安全问题，如果现场驻场安全工程师无法及时对该事件进行处理或解决时，在收到省戒毒管理局应急响应服务信息后，需供应商安排二线专家在 1 小时内赶到现场，协助查明安全事件原因，确定安全事件的威胁和破坏的严重程度，解决出现问题；对于省直单位以及各地市戒毒所的安全事件，供应商需能提供二线专家指导以及远程协助，必要时需要二线专家到现场进行技术支持，供应商不能以任何理由额外收取费用，如果因为供应商响应不及时或处置不当造成损失的，省戒毒管理局有权向供应商追究责任。

2.2 安全培训服务需求

本次项目涉及的安全培训服务按下表中的要求，提供包括但不限于表中所列的培训方案。

培训项目	地点	要求
安全意识培训	省局	1.在省局召开全省视频会议形式进行培训，基层单位人员远程接入 2.包括但不限于《网络安全法》《网络安全等级保护》《应急响应》《应急演练》等内容。 3.服务周期内，至少组织 2 次培训
安全产品操作培训	现场	1.产品厂家为局机关及省直戒毒单位进行产品培训 2.讲师必须是原厂工程师
	不限	1.安全产品统一培训：培训人数不少于 35 人，分 2 批次进行培训 2.培训服务商需要提供实际操作演示环境 3.培训服务涉及的所有学员培训期间的食宿及培训场所、培训教材等费用包含在本次投标总价中。 4.每次脱产培训 2-3 天 5.培训对象为局机关和省直单位的技术人员，各省直单位约 2-3 人
安全专家 CISP 课程认证培训	不限	1.培训人数至少 3 人，可分批次进行培训 2.CISP 课程认证培训 3.培训服务涉及的所有学员培训期间的食宿及培训场所、培训教材等费用包含在本次投标总价中。 4.每批次脱产培训至少 5 天 5.培训对象局机关技术人员

2.3 安全产品需求

2.3.1 安全产品整体要求

本次项目涉及的安全产品主要是采购 1 套终端安全管理系统，产品使用范围包括广东省戒毒管理局政法专网和电子政务外网，部署地点包括省戒毒管理局局机关及 11 个省直戒毒单位。含 3000 个客户端管理授权（包含 PC 终端、服务器），管理端授权不限，质保期 3 年。

本次项目按照广东省戒毒管理局的业务应用、工作职能，根据等保 2.0 提出新的“集中管控”安全要求，在政务专网内，省戒毒管理局局机关统一部署终端安全管理系统，在 11 个省直戒毒单位进行二级部署，对局机关和省直单位的电脑终端、服务器、外设设备以及非法外联行为进行统一的安全防范和管控实现统一收集、集中监控、集中分析、集中管理等一系列新的安全运营要求（包括不限于统一资产管理、终端病毒防护、统一补丁管理、移动存储管理、运维安全管控、报表和查询等功能，以及网络安全准入模块和终端安全态势大屏分析模块等方面），通过安全控制中心平台，建立围绕终端的综合安全评估体系、建立终端威胁发现与快速应急响应体系、全面的终端安全审计体系。

终端安全管理系统具体建设内容为：

1.通过终端安全管理系统实现省戒毒管理局机关、省直戒毒单位统一的、分级管控的病毒防护、补丁管理、资产管理、运维管控、移动存储管理等基础防护，对终端（含不限于终端 PC、服务器、外设网络设施、U 盘等）实施基础的安全防护、管理措施，对终端安全日志等数据进行统计分析，实现终端安全信息可视化展示，为终端安全管理提供可视化分析的技术支撑。另外，省戒毒管理局部署终端安全拓展功能身份准入模块，覆盖省局范围内人员设备的入网。

2.在省戒毒管理局局机关部署私有云查杀措施，利用动态检测、沙箱检测、机器学习等技术，实现文件威胁鉴定、评估与高级威胁发现，同时基于该私有云查杀引擎提升终端安全管理系统的病毒检测和防护能力。

供应商需出具合理的安全产品实施方案并在规定工期内完成实施。

凡项目技术指标要求中列出的配置及技术参数要求，均要求全部配置开通，不得在产品交付后以产品支持该功能，但需单独购买等理由要求采购方额外支出修改费用。

本项目安全产品需预留未来与上级部门或省直单位系统及设备对接的接口，涉及本项目安全设备的对接费用均包含在本次报价中，采购人不再额外支付。

投标产品必须达到等保二级要求；与软件安装调试后必须稳定运行，设备或软件出现问题三次或不能满足业务需求影响使用的，不能查明原因或给出的理由不能让采购人或监理接受的，省戒毒管理局有权要求供应商更好性能更好的产品，因此产生的一切费用由供应商承担。所有投标

产品必须满足技术参数的性能指标、产品资质、服务要求，低于性能指标、不提供产品资质（或提供资质不全）以及低于服务要求的全部视为不符合招标要求。

2.3.2 安全产品部署说明

为了实现全省戒毒系统终端安全防护与安全管理，方案规划在省戒毒管理局机关及省直戒毒单位分级部署终端安全管理系统，实现全面的终端安全防护与终端运维管理。

2.3.2.1 省局的部署

1.控制中心、代理客户端——在广东省戒毒管理局局机关在政务专网、电子政务外网分别部署终端安全管理系统控制中心，在各办公业务终端、服务器部署客户端，控制中心能集中向各终端推送终端防护策略和功能，包括：防病毒、补丁更新、安全管控、移动存储管理、运维安全管控、报表和查询等功能，以及网络安全准入模块、终端安全态势大屏分析等策略，终端客户端执行相关策略并上报终端系统安全日志数据，并实现终端安全信息可视化展示，省局管理员对省直戒毒单位有监测、监督及指导权限，能够总览全省终端安全状况。

2.私有云查杀引擎——由于广东省戒毒管理局处于政法网内，与互联网隔离，因此需要在本地部署私有云查杀引擎，私有云查杀引擎集成海量病毒样本信息库，实现内网环境下病毒查杀。病毒库更新通过手工离线更新的方式进行，并配备专用的病毒更新工具。

2.3.2.2 省直戒毒单位的部署

各省直戒毒单位需要在各单位内部部署控制中心、客户端，客户端根据控制中心制定的安全策略，进行杀毒、修复漏洞、运维管控、移动存储管理等安全操作。

2.3.3 安全产品主要功能描述

2.3.3.1 终端资产管理

终端安全管理系统具备跟踪硬件资产变更功能，可帮助管理员及时获取硬件资产的变更记录，硬件新增、丢失情况，对硬件变更准确监控，及时预警，方便财务审计，轻松构建专业的企业硬件资产监控与审计平台。

资产信息采集内容需包括以下两个方面：

终端硬件资产：采集统计包括计算机类型、计算机型号、CPU、内存、硬盘、显卡、显示器、硬盘序列号、MAC 地址等硬件相关信息。

操作系统资产：采集统计包括操作系统版本、系统类型、系统升级包、系统语言、激活状态、产品密钥、注册人、安装时间等信息。

2.3.3.2 终端病毒与恶意代码防范

终端安全管理系统包含技术先进的网络版防病毒功能，支持对蠕虫病毒、恶意软件、广告软件、勒索软件、引导区病毒、BIOS 病毒的查杀，这依赖于人工智能引擎、云查杀引擎等多引擎的协同工作，防御病毒木马变种及新型病毒，基于主动防御技术防御未知病毒、未知威胁和 0-Day 攻击。

1.病毒云查杀：查杀建立在云端庞大的黑白名单数据库基础上，病毒检出率高，系统资源占用低。通过使用云端的黑白名单验证的方法，可以最大限度的保护数据安全。在广东省戒毒管理局隔离网环境下，云查杀优势无法很好的体现，病毒查杀率将降低，因此系统为广东省戒毒管理局配备私有云查杀引擎，通过在隔离网部署私有云查杀引擎，使病毒查杀效果与客户端联网时没有差别。

2.主动防御：主动防御功能可以防御未知病毒、未知威胁和 0-Day 攻击。主动防御是基于程序行为自主分析判断的实时防护技术，不以病毒的特征码作为判断病毒的依据，而是从最原始的病毒定义出发，直接将程序的行为作为判断病毒的依据。主动防御解决了传统安全软件无法防御未知恶意软件的弊端，从技术上实现了对木马和病毒的主动防御。在实现机制上可以对文件访问、进程创建、注册表读写、网络 IP 请求、设备加载完成主动防御拦截。

2.3.3.3 私有云查杀引擎

为适应内网中病毒查杀，本方案中通过部署私有云查杀引擎，提升内网环境下病毒查杀能力。私有云查杀引擎提供病毒 MD5 静态查验及动态行为分析能力。

2.3.3.4 补丁管理

在全省戒毒系统办公网络中存在各种不同类型、不同版本的操作系统都需要管理员进行全面的补丁管理，管理员往往需要甄别不同的操作系统并根据各个系统的不同情况有选择性的下发系统补丁。终端安全管理系统可以对全网计算机进行扫描，发现存在漏洞风险的主机，管理员可以批量下发主机补丁并安装。同时可以根据终端或漏洞进行分组管理，并且能够根据不同的计算机分组与操作系统类型将补丁错峰下发，在保障网络带宽的前提下可以有效提升企业整体漏洞防护等级。

2.3.3.5 终端安全管控

实现终端安全合规管控，实现包括终端流量管理、非法外联检测、应用程序管控、网络管控、外设管理等终端管控功能。

1.流量管理：通过终端安全管理系统流量管理，管理员可以了解各终端的网络流量情况，包

括终端的实时网络速度、一段时间内的下载上传流量等，同时能够对终端的上传及下载流量限制进行统一管控，帮助管理员管理网络流量，避免非法应用占用大量带宽，保证正常业务的平稳运行。

2.非法外联：非法外联管理模块可以针对通过 3G 网卡、随身 Wifi 等方式使内网电脑可以通过非法途径连接外网导致敏感数据泄漏等问题的出现，非法外联管理模块无论终端使用何种方式连接外网都可以在第一时间对管理员发送告警并隔离非法终端,在最大程度上保障核心数据安全。

3.应用程序安全：应用程序安全支持进程黑白名单，添加进白名单的进程为信任进程，而黑名单中的进程为恶意进程，系统将直接阻断该类进程。另外，还有进程红名单，添加进进程红名单的进程为必须运行进程，可以防止恶意程序对该必备类型应用进行破坏。

4.网络安全：网络安全防护通过黑白名单准测来确保网络安全。管理员可以添加某些网络连接的协议类型，IP 地址和端口号或者添加 URL 地址来使它成为黑名单或者白名单，从而保证我局网络安全。

5.外设管理：外设是 PC 使用者传输数据的通道，为我们日常的工作带来了极大的方便，但是，对于终端的安全运维管理同时带来了难题。一方面终端用户可能会通过外设将数据传出到单位外，另一面终端用户可能会通过外设通道将病毒感染至单位内部各个终端。采用策略化的外设管理模式，可帮助管理员对终端的 USB 口、1394、串口、并口、PCMCIA 卡等接口进行启用和禁用控制，支持的设备有 USB 移动存储、非 USB 移动存储、存储卡、冗余硬盘、软驱、打印机、扫描仪、磁带机、键盘、鼠标、红外、蓝牙、摄像头、手机/平板等常用设备进行禁用管理，也支持光盘的读写控制功能。管理员可通过终端安全管理系统对 PC 终端外设进行强有力的全面管控，杜绝数据外泄和感染病毒的风险。

2.3.3.6 移动存储管理

实现对移动存储设备的管控，保证终端与移动存储介质进行数据交换和共享过程中的信息安全要求。移动存储管理包括移动存储介质的身份注册、网内终端授权管理、移动介质挂失管理、外出管理和终端设备例外等功能。

2.4 网络安全需求清单

★2.4.1 建设内容要求描述

本期项目建设内容要求符合我国工信部关于政府单位信息化建设的指导意见，确保在产品质保期内所建系统满足国家上级部门针对信息安全提出的规范，要求采购的安全产品能全面兼容龙芯、鲲鹏、兆芯、飞腾、海光等不同 CPU 架构，中标麒麟、银河麒麟、中科方德、UOS 等众多操作系统，

建设内容包括后续与以上系统迭代版本的适配工作。投标方承诺供货时提供安全产品厂商针对此项目的售后服务承诺函和主要设备点对点技术参数响应表（加盖公章），不响应视为虚假响应，承担相关法律责任。网络安全需求清单所示服务数量为交付最低标准，服务商需要按照省戒毒管理局的要求提供该清单指定服务数量之外的安全相关服务次数。

2.4.2 需求清单

本次项目建设网络安全需求如下：

序号	类 别	小 项	内容	数量	单位	备 注
一、安全服务						
1	驻场安全工程师安全运营驻场服务： 1.高级驻场工程师及中级驻场工程师各 1 人，共 2 人； 2.现场驻场服务 2 年； 3.二线团队服务 4.**详细要求见“2.1 安全服务需求”以及“3.1 安全驻场等服务要求”等相关内容）**	现场驻场	2 名安全服务工程师现场值班，现场服务周期 2 年，工作日 5*8 小时，节假日（含周六日）7*24 小时。节假日（含周六日），安全服务供应商需统筹安排其中 1 名驻场安全工程师现场值班轮班，下一个月的值班表每月 20 日前报省戒毒管理局。	2	年	驻场地点：主要在局机关，特殊情况需要到基层戒毒单位服务
2		安全运营体系建设	服务期内，从管理、技术、运营三个层面协助省戒毒管理局完成安全运营体系建设，包括不限于以下相关内容：1.安全管理制度；2.安全管理机构；3.人员安全管理；4.系统建设管理；5.系统运维管理；6.运行管理机制。			
3		风险评估服务	按需开展风险评估服务，至少每季度 1 次，2 年至少 8 次。该服务基于目前已有的安全设备以及本项目中设计的终端安全管理系统分析所的数据，为省戒毒管理局提供内部失陷主机、外部攻击、内部违规和内部风险等关键信息安全问题的周期性检测、发现、响应服务。			
4		安全加固服务	按需开展安全加固服务，至少每季度 1 次，2 年至少 8 次。针对省戒毒管理局现有的网络环境、运维人员信息、现有安全策略进行收集分析，需要通过工具及人工的方式进行检测、分析优化。			
5		安全应急服务	按需提供安全应急服务。当安全威胁事件发生后迅速采取的措施和行动，其目的是最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。			
6		漏洞扫描服务	按需开展安全漏洞扫描服务，至少每季度 1 次，2 年至少 8 次。全省戒毒系统现网运行的服务器、终端、网络设备、安全设备、网站及应用系统，可能存在硬件、软件、协议的具体实现或系统安全策略上的缺陷。			
7		渗透测试服务	按需开展渗透测试服务，至少每季度 1 次，2 年至少 8 次。渗透测试范围包括局机关所有信息化基础设施、服务器、操作系统、网络设备以及非涉密信息系统等。			

8		安全攻防演练	服务期内，每年度至少 1 次，2 年至少 2 次，协助提升省局信息化队伍网络安防能力和全体人员安全意识。			
9		安全重保服务	在国庆、两会、春节、重要节假日（如清明、五一、中秋、端午等）、重要会议、极重要业务服务时间段以及局机关要求的期间提供 7*24 小时现场安全值守服务。重大节假日以及戒毒管理局要求的重要保障期间内，除现场驻场的 2 名安全工程师外，可增加二线专家参与现场值班轮班，值班表需提前 5 个工作日报省戒毒管理局报备。			
10	安全培训服务 **（详细要求见“2.2 安全培训服务需求”以及“3.2 信息安全培训服务要求”等相关内容）**	安全意识培训	召开全省视频会议，服务周期内至少 2 次。	1	项	局机关及全省戒毒单位
11		安全产品操作培训	1.培训人数不少于 35 人，省直戒毒单位 2-3 人。 2.每次脱产培训时间 2-3 天。 3.分 2 批组织。	1	项	局机关及省直戒毒单位
12		安全专家 CISP 课程认证培训	1.根据省委网信办对省直机关的网络安全专业技术岗位人员获得网络安全专业资质占比要达到 60%以上的考核标准，培训人数至少 3 人。 2.培训时间不少于 5 天 3.可分批组织	1	项	局机关
二、安全产品						
13	终端安全管理系统 **（详细功能见“2.3 安全产品需求”以及“3.3 安全产品技术要求”等相关内容）**	防病毒软件	1.采用 B/S 架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理、移动存储管理、运维安全管控、报表和查询等功能，以及网络安全准入模块和终端安全态势大屏分析模块。 2.3000 个客户端管理授权，管理端授权不限，含普通 PC 终端和服务器端。 3.三年质保期内所有授权免费国产化授权替代及适配。 4.质保期三年	3	年	内网：局机关一级部署，省直单位二级部署。 外网：局机关外网独立部署。
14		安全运维系统				

3 项目建设内容

3.1 安全驻场等服务要求

3.1.1 驻场安全运维服务要求

3.1.1.1 现场驻场人员的运维服务要求

2 名驻场安全工程师及二线团队要求如下：

人员类别	具体要求
驻场安全工程师安全运营驻场服务 1.高级驻场工程师及中级驻场工程师各 1 人，共 2 人； 2.现场驻场服务共 2 年； 3.二线专家团队服务	自合同签订之日起 2 年； 高级驻场工程师及中级驻场工程师各 1 人，现场驻场服务 2 年，负责安全服务的组织、管理、日常事务性等工作。要求是计算机相关专业，本科或以上学位，具有 2 年或以上、安全服务等工作经验，熟悉网络相关技术，请提供安全服务项目经验及合同证明，加盖公司公章。考取 CISP 证书。
	高级驻场工程师要求有 2 年以上信息安全工作经验，至少具备 1 年及以上渗透测试工作经验，需具备参加省级或以上的护网行动的经验，负责对局科技部门技术人员进行具体技术指导。
	提供工作日 5x8（8:30-12:00,13:00-17:30）的现场驻场服务和提供 7x24 小时电话响应；周六日提供 2x24 小时现场驻场值班轮班；响应要求为，驻场服务期间必须 5 分钟之内到达处理现场，非驻场服务期间在接到服务响应时需 1 小时内到达处理现场；遇特殊情况需要现场安全咨询顾问处理时，不受 5x8 小时服务时间限制。现场驻场工程师需每月提交一份安全月报，描述采购人信息安全总体情况，并协助采购人定制安全评价指标体系，提供展示图表；对重大安全事件，应提交独立报告，详细描述从发现到解决的完整过程。
	在国庆、两会、春节、重要节假日（如清明、五一、中秋、端午等）、重要会议、极重要业务服务时间段以及局机关要求的期间提供 7x24 小时现场安全值守轮班服务。针对出现的任何问题，如果驻场安全工程师无法处理，则提供驻场服务的厂商必须及时协调其他专家支援并在接到电话后 1 小时内到达现场，确保在戒毒管理局要求的期限内解决问题。
	驻场人员的服务工作包括在现场驻场值守、安全运营体系建设、风险评估服务、安全加固服务、安全应急服务、漏洞扫描服务、应用系统渗透测试、安全攻防演练服务、安全重保服务等安全运营驻场服务需求中提到的内容，因人手、技术能力或资质要求无法保障，提供安全驻场服务的供应商必须按照实际情况及省戒毒管理局的要求及时安排二线专家团队进行技术保障，因安排不及时或处置不当造成的不良影响甚至损失的，省戒毒管理局有权依法追究提供安全驻场服务供应商的责任。当需要二线专家团队工程师要提供现场服务，非工作时间，供应商接到省戒毒管理局的应急响应请求后，需在半小时内作出响应，1 小时内派工程师到达省戒毒管理局指定办公地点，若省戒毒管理局发现二线专家工程师没有达到运维要求时，有权要求供应商进行人员更换，供应商商必须响应。上述服务因实际需要增加的人手、二线专家或专业公司服务的所有费用均包含在投标总价中，不得另行收取费用。
	省戒毒管理局可对驻场安全工程师进行考核，省戒毒管理局有权要求变更驻场安全工程师，提供驻场服务的厂商必须在省戒毒管理局要求的期限内补齐满足要求的驻场安全工程师。未经省戒毒管理局批准，驻场服务人员不得中途变更。服务期内，驻场工程师原则上不得更换三人以上。

针对省局的网络设备，要求提供信息安全产品常态化运行维护工作，包括设备运行安全监测、设备运行安全审计、设备及策略备份更新等工作。

1.设备运行安全监测

信息系统运行过程中，可能面临安全产品和其它重要系统运行异常、安全事件的发生等情况，这些情况的出现需要第一时间发现并进行有效处理。

为对安全产品和其它重要系统运行状态进行监测，需每天对网络设备进行至少一次巡检，巡检采用远程登录和本地检查的方式进行，主要巡检内容如下：

a、重要网络设备

序号	服务项	巡检内容
1	设备硬件状态巡检	设备硬件的运行情况：电源、风扇、机箱、各个板卡、flash 卡、状态灯的运行状态等 各个物理端口的稳定性检查 连线情况、标签和标识情况 设备硬件报警信息
2	设备软件状态巡检	系统内核运行状况 是否有新的内核升级程序可以使用
3	设备性能状态巡检	CPU 利用率 内存利用率 网络接口使用率 Buffer 使用情况
4	安全策略检查与优化	安全策略正确性和有效性复核
5	日志检查	日志接收是否正常 日志是否需要满日志处理 日志收集和分析

b、安全设备

序号	巡检项	巡检内容
1	设备硬件状态巡检	设备硬件的运行情况：电源、风扇、机箱、各个板卡、flash 卡、状态灯的运行状态等 各个物理端口的稳定性检查 连线情况、标签和标识情况 设备硬件报警信息
2	设备软件状态巡检	系统内核运行状况 是否有新的内核升级程序可以使用 软件系统版本升级
3	设备性能状态巡检	CPU 利用率 内存利用率 网络接口使用率 Buffer 使用情况
4	安全策略优化	安全策略正确性和有效性复核
5	日志检查	日志接收是否正常 日志是否需要满日志处理 日志收集和分析
5	规则库检查	检查防毒墙等病毒定义升级情况 检查 IDS/IPS 规则库升级情况

c、主机巡检

序号	巡检项	巡检内容
1	主机硬件状态巡检	主机设备硬件的运行情况：电源、风扇、机箱、各个板卡、状态灯的运行状态等 网卡的状态、IP 地址、路由表等信息 磁盘阵列运行状态 系统故障灯显示情况 系统硬件错误报告
2	主机操作系统安全检查	操作系统软件版本情况 Windows 系列补丁安装情况 Linux 系列补丁安装情况 Unix 系列补丁安装情况 操作系统安全配置检查与优化：账户、安全策略、服务等 系统日志分析 补丁安装
3	主机性能检查	CPU 利用率 内存利用率 交换区使用率 磁盘占用空间 I/O 工作情况
4	可疑服务进程检查	开启服务名称 服务开启必要性 服务占用资源情况
5	病毒检查	客户端病毒软件安装情况 病毒定义库升级情况 策略分发情况 病毒处理情况

另外，可以通过部署运维管理平台等系统或工具，对安全产品的 CPU 利用率、内存利用率、磁盘利用率、网络接口连通性等各项功能指标设置告警阈值和告警规则，实时进行监控，及时发现安全产品运行状态异常的情况，如果确认是产品故障则启动故障处理流程。在监测过程中根据实际情况对阈值不断进行调整，最终得到《安全产品运行状态基线》，为安全状态监控提供依据。

2.安全事件告警监控

在巡检过程中出现的事件可以通过人工的方式进行告警，也可以通过安全管理平台进行告警处理。配置安全产品告警规则，对监测到的安全事件按照不同的级别和类型产生不同告警，并将告警信息发送到安全管理平台，通过配置和使用安全管理平台，对各种安全产品产生的安全事件告警通过邮件、弹出窗口等方式通知驻场安全工程师，驻场安全工程师根据安全事件的具体情况采取针对性的处理措施；

3.安全审计

全省戒毒系统部署的安全产品会产生大量的网络访问日志、管理行为记录、操作行为记录、

产品运行记录和网络流量等数据，以及安全监测产生的大量信息，这些信息数量庞大并且无明显关系，但其中可能隐含着潜在的网络攻击行为或已经发生但未发现的攻击行为、产品故障等。安全审计工作是利用安全管理平台等工具，结合资产信息等实际情况，找出这些海量数据中的关联关系，设置各种关联分析规则和过滤条件，挖掘出有价值的网络攻击、运行故障等信息。

4.配置及备份更新

全省戒毒系统的整体安全防护是通过全面落实安全策略、合理配置安全产品防护规则，对来自各网络区域的网络攻击行为进行防护，具体实施方法是通过日常的策略配置、设备升级使安全防护有效发挥作用，通过不断对策略进行优化，提高安全防护效率。同时，通过对安全产品的策略和配置备份等日常维护，保证安全产品的稳定运行，在出现故障时及时恢复，不会严重影响安全防护水平。具体为：

（1）策略配置

按照总体安全策略，分析业务系统实际安全需求和安全产品功能，对安全产品的安全策略进行配置，配置过程遵循策略配置流程，对策略需求进行严格审核。

（2）策略梳理

定期对安全产品的策略配置进行梳理，对冗余的策略和废弃的策略进行梳理，在和业务系统相关人员进行确认后进行删除，提高安全产品运行效率，优化周期最少一月一次。

（3）设备升级

驻场安全工程师定期对安全产品的软件版本和规则库、特征库等进行升级，升级前对原系统进行备份并对升级包进行测试，确保升级后安全产品正常运行，升级周期至少每周检查一次厂商版本更新，更新操作记录备案。

（4）备份恢复

为了保证安全产品出现故障时能够及时恢复，需要定期对产品的配置和策略进行备份，备份内容存放在专用的服务器，并对备份操作记录备案。

在安全产品运行维护过程中，对于新增加的安全设备，同样应纳入到整体运行维护体系中来，在项目实施过程中，安全服务人员有责任完成新增安全产品的到货加电测试、上架、安装配置、优化、后续例行巡检、故障排除和升级等一系列工作。

（5）交付要求

针对所有需要安全产品运维的安全设备输出安全产品运维记录单，该记录单内容是记录了安全产品运行过程中变化情况、出现的问题、问题的解决等。

在服务期内，驻场安全工程师 需每月提交一份安全月报，描述采购人信息安全总体情况，并

协助采购人定制安全评价指标体系，提供展示图表；对重大安全事件，应提交独立报告，详细描述从发现到解决的完整过程。

3.1.1.2 服务商要求

服务商应建立良好的服务管理流程和体系，根据网络中心的实际需求与管理要求安排项目管理人员和技术人员有序的开展服务工作。在服务过程中服务商应做到技术专业、响应及时、管理规范。

服务商应对服务人员进行约束，要求其遵守法律法规、保密规定及合同约定，诚实守信、勤勉尽责，不得将网络中心系统漏洞、架构等情况泄露给外部单位或无关的组织，不得与从事各类黑客活动的个人和组织形成利益输送。

3.1.2 安全运营体系建设

协助建设广东省戒毒管理局信息安全运营体系。广东省戒毒管理局负责整个业务系统的运作，包括开发、实施、维护等，涉及的因素多、对象广、流程复杂，对信息安全管理的要求较高，需要建立较为完善的信息安全运营体系并执行，才能发挥安全技术措施的效果，确保持续的整体安全保障能力；服务商需协助用户方建立完善的信息安全管理制度，结合用户的自身需求与国内相关法律法规及上级单位标准组成，重点对第三方安全管理制度、数据安全管理、数据存储管理等方面建立严格且可执行性强的管理制度，根据省戒毒管理局的网络安全现状，梳理运营管理流程，动态完善运营体系和管理架构。

1.管理层面

（1）明确统一的终端安全运营团队及其职责；

（2）搭建信息安全管理架构，制订完善各项网络安全管理制度。

2.技术层面

（1）制定科学合理的信息安全技术架构，确定终端安全的功能需求、用户场景，选择相应的终端安全产品进行测试；

（2）分阶段部署相应的功能，如资产管理、防毒软件、补丁工具、个人防火墙、终端控制工具、统一 OS 镜像、身份管理、相关审计工具等。

3.运营层面

（1）终端运营团队的常态运营与突发事件响应相结合。处理问题、积累经验；

（2）修订与变更。对网络安全管理制度进行修订。包括部署策略、管控策略、检查、培训、通知、应急响应等；对网络安全场景与手段进行优化，包括脚本开发、功能测试与验证、数据的

查找与溯源，以及对产品的升级、替换与日常支持等。

▲在服务期内，为做好安全运营体系建设服务，供应商需提供便于安全运营管理的系统或工具在广东省戒毒管理局使用，提供与终端安全产品同品牌的安全 USB 设备，安全服务服务人员使用的所有安全 USB 设备需通过公安部的 USB 移动存储介质管理系统类检测，并具备公安部颁发的销售许可证（USB 移动存储介质管理系统），以保证使用的 USB 设备的安全可靠，清除数据方可撤出省戒毒管理局服务，以上所需费用均包含在投标报价中。

工作内容（举例）：

事件类型	具体类型	描述
例行任务	产品运行状态检查	每日检查产品运行情况、病毒库与补丁库日期、授权期限等
	日/周巡检报告	每日/每周的产品巡检报告
	月/年度运营报告	月/年度安装率、正常率、基线合规率数据报告
日常工作	策略配置	产品策略的调整配置
	数据更新	按时完成病毒库、补丁库、授权、系统版本数据的更新
	三大指标提升	终端安装率、正常率、合规率。辅助客户，推动不合规用户的终端状态改进，含客户端或服务端程序的安装与卸载
	热线接听	接听并受理客户关于产品疑问的热线电话
	产品软硬件故障处理	产品使用中问题与 BUG 的处理与跟踪，相关硬件的报修与更换
	漏洞库维护与升级	漏洞库更新，漏洞修复以及漏洞修复衍生问题处理
	病毒库、病毒检测与杀毒支持	病毒库更新，病毒查杀以及衍生问题处理
	解惑答疑	给客户进行产品培训或者解答客户的提问
应急事件	接收/发起应急	接收来自用户紧急事件，或主动发现并发起的紧急事件流程
	应急方案执行	做为一线，接受由终端安全厂家后端二线提供的应急处理方案，并具体执行
多方协同	产品需求的汇总	将用户提出或运营中发现的产品需求进行汇总
	产品需求反馈和跟踪	将汇总的需求，反馈终端安全厂家并跟踪处理进度
	配合调查与取证	配合安全相关的调查与取证，包括对企业 IT 审计的要求
	硬件设备上架	配合相关人员上架硬件设备

	产品测试	现场进行产品的功能测试
	撰写材料	撰写与工作相关的文档、表格、ppt 等材料。

3.1.3 风险评估服务

该服务基于目前已有的安全设备以及本项目采购的的终端安全管理系统分析所的数据，为省戒毒管理局提供内部失陷主机、外部攻击、内部违规和内部风险等关键信息安全问题的周期性检测、发现、响应服务。

深度风险评估服务除了可提供上述检测能力以外，还可以使广东省戒毒管理局建立起内部的安全大数据中心，为后续利用大数据分析技术来开展安全分析、安全数据的基线、安全数据的深度挖掘和安全数据的审计都提供了必要的基础。提升广东省戒毒管理局主动应对新型安全威胁的能力，构建起有效的检测响应机制。

在服务期内，为做好网络安全风险评估服务，供应商需提供正版或具有自主产权的系统或工具在广东省戒毒管理局使用，清除数据方可撤出省戒毒管理局服务，以上所需费用均包含在投标报价中。

本次深度风险评估服务主要包括内部失陷主机检测、外部攻击检测、内部攻击检测、内部违规检测等方面，具体内容如下：

序号	检查内容	检查项	检查要点
1	资产梳理	服务器类型、服务器版本、在线状态、开发语言、开放端口、新增资产、资产变更、新增端口、端口变更等。	资产类型、开放服务及端口识别 资产 Web 应用识别 资产 Web 中间件识别 资产 Web 业务类型识别 资产 Web 开发语言识别 资产服务状态变更监测 资产端口状态变更监测
2	数据库行为分析	数据库服务器敏感操作行为进行梳理，主要可抓取信息包括：源 IP、目的 IP、数据库类型、时间、具体操作行为等。	数据库的内置高危存储过程识别 数据库敏感操作识别 数据库目录遍历、权限提升、非常规操作识别
3	非常规检测分析	针对网络中存在一些非常规类代理进行梳理分析，主要可抓取信息包括：源 IP、目的 IP、代理地址、代理方式、使用次数等。	Regeory Tunnel 识别 HTTP 代理识别 SOCKS 代理识别 TeamView/IRC 识别 非标准端口分析

4	登录行为分析	针对登录行为进行梳理分析，主要可抓取信息包括：源 IP、目的 IP、口令、登录方式、使用频率、来源属地、访问时间、常用登录地址、异常登录地址等。	主动式弱口令探测 基于企业相关信息生成弱口令 暴力破解识别 被动式邮件、WEB 等弱口令探测 通用默认密码检测
5	服务器危险行为分析	对内网服务器存在的高危漏洞服务进行梳理，主要可抓取信息包括：源 IP、目的 IP、up_payload、down_payload 等。	反弹 shell 识别 Redis 命令执行识别 DNS Tunnel 检测 反序列化攻击检测 其他高危漏洞，例如 NSA 等
6	WEB 攻击分析	针对内网中存在的 web 攻击进行梳理分析，主要可抓取信息包括：源 IP、目的 IP、利用模块、攻击方式、结果类型、敏感信息等。	Web 通用弱口令检测识别 弱口令爆破成功识别 Webshell 存在识别 Web 漏洞扫描识别 黑产后门扫描识别 SQL 注入攻击识别 Struts 2 攻击识别 上传行为攻击识别 敏感信息泄露识别 XSS 跨站攻击识别 敏感路径访问识别 远程代码执行识别 XML 实体注入识别
7	威胁情报告警分析	可对 APT 攻击、新型木马进行分析，主要可抓取信息包括：源 IP、目的 IP、木马类型、事件活跃量等。	威胁情报（IOC）告警分析 WEB IDS 告警分析

深度风险评估服务结合广东省戒毒管理局的实际情况，为广东省戒毒管理局提供如下交付物成果：《安全风险评估报告》。

另外，风险评估服务可以满足以下法律法规要求：

（1）满足《中华人民共和国网络安全法》以下要求：

第三十八条 关键信息基础设施的运营者应当自行或者委托网络安全服务机构对其网络的安全性和可能存在的风险每年至少进行一次检测评估，并将检测评估情况和改进措施报送相关负责关键信息基础设施安全保护工作的部门。

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

安全管理员应负责定期进行安全检查，检查内容包括系统日常运行、系统漏洞和数据备份等情况。应根据业务需求和系统安全分析确定系统的访问控制策略；应定期进行漏洞扫描，对发现的系统安全漏洞及时进行修补。

3.1.4 安全加固服务

根据风险评估、漏洞扫描、渗透测试及巡检中发现的问题，提供相应的业务系统加固服务。网站安全加固服务针对重要网站的软硬件技术架构、网站运行状态和最新的安全威胁等因素提高网站安全防护能力，该服务包括但不限于底层操作系统安全、通信安全、网站开发平台、网站日志、网站漏洞补丁和最新安全风险防护等加固工作。

加固内容包括调整策略、修改配置、修改代码、升级补丁等实施，分析单个漏洞形成原因、危害程度、修复方法、分析总体网络架构和系统全局安全性，从而编制汇总形成详细的系统加固解决方案。

安全策略优化是指对安全控制策略是否起到作用、是否合理高效进行检查和改进，可以及时地发现和控制风险。在运维服务的过程中，需要持续地对信息系统各个层面的安全策略进行优化，需要通过工具及人工的方式进行检测、分析、优化。

▲在服务期内，服务商需提供与终端安全产品厂商同品牌的主机安全加固工具，进行主机层面的安全事件工作，主机安全加固工具要求通过了公安部主机安全加固类产品检测，并获得了公安部颁发的销售许可证（主机安全加固类），清除数据方可撤出省戒毒管理局服务，以上所需费用均包含在投标报价中。

安全策略优化服务流程主要包括：现场调研、制定方案、策略优化、编制报告四个阶段工作。

1.现场调研

现场调研主要工作为收集安全设备、网络环境、运维权限及现有安全策略等信息。具体收集信息如下：

信息项	收集内容
安全设备信息	设备名称； 设备负责人； 设备厂商及型号； 管理地址及方式； 物理地址； 设备管理员信息； 用户名口令； 设备白皮书；
网络环境基本信息	网络拓扑图（含设备、IP 地址、网络区域等）； 服务器资产信息； 网络设备资产信息； 业务系统信息；
驻场安全工程师基本信息	驻场安全工程师权限； 维护管理地址；

现有安全策略	访问控制策略； 安全防护策略； 行为审计策略；

2.制定方案

在完成信息收集后，结合全省戒毒系统实际业务安全需求，对现有安全策略进行差距分析，发现策略缺失、策略冗余、策略未废止等问题，并制定相应工作方案开展进一步工作。具体差距分析及工作方案内容如下：

（1）安全策略差距分析

工作项	主要内容
分析用户业务安全需求	汇总业务系统、资产信息； 制定安全防护策略要求；
分析现有安全策略差距	访问控制策略差距分析； 安全防护策略差距分析； 行为审计策略差距分析；
安全策略差距分析总体状况	安全策略差距分析总体状况；

（2）安全策略优化工作方案

工作项	主要内容
安全策略差距分析总体状况	安全策略差距分析总体状况；
策略优化工作方案 a	访问控制策略优化实施方法； 安全防护策略优化实施方法； 行为审计策略优化实施方法；

3.策略优化

在确定巡检对象信息后，依据巡检服务表对设备进行物理巡检及远程巡检，并做好相关记录工作。具体优化内容如下：

（1）访问控制策略优化

序号	服务项	服务内容
1	边界访问控制设备	梳理业务系统访问需求； 按照业务制定访问控制策略，对于策略要明确原地址、目的地址、服务等信息，并表明策略开启工单号、日期、申请人等； 新增缺失的策略、修改较粗的策略、删除冗余的策略；

序号	服务项	服务内容
2	运维管理设备	梳理驻场安全工程师及维护需求信息； 按照所在单位组织结构创建或调整驻场安全工程师，要求明确人员姓名、联系方式等基本信息； 按照业务责任单位创建或调整资产信息，要求明确资产ip地址、所承载业务、物理位置等基本信息； 对每一个驻场安全工程师创建相对应的策略；

（2）安全防护策略优化

序号	服务项	服务内容
1	入侵检测设备	梳理业务系统基本信息； 按照业务系统创建入侵检测防护对象，要求明确所含资产、责任人员等信息； 制定入侵防护策略，应包含入侵攻击类策略、木马病毒累策略、审计累策略等； 针对每个业务系统创建入侵防护策略，可根据业务系统所含资产类型，操作系统类型、软件业务类型对策略进行合理优化；
2	Web应用防火墙	梳理业务系统基本信息； 按照业务系统创建web应用防护对象，要求明确所含资产、责任人员等信息； 制定防护策略，应包含web恶意扫描防护策略、SQL注入防护策略、XSS攻击防护策略、网站挂马防护策略、盗链防护策略、网页篡改防护策略等；

（3）行为审计策略优化

序号	巡检项	巡检内容
1	网络安全审计	梳理业务系统基本信息； 按照业务系统创建业务访问审计策略和管理维护审计策略 ； 业务访问审计策略应能对该业务系统所有被访问的网络行为进行审计； 管理维护审计策略应能对该业务系统所有管理维护网络行为进行审计；
2	数据库审计	理业务系统基本信息及数据库信息； 针对每一个数据库创建审计策略，至少应包含危险指令审计、异常登录审计、异常维护审计、异常工具审计等； 根据业务系统基本信息，创建业务系统对象，并根据不同业务系统创建报表策略，实现针对每个业务系统的生成审计报表；
3	上网行为管理	梳理终端基本信息； 按照所在单位组织结构创建或调整终端用户； 针对所有用户创建上网行为审计策略，应包含邮件审计策略、网站访问审计策略、通讯聊天审计策略、发帖审计策略、关键字审计策略等；

4.编制报告

结合策略优化结果，编制相关安全策略优化报告，并对策略优化过程中发现的重点问题及时通报用户。

针对所有需要安全策略优化的安全设备输出安全策略优化报告，该报告内容是记录了优化前和优化后的策略变化情况。

3.1.5 安全应急响应

现场驻场工程师需要了解零日漏洞、业界新发现的高危安全漏洞、突发安全事件的影响，根据网络设备、网站与信息系统资产指纹库，进行预警，提出遏制和缓解措施。发生紧急安全事件或特殊安全保障任务期间，驻场人力不足情况下，供应商需增派二线团队专业人员应急处置，分析入侵行为，提供最佳防范方法，将情况控制并将损失缩至最小，同时提供入侵事故过程描述并提交相应的防范报告，使广东省戒毒管理局的信息系统在最短时间内恢复正常工作。

1.工作定位

紧急安全事件应急响应，是当安全威胁事件发生后迅速采取的措施和行动，其目的是最快速恢复系统的保密性、完整性和可用性，阻止和降低安全威胁事件带来的严重性影响。此服务主要是为 XX 客户在安全服务期间提供安全事件应急响应服务，并依托大数据分析技术提供互联网层面攻击溯源服务，保障系统平稳运行，维护业务系统的安全。

安全应急响应主要工作包括：

- 分析安全事件原因；
- 基于安全事件提供安全解决方案；
- 基于安全大数据资源，进行互联网层面与本地攻击溯源服务。
- 协助追查事件来源；
- 协助安全事件的后续处置。

2.工作方法与流程

（1）安全事件分类分级响应

应急响应服务通常是根据不同的安全事件类型和安全事件级别，采取针对性的应急响应方式和流程，由相关的人员完成应急响应工作。

（2）应急响应方式

当出现安全事件时，现场驻场工程师在驻场服务期间必须 5 分钟之内到达处理现场，非驻场服务期间在接到服务响应时需 1 小时内到达处理现场。

当发生较大及以上网络安全事件或遇特殊情况时，需要现场驻场工程师、技术顾问、技术专家和资深顾问等应急力量提供技术支撑，不受 5x8 小时服务时间限制。

响应方式：现场驻场工程师提供现场应急支持服务，协调后端资源配合开展应急响应，并通过建立在本地的重点流量采集、存储、威胁分析平台，结合云端威胁情报，进行 APT 攻击与未知威胁事件溯源服务，开展应急响应处置工作。技术顾问技术专家或资深顾问需 1 小时内到现场提供现场支持；项目经理协调有关外部相关部门资源。

3.工作重点

本项工作需要重点做好如下内容：

做好安全事件的分类:由于安全事件种类繁多，对信息系统及用户使用的影响也不尽相同，如果对于安全事件产生不加以区别对待的话，将会造成资源过度投入或者不足，因此，根据长期项目经验，为用户预拟定了安全事件级别分类和响应方式，能够快速准确保障响应服务的到位。

做好安全事件的快速发现及处置：安全事件的快速发现是安全事件应急处置的重要前提，需要及时监控并发现业务系统中出现的安全问题，以便对安全事件进行及时的响应，并在在安全事件响应中准确定位问题所在，及时排查故障，回复业务。

安全大数据与应急工作结合：充分利用安全大数据资源及安全威胁情报信息，有提升未知威胁感知和防御能力，有效防御 APT 等新型攻击，实现早期的快速发现未知威胁的网络行为，攻击源头进行精准定位。

4.工作成果

每次安全事件输出一份《应急响应报告》，并获得省戒毒管理局确认。

3.1.6 漏洞扫描服务

全省戒毒系统现网运行的服务器、终端、网络设备、安全设备、网站及应用系统，可能存在硬件、软件、协议的具体实现或系统安全策略上的缺陷，这些缺陷可能被攻击者所利用从而产生不利影响，这些缺陷就是安全漏洞。

在服务期内，为做好漏洞扫描服务，供应商需免费提供正版或具有自主产权的系统或工具在广东省戒毒管理局使用，清除数据方可撤出省戒毒管理局服务。

通过安全扫描评估，可以及时发现信息系统中存在的安全漏洞，通过对 Windows、Linux 服务器及安全设备漏洞的整改，可以及时地消除安全漏洞可能带来的安全风险。

安全扫描评估主要依靠带有安全漏洞知识库的网络安全扫描工具对信息资产进行安全扫描，其特点是能对被评估目标进行覆盖面广泛的安全漏洞查找，能够真实、全面地反映主机系统、网

络设备、应用系统所存在的网络安全问题和面临的网络安全威胁。

对省戒毒管理局运行的各信息系统内的网络设备、操作系统、应用软件、中间件和服务等进行安全漏洞识别（因工作需要对基层单位进行漏洞扫描的，经省戒毒局审核同意方后进行），详细内容包括不限于以下内容：

(1)网络层漏洞识别

①版本漏洞，包括但不限于IOS存在的漏洞，涉及包括所有在线网络设备及安全设备。

②开放服务，包括但不限于路由器开放的Web管理界面、其他管理方式等。

③空弱口令，例如空/弱telnet口令、snmp口令等。

④网络资源的访问控制：检测到无线访问点。

⑤域名系统：ISC BIND SIG资源记录无效过期时间拒绝服务攻击漏洞，Microsoft Windows DNS拒绝服务攻击。

⑥路由器：Cisco IOS Web配置接口安全认证可被绕过，Nortel交换机/路由器缺省口令漏洞，华为网络设备没有设置口令。

(2)操作系统层漏洞识别

①操作系统（包括Windows、AIX和Linux、HPUX、Solaris、VMware等）的系统补丁、漏洞、病毒等各类异常缺陷。

②空/弱口令系统帐户检测。

③例如：身份认证：通过telnet进行口令猜测。

④访问控制：注册表HKEY_LOCAL_MACHINE普通用户可写，远程主机允许匿名FTP登录，FTP服务器存在匿名可写目录。

⑤系统漏洞：System V系统Login远程缓冲区溢出漏洞，Microsoft Windows Locator服务远程缓冲区溢出漏洞。

⑥安全配置问题：部分SMB用户存在薄弱口令，试图使用rsh登录进入远程系统。

(3)应用层漏洞识别

①应用程序（包括但不限于数据库Oracle、DB2、MS SQL，Web服务，如Apache、WebSphere、Tomcat、IIS等，其他SSH、FTP等）缺失补丁或版本漏洞检测。

②空弱口令应用帐户检测。

③数据库软件：Oracle tnslsnr 没有设置口令，Microsoft SQL Server 2000 Resolution服务多个安全漏洞。

④Web服务器:Apache Mod_SSL/Apache-SSL远程缓冲区溢出漏洞,Microsoft IIS 5.0.printer

ISAPI 远程缓冲区溢出，Sun ONE/iPlanet Web 服务程序分块编码传输漏洞。

⑤电子邮件系统：Sendmail 头处理远程溢出漏洞，Microsoft Windows 2000 SMTP 服务认证错误漏洞。

⑥防火墙及应用网管系统：Axent Raptor 防火墙拒绝服务漏洞。

⑦其它网络服务系统：Wingate POP3 USER 命令远程溢出漏洞，Linux 系统 LPRng 远程格式化串漏洞。

扫描工作流程：

1.提出扫描申请

在扫描开始前，现场驻场工程师以书面形式向省戒毒管理局提出安全扫描评估申请，申请内容应包括：安全扫描评估工作开始时间、结束时间、执行人、扫描 IP 地址范围等相关信息。

2.执行扫描操作

在安全扫描评估申请获得批准后，将非业务高峰期执行漏洞扫描操作。安全扫描评估以网络为基础进行，扫描工具通过网络对被评估对象进行安全评估，因此这种扫描方式会消耗一定的网络带宽资源，并对被评估的对象消耗很小一部分的网络连接的资源，对于其他的资源没有特殊的要求。实际的使用情况表明，网络扫描对网络资源和被评估系统的资源占用在 3%-5%之间，并且可以通过修改、配置一定的扫描策略来使这些资源消耗降低至最小。

在扫描过程中避免使用含有拒绝服务类型的扫描方式，在扫描过程中如果出现被扫描系统没有响应的情况，立即停止扫描工作，与配合的工作人员一起分析情况，在确定原因后，并正确恢复系统，采取必要的预防措施（比如调整扫描策略等）后，才可以继续进行。

3.编制评估报告

安全扫描评估实施结束后，现场驻场工程师将就本次扫描的结果编制安全扫描评估报告，扫描报告应包含以下信息：执行时间、执行人、IP 地址范围、高中低漏洞分布、高中低漏洞列表、漏洞整改方法等信息。

4.漏洞整改

提交的漏洞报告经客户审核后，现场驻场工程师协助对扫描范围内的 Windows、Linux 服务器及安全设备的漏洞进行修复操作，所有修复工作将在客户的监督下进行；对于应用及数据库等漏

洞的加固工作，将提供技术支持。

5.编制处置报告

漏洞加固修复工作完成后，工程师将详细记录漏洞处置的过程并编制漏洞处置报告。

6.交付成果

针对所有进行安全扫描评估的服务器、安全设备等输出安全扫描评估报告及漏洞修复报告，报告内容详细描述安全扫描结果和修复结果。

3.1.7 渗透测试服务

渗透测试服务根据测试的位置不同可以分为内部测试和外部测试。

内部测试是指经过单位授权后，测试人员到达单位工作现场，根据单位的期望测试的目标直接接入到单位的办公网络甚至业务网络中。这种测试的好处就在于免去了测试人员从外部绕过防火墙、入侵保护等安全设备的工作。一般用于检测内部威胁源和路径。

外部测试与内部测试相反，测试人员无需到达客户现场，直接从互联网访问单位的某个接入到互联网的系统并进行测试即可。这种测试往往是应用于那些关注门户站点的单位，主要用于检测外部威胁源和路径。

1.渗透测试服务介绍

渗透测试采用各种手段模拟真实的安全攻击，从而发现黑客入侵信息系统的潜在可能途径。渗透测试工作以人工渗透为主，辅助以攻击工具的使用。

2.渗透测试服务流程

渗透测试服务主要分为五个阶段，包括测试前期准备阶段、信息收集阶段、测试阶段实施、复测阶段实施以及成果汇报阶段：

（1）前期准备阶段

在实施渗透测试工作前，负责项目实施的技术人员会和企业用户对渗透测试服务相关的技术细节进行详细沟通。由此确认渗透测试的方案，方案内容主要包括确认的渗透测试范围、最终对象、测试方式、测试要求的时间等内容，企业用户签署渗透测试授权书。

在测试实施之前，会做到让企业用户对安全测试过程和风险的知晓，使随后的正式测试流程都在企业用户的控制下。

（2）信息收集阶段

通过安全测试工具进行信息收集，内容包括：操作系统类型收集；网络拓扑结构分析；端口扫描和目标系统提供的服务识别等。

（3）测试实施阶段

在测试实施过程中，测试人员首先使用自动化的安全扫描工具，完成初步的信息收集、服务判断、版本判断、补丁判断等工作。

然后由人工的方式对安全扫描的结果进行人工的确认和分析，并且根据收集的各类信息进行深入渗透测试，测试人员在获取到普通权限后，尝试由普通权限提升为管理员权限，获得对系统的完全控制权，此过程将循环进行，直到测试完成。

测试人员需整理渗透测试服务的输出结果并编制渗透测试报告，最终提交企业用户和对报告内容进行沟通。

（4）复测阶段

在经过初次渗透测试报告提交和沟通后,等待企业用户针对渗透测试发现的问题整改或加固。经整改或加固后，测试人员进行回归测试，即二次复测。复测结束后提交给企业用户复测报告和对复测结果进行沟通。

（5）成果汇报阶段

根据初次渗透测试和二次复测结果，整理渗透测试服务输出成果，最后汇报项目领导。

3.渗透测试服务方法

（1）信息收集

信息收集的方法包括主机网络扫描、端口扫描、操作类型判别、应用判别、账号扫描、配置判别等等。入侵攻击常用的工具包括 nmap、nessus 等，有时，操作系统中内置的许多工具（例如 telnet）也可以成为非常有效的攻击入侵武器。

（2）口令猜测

口令猜测也是一种出现概率很高的风险，几乎不需要任何攻击工具，利用一个简单的暴力攻击程序和一个比较完善的字典，就可以猜测口令。

（3）Web 脚本及应用测试

Web 脚本及应用测试专门针对 Web 类服务及数据库服务器进行。OWASP 最新的技术统计显示：脚本安全漏洞为当前 Web 系统最严重的安全弱点之一。利用脚本相关弱点如跨站脚本攻击、SQL 注入等攻击方法，轻则可以获取系统其他目录的访问权限，重则将有可能取得系统的控制权限。

（4）业务逻辑测试

对关键业务逻辑进行测试，检查业务流程中是否存在相互矛盾或使用了脆弱验证方法控制业

务。通过该方法可以测试出相关业务设计/架构人员的安全意识，并可以为深层次的渗透提供方法与思路。

（5）其它

为模拟真实的攻防环境与场景，渗透测试中不排除使用一些其他的黑客入侵思路。

在服务期内，为做好渗透测试服务，**供应商**需免费提供正版或具有自主产权的系统或工具在广东省戒毒管理局使用，清除数据方可撤出省戒毒管理局服务。渗透测试方法包括但不限于信息收集、端口扫描、口令猜测、远程溢出、本地溢出、企业用户端攻击、中间人攻击、web 脚本渗透、B/S 或 C/S 应用程序测试、社会工程、脚本测试、权限获取，最大限度的地挖掘如 SQL 注入、远程命令执行、Struts2、越权、webshell、逻辑错误、跨站、弱口令等漏洞，并对测试结果进行验证。渗透测试需提供专业漏洞修复方案，协同进行修复指导，并提供复测验证修复情况。

3.1.8 安全攻防演练

通过应急演练方案设计，并每年组织一次安全应急演练，提高省戒毒管理局对信息安全事件的应急储备能力。服务商在本项服务中需制定并完善安全应急演练方案，作为安全应急演练的组织者，按照应急响应流程及预案，组织应用系统运维服务商模拟突发网络与信息安全事件，验证应急预案中：事件分级分类、组织结构及职责、预防和预警机制、应急处理流程、应急响应保障措施合理性，并对不合理给出整改意见。

1.应急演练整体流程

在完善安全整改工作后，组建防守方和攻击方进行实际的演练攻击，攻击方采用各种技术手段模拟黑客攻击，发起各类攻击事件，防守方检测和发现外部攻击，并对攻击采取相应的防护措施，导演方负责演练导演、监控进程、全程指导、应急处置、演习总结、技术措施与策略优化建议等技术咨询工作。通过攻防演练，通过实战，真刀真枪的检验省戒毒管理局的安全产品、安全策略、安全体系、人员能力和协同处置等多方面内容

总体的应急演练的基本流程主要包括如下阶段：

- 准备阶段
- 监测及事件分析阶段
- 事件处理阶段
- 结束响应阶段
- 总结及预警阶段

（1）准备阶段

包括了人员、组织的准备以及技术的准备，技术准备主要是要建立监控管理的技术体系和平台，为事件发生后的技术分析，及时的通告和响应等提供条件和保障。同时，尽可能地在事前做好相应的安全防范工作，准备好进行应急处理的技术工具等内容。

（2）监测及事件分析阶段

监测人员通过手动监测方式以及在准备阶段建设好的安全运行管理中心的监测方式，监测是否有异常现象的发生；当发生异常情况时，根据异常的性质与影响，决定是否向相关人员进行报告。上报方式除了通常的电话外，还可以利用安全运行管理中心平台中的告警机制，根据告警级别的不同，通过工单、邮件、短信的方式上报和通知到相关人员。

上报到应急响应管理小组后，对异常情况进行分析，判断事件类型，识别攻击的性质以及攻击强度，同时根据事件影响决定是否报告网络与信息安全工作小组；在必要的时候，向公安机关报案以获得帮助；

（3）事件处理阶段

根据事件的不同，采取不同的处理方案，启用相应的专题应急预案，对于常见的、主要的事件类型，需在预案中设计两个典型场景应急演练流程，如需其他场景，需要后续根据实际情况中进行调整。该阶段中的技术处理主要为抑制事件的影响，并进行根除。

（4）结束响应阶段

网络与信息安全工作小组根据之前判断的攻击信息，采取必要的技术手段控制攻击行为、恢复系统服务并对攻击的来源进行追踪；必要时向公安机关通报相关信息，对攻击者进行抓捕。

（5）总结汇报阶段

当攻击事件结束后，系统恢复正常，由网络与信息安全管理小组对整个事件进行总结分析，向网络与信息安全领导小组进行汇报；网络与信息安全领导小组组织相关人员就本次事件总结经验教训，同时从中总结预警方案和内容，一方面进一步改进和完善应急响应体系，另一方面在公司内部的发布渠道上，适时发布总结后的预警信息，从而逐渐完善信息安全的整体安全保障能力。

2.应急演练场景模拟

（1）应急演练流程

现场驻场工程师按照应急预案制订规范的、可操作性的、接近实战的应急演练流程。

（2）事件处理程序

- 现场驻场工程师对系统运行情况进行监控,并从各现场其他值班人员/用户端反映的情况中分析，判定为疑似计算机病毒爆发事件；
- 现场驻场工程师将疑似计算机病毒爆发事件通报给驻场服务工程师和相关系统管理员；

由驻场服务工程师判定是否为计算机病毒爆发事件；由相关系统管理员判定是否为系统自身应用故障；

- 如果是系统自身应用故障，则相关系统管理员应立即启用该系统自身应用故障情况下的应急预案；
- 如果是计算机病毒爆发事件，则驻场安全工程师应立即按照省戒毒管理局总体应急预案执行通报；同时驻场服务工程师应判断该病毒是否具备网络传播性；
- 如果该病毒具备网络传播性，驻场服务工程师应和被感染病毒系统的系统管理员联系，明确是否可以将被感染病毒主机进行网络隔离；
- 如果可以将被感染病毒主机进行网络隔离，相关系统管理员应立即启用被感染病毒主机系统网络连接完全断开情况下的应急预案；
- 驻场服务工程师协同终端安全产品的防病毒专家一起制定病毒查杀方案；并分析病毒查杀方案可能对系统原有数据产生的破坏性；
- 如果病毒查杀方案会对系统原有数据产生破坏,则由系统管理员进行必要的系统备份后，再由驻场服务工程师和防病毒专家一起进行病毒查杀工作；否则可以由驻场服务工程师和防病毒专家直接进行病毒查杀工作；
- 完成病毒查杀工作后,驻场服务工程师和防病毒专家对原被感染病毒主机进行病毒分析，判定是否仍然存在病毒；如果仍然存在病毒，则继续制定新的病毒查杀方案，否则可以恢复原被感染病毒主机的网络连接；
- 被感染病毒主机的网络连接恢复后，驻场安全工程师按系统恢复事件，执行通报流程。

（3）预案处置操作检查单

序号	预案执行关键点	执行效果	意外描述（执行失败时填写）	检核人
1	现场驻场工程师发现疑似计算机病毒爆发事件	□成功 □失败		
2	驻场服务工程师和系统管理员对疑似计算机病毒爆发事件进行正确的判定	□成功 □失败		
3	驻场服务工程师按照按照省戒毒管理局应急预案完成通报	□成功 □失败		
4	驻场服务工程师应和被感染病毒系统的系统管理员联系，并对是否能够将被感染病毒主机进行网络隔离作出正确判定	□成功 □失败		
5	完成病毒查杀后，驻场服务工程师和系统管理员应对系统是否还存在别的病毒进行进一步检查	□成功 □失败		

（3）服务结果输出

根据实际的应急演练情况输出：《XX 安全事件应急演练报告》

3.1.9 安全重保服务

1.服务内容

在国庆、两会、春节、重要节假日（如清明、五一、中秋、端午等）、重要会议、极重要业务服务时间段以及局机关要求的期间提供 7x24 小时现场安全值守服务。

▲在服务期内，服务商需提供检测工具，检测工具要求具备公安部颁发的销售许可证（Wi-Fi 网络数据链路层入侵检测产品类），以满足以上重要事件期间的安全保障工作，清除数据方可撤出省戒毒管理局服务。

主要服务安排如下：

事前服务：重大节假日开始之前，对服务范围内的重要系统进行全面安全检查，并协助进行安全加固，并对安全加固的结果进行复测，确认安全问题的及时有效的修复；

事中值守：

- 在重大节假日期间提供增强的安全运维服务，包括至少额外增派 1 名经验丰富的专家进行现场值守。
- 安全职守时间，自重大节假日前 1 周到该节假日结束为止。

事后服务：在重大节假日提供重要时期安全保障服务后进行安全保障工作的总结，于 1 周内提供《重要时期安全保障服务报告》。

2.服务流程

为了保证省戒毒管理局在重大节假日时期的安全，专门设计了以安全保障为核心的服务，该服务覆盖事前、事中、事后三个重要环节的监测预警、安全测试、事件发现等，贯穿预警、防护、监控、响应全过程。保障省戒毒管理局信息系统持续的安全，在影响发生前降低风险，在事件发生后及时发现、解决问题。

- 事前服务

（1）资产发现与实时漏洞监测

为了应对瞬息万变的网络安全形势，尽可能实时的发现企业在互联网上暴露的资产信息与变更情况，推出资产发现与实时漏洞探测服务，主动探测用户在外网上暴露的资产，可以形成明确的资产清单。可帮助用户发现自己的未知资产。根据资产发现的结果进行精准漏洞扫描，可针对

特定漏洞准实时进行全面排查。

（2）最新安全动态通告

对于近期影响广泛的重大安全事件如：高危系统漏洞、高危蠕虫病毒、恶劣入侵与攻击等，我们将在第一时间通知省戒毒管理局相关人员，同时提供事件类型、影响范围、如何解决（对于还没有彻底解决方法时，我们将提供临时解决方案）、如何预防等全方位详细情况通告。

（3）检测前评估、加固协助与测试

在重大节假日开始之前完成对服务范围内的重要系统进行全面安全检查。因为安全不是绝对的，风险事件的发生率也不可能为零，风险只能通过对信息系统脆弱性采取一定措施的方式进行处理。风险的处理方式有以下四种：避免、转移、降低、和接受，但不可能完全被消灭。

- 避免，指通过不继续进行可能产生风险的活动来避免风险（在可行的情况下）；
- 转移，涉及承担或分担部分风险的第三方，包括使用合同、保险以及合伙，合资等组织结构；
- 降低，通过采取相应的风险控制措施、安全机制来降低风险；
- 接受，在风险降低或转移后，可能还有剩余的风险，完全的零风险是不可能的，而且降低风险的成本随着风险的降低而增大，必须考虑处理风险的成本与所得到的利益相称，因此特殊保障期间应该根据实际情况接受一定量可以承受的风险。

根据在重大节假日开始之前安全评估的结果，对服务范围内的系统进行安全加固协助，并对加固后的系统进行二次安全评估，确保重大节假日开始之前的安全状况符合省戒毒管理局的安全要求。

- 事中现场职守

（1）安全监控

针对根据安全集成所部署的相关安全产品，项目要求提供 7*24 小时的安全监控，监控内容包括：

- 全部安全产品(包括防火墙、Web 应用防火墙、IDS/IPS、负载均衡、网页防篡改系统、网络安全审计系统等等)实时告警监控和每天日志分析；
- 防病毒软件监控与查杀记录；
- 对应用系统、数据库系统的状态和业务平台如关键的 Web 服务日志进行监控和日志分析。
- 接受安全预警、告警，及时避免风险或根据需要指导维护工作；

（2）事件响应

项目要求提供的紧急响应服务提供高效的信息安全事故反应体系以帮助省戒毒管理局尽快对

突发的信息安全破坏事故作出反应。重大节假日期间的安全事件发生后，安全职守工程师以现场支持的方式提供服务，包括事故处理及恢复、事后的事故描述报告以及后续的安全状况跟踪。

当省戒毒管理局的主机或网络正遭到攻击或发现入侵成功的痕迹，现场驻场工程师无法当时解决和追查来源时。安排二线专家团队需在收到通知后 1 个小时内赶到现场，协助省戒毒管理局解决问题，查找后门，保存证据和追查来源，共同完成对省戒毒管理局网络安全事件的紧急响应和处理。

对于省戒毒管理局信息系统应急响应服务内容包括：

- 调查事故原因；
- 分析事故；
- 提出解决方法；
- 实施并解决事故，避免以后发生类似情况；

如果由于人为恶意破坏，导致突发事故的，协助追查导致事故的人员，配合省戒毒管理局，必要时配合执法部门一起追查事故发起者；

在事故处理后两天内向省戒毒管理局提交详细的文档记录，根据事故分析，事故记录，解决问题，追查方案等形成专题报告。

- 事后服务

在重大节假日结束之后进行重要期间安全保障服务的总结，于 1 周内提供《重要期间安全保障服务报告》。

- 服务结果输出

每周期的重保服务输出一份《XX 重要时期安全保障服务报告》。

3.2 安全培训服务要求

本次项目涉及的安全培训服务要求供应商保证提供并安排有经验的教员以及适当的培训课程、设施、地点和有关教材，使客户在培训后在日常操作和预防性维护以及对所有设备的故障搜寻和维修方面，都有足够的知识，能够独立地对系统进行日常管理和维护，对安全事件能做基本的处理。培训实施方案需由省戒毒管理局审批同意后方可执行。具体要求如下：

1.培训教材应使用简体中文。

2.培训内容：安全意识培训，安全产品操作培训，安全专家 CISP 课程认证培训。

3.供应商应提供包括培训计划以及培训大纲。在相关附件里，应详细列出所设置的课程教材目录，注明每次课程的内容和目的以及每次课程的文件和资料，并注明每次培训课程的时间、地点及课时。

4.培训对象：局机关以及基层单位的工作人员培训。安全意识培训主要针对全省戒毒系统全体干警职工，以视频会议的形式开展；安全产品操作培训主要是针对部署了本项目安全产品的局机关及省直单位科技部门技术人员，分 2 批开展，每批脱产 2-3 天，计划 5 天完成；根据省委网信办对省直机关的网络安全专业技术岗位人员获得网络安全专业资质占比要达到 60%以上的考核标准，安全专家 CISP 课程认证培训主要是安排局机关至少 3 名技术人员参加培训，培训时间不少于 5 天，可分批组织。

5.授课教师要求：教员不仅要有理论知识，也要有实际工作经验；培训的教员是原厂商或拥有原厂商认证的教员。

6.时间：供应商应在投标文件中拟定培训的时间安排；培训课程应安排在招标人整个项目计划的合适时间段内，开课时间最迟不超过招标人发出开展培训通知后的一个月。安全意识培训主要以视频会议的形式开展；安全产品操作培训分 2 批开展，每批脱产 2-3 天，计划 5 天完成；安全专家 CISP 课程认证培训培训时间不少于 5 天，可分批组织。

7.费用：供应商应详细列明培训所需的各项费用标准，包括培训费、教材费、场租费等其它与培训相关的费用。

3.3 安全产品技术要求

本次项目涉及的安全产品终端安全管理系统要求具备以下功能：

功能项	功能描述
系统管理	★控制中心：采用 B/S 架构管理端，具备设备分组管理、策略制定下发、全网健康状况监测、统一杀毒、统一漏洞修复、网络流量管理、终端软件管理、硬件资产管理、移动存储管理、运维安全管控、报表和查询等功能，以及网络安全准入模块和终端安全态势大屏分析模块。
	控制中心部署在硬件环境为CPU数量4核以上;内存高于4GB;硬盘高于500GB;操作系统为 Windows Server 2008 R2/2012/2012 R2/2016 的 64 位版本（简体中文版）的服务器上；
	客户端（含 PC、服务器）：与安全控制中心通信，提供控制中心管理所需的相关数据信息；执行最终的木马病毒查杀、漏洞修复等安全操作。
	支持根据分组、计算机名称、IP 地址、操作系统、在线状态等条件的组合筛选出符合条件的终端进行管理；（提供产品界面截图）
	支持加密的控制中心远程访问，支持管理账户并发、密码有效期、鉴别失败锁定等设置；（提供产品界面截图）
	支持控制中心数据恢复与备份
资产管理	按终端维度展示终端的硬件、软件、操作系统、网络、进程等信息；可监控 CPU 温度、硬盘温度和主板温度
	支持统计指定分组或全网的终端扫描数、终端管理软件安装数、未安装终端数及安装率。
	支持自动发现设备的 IP-MAC 地址的绑定（提供产品界面截图）

		支持插件清理，按插件显示展示全网存在的插件和涉及的终端，可清理指定或全部插件、加入信任；按终端显示展示全网每个终端存在的插件，可清理插件（提供产品界面截图）
		▲支持正版软件(指定)的正版序列号的读取功能，确保软件正版化。（提供产品界面截图）
		支持终端态势可视化大屏，支持通过三维可视化能力对终端安全进行呈现，呈现内容包括终端部署情况，终端资产情况等大屏（提供产品界面截图）。
日志报表		展示全网终端健康状态、报警信息；可方便的查看不健康、亚健康终端列表；展示全网终端木马库日期比例，可方便的查看全网终端木马库的情况；展示全网终端病毒库日期比例，可方便的查看全网终端病毒库的情况
		展示指定时间段内指定终端修复漏洞，病毒查杀，木马查杀的情况（提供产品界面截图）
		▲支持邮件报警，可以设定多种触发条件，满足条件后自动发送邮件通知到相关人。邮件触发条件至少包括：一定时间内的病毒数量阈值、一定时间内的未知文件数量阈值、重点关注的终端发现病毒、病毒库超期等（提供产品界面截图）
		支持大数据引擎系统，可将全网终端日常运维数据汇聚存储分析，并根据客户运维管理所需的要求定制报表
设备联动		▲支持与 NGFW、上网行为管理、VPN 产品联动，达到网关边界联动防御效果（提供产品界面截图）
病毒、恶意代码、木马防护	内存防护	支持内存实时监控查毒，能够自动隔离感染而暂时无法修复的文件；
	启动防护	支持抢先加载防毒，在系统未加载前启动文件监控，通常情况下不必重启到安全模式也能清除病毒。
	注册表、引导区防护	支持文件、引导区、内存、注册表、服务、进程、进出文件、目录、压缩文件、网页等恶意代码、恶意样本查杀。
	电子邮件防护	支持电子邮件内文件检测，可清除隐藏于电子邮件计算机病毒和恶性程序。
	网页防护	能够对网页提供安全防护，发现网页中的危险行为实时阻断；能够对网页挂马进行拦截，能够自动拦截网页中的钓鱼、欺诈信息。
	网络防护	拦截下载器自动下载木马程序；拦截恶意推广程序；拦截黑客远程控制本机；拦截盗号木马。
	移动设备病毒防护	提供 U 盘等移动设备接入电脑自动检测功能，全面拦截和清除在移动设备接入系统可能带来的病毒木马；
	局域网共享查杀	能够对局域网共享文件传输进行检测和查杀；
	浏览器防护	▲支持浏览器防护，对篡改浏览器设置的恶意行为进行有效防御，并可以锁定默认浏览器设置（提供产品界面截图）
	聊天安全防护	检测 QQ、MSN、阿里旺旺等常用聊天软件传输文件的安全性，确保传输文件不中毒；检测 QQ、YY、飞信等聊天软件中对方发来网址的安全性（提供产品界面截图）
		聊天软件传输某些文件会添加“.重命名”，如果文件安全，将自动去除“.重命名”（提供产品界面截图）
	定时查杀	能够自定义时间、自定义扫描频率，自定义扫描类型，对终端进行定时查毒，并且可以自定义查杀病毒后的处理方式自定义；

	黑白名单例外	支持文件、目录和数字签名自定义黑白名单的方式来管理全网终端的文件；
		▲支持手工导入 MD5+SHA1 的黑白名单方式，支持 txt 批量导入方式；（提供产品界面截图）
		文件被加入白名单，客户端不再查杀，加入黑名单，客户端不可执行此文件；
		支持对 windows/Linux/国产操作系统终端的文件黑白名单和信任区在服务端统一管理;（提供产品界面截图）
	病毒查杀统计	支持按病毒、木马、终端等维度统计全网病毒感染状况；
		支持对网内未知文件云查询的控制，可以选择直接连接互联网云查询中心查询，也可以选择采用私有云查杀引擎完成未知文件查询；
		上报文件至少包括:文件名称、发现时间、鉴定结果、文件大小、数字签名和文件所属源计算机等信息
	漏洞利用防御	能够支持漏洞利用防御，尤其对通过文件漏洞（尤其是 0day 漏洞）的攻击行为进行有效检测与防御；（提供产品界面截图）
	压缩包杀毒	支持文件解压缩病毒查杀，支持对 zip、rar、7z 等多种格式的压缩文件查杀能力；可对压缩包层级设置以节省终端计算资源；（提供产品界面截图）
	宏病毒查杀	有针对宏病毒的专杀模块；
	备份区隔离区管理	可对备份区、隔离区的文件进行有效管理。能够对单个、指定的文件和全部文件，进行文件的删除、恢复等多项管理措施。
	敲诈者病毒防御	对敲诈者病毒提供防护机制。（提供产品界面截图）
	多杀毒引擎	产品具备本地多引擎查杀能力
	程序自身安全	控制中心自身具有抵抗各种渗透攻击的安全机制；
	样本库数量	支持私有云查杀
	Linux、国产操作系统杀毒	▲支持 linux、国产操作系统杀毒（提供至少 4 个国产化操作系统厂商的兼容性认证证书）。
	XP、Win7 防护	支持针对 Windows XP、Windows7 系统可带来安全隐患的设计机制进行加固性修复.
	病毒库升级管理	支持客户端升级时对网络带宽的保护，可以设定服务器端最大升级带宽。（提供产品界面截图）
	数据分析与采集模块	▲实现对终端安全产品的报表配合进行数据下钻分析，呈现终端安全概括、态势等内容。（提供产品界面截图）
补丁分发与漏洞修复		产品具有定时修复漏洞功能，同时可以设置筛选高危漏洞、软件更新、功能性补丁等修复类型；
		▲支持设置对特定分组优先进行补丁分发，一段时间后再全网升级（提供产品界面截图）
		终端支持智能屏蔽过期补丁、与操作系统不兼容的补丁，可以查看或搜索系统已安装的全部补丁；（提供产品界面截图）
		产品具备漏洞集中修复，强制修复，自动修复；具备蓝屏修复功能（提供产品界面截图）

		产品具备漏洞集中修复过程中的流量控制和保证带宽,补丁分发支持服务端带宽限流与客户端 P2P 补丁分发加速，有效节省外网带宽资源（提供产品界面截图）
运维管控	流量管理	可统计指定终端网络、应用程序的上传，下载速度与流量；
	应用程序安全	支持终端进程红名单、黑名单、白名单功能，可设置核心进程必须运行，也可保护核心进程不被结束。
	网络安全防护	支持网址白名单，通过信任网址白名单可以管理网络内信任的网址，加入信任后终端不再将此网址视为威胁
		支持网址黑名单，可设置终端不能访问的网址 URL，终端访问这些 URL 时会被拦截，并展示拦截记录
	外设管理	支持对终端各种外设（USB 存储、硬盘、存储卡、网卡、光驱、打印机、扫描仪、摄像头、手机、平板等）、接口（USB 口、串口、并口、1394、PCMIA）设置使用权限
	桌面安全加固	支持对终端桌面系统的账号密码、本地安全策略、控制面板、屏保与壁纸、浏览器安全、杀毒软件检查
	管控策略	支持远程协助终端（不依赖 Windows 远程桌面协议）、远程关机、重启终端；
		支持远程操作时锁定屏幕、截取屏幕，远程锁定屏幕后需要输入解锁密码才可再次使用；
		支持按照域名、操作系统、WIFI SSID 等条件匹配预先设定好的场景策略；
		支持 LDAP 账号的终端用户策略模式；（提供产品界面截图）
移动存储介质管理		支持管理员对入网的移动存储介质进行注册，可以对已注册的移动介质进行管理，包括学习注册、授权、启用、停用、删除、取消注册、导出注册列表等（提供产品界面截图）
		▲支持客户端自主申请移动存储介质注册，管理员统一对申请进行审批；支持管理员设置自动审批客户端注册请求；
		支持移动存储介质读写权限划分设置，有效控制不明来历的移动存储可能带来的病毒传播等隐患
		支持移动存储介质外出管理，并可以设置外出使用权限以及外出使用次数与有效时间；
		▲支持提供同一品牌的硬件安全 U 盘与终端安全管理系统联动。（提供产品界面截图）
终端准入		支持旁路终端准入部署方式，避免串行设备部署单点故障； 支持有线、无线基于应用协议准入方式，准入配置支持保护服务器区域、例外终端等灵活的配置方式 支持标准 802.1X 准入，支持动态 VLAN、动态 ACL 下发；
		客户端连不上控制中心之后禁止接入任何网络
		▲支持 802.1X 认证技术上基于终端快速认证，与终端管理客户端联动无需输入账号快速入网，避免重复输入账号口令。（提供产品界面截图）
		支持 AD、LDAP、Email、HTTP、本地等多种方式认证源统一认证管理。（提供产品界面截图）
		支持入网健康检查策略，策略检查项至少包括：远程桌面、U 盘自动运行、防火墙、IP 获取方式、文件共享、屏幕保护、空密码、IE 代理；支持终端修复向导，对不合规的终端提供软隔离，并进行修复向导和一键修复功能
产品厂商需提供		▲提供全球 IPv6 Ready 测试中心出具的认证证书。

	▲提供公安部颁发的《计算机信息系统安全专用产品销售许可证》内网主机监测（一级）、网络版防病毒产品（一级品）安全专用产品资质证书。
	▲提供该软件产品的软件著作权，并提供相关的《计算机软件著作权登记证书》资质证书。
	▲提供公安部颁发的《计算机信息系统安全专用产品销售许可证》终端接入控制（一级）安全专用产品资质证书。
★质保期管理及服务	1.要求提供三年原厂服务（包含软件升级，全功能模块使用升级、特征库升级，硬件维保，技术支持、安装实施） 2.3000 个客户端管理授权，管理端授权不限，含 PC 终端、服务器涉及的所有相关的功能模块、软件等所有授权。 3.三年质保期内所有授权免费国产化操作系统的授权替代及适配。 4.需预留未来与上级部门或省直单位系统及设备对接的接口，在三年质保期内免费接入。

4 提交的成果

4.1 提交的成果文档

本项目应提交包括但不限于以下项目成果：

安全管理制度体系类交付文档，包括不限于：网络安全工作总体方针和安全策略、物理安全管理制度、网络安全管理制度、主机安全管理制度、应用安全管理制度、数据安全管理制度、设备操作规程、制度制定、发布、评审和修订管理制度、安全管理组织制度、授权和审批管理制度沟、人员管理制度、信息安全培训管理制度、外部人员访问管理制度、网络与信息系统安全设计制度、软件开发管理制度、代码编写安全制度、外包软件开发管理、工程实施管理制度、服务供应商安全管理、机房安全管理制度、办公环境保密管理、信息资产和设备管理制度、信息系统风险管理制度、系统安全管理制度、恶意代码防范管理制度、配置变更管理程序、账户权限、口令管理制度、保密管理制度、数据备份与恢复管理制度、安全事件报告和处置、信息安全应急预案、信息安全外包运维管理制度。

安全服务类交付文档，包括不限于《项目实施方案》《安全现状调研报告》《网络安全规划报告》《安全管理体系规划报告》《物理安全建设方案》《区域边界安全设计方案》《通信网络安全设计方案》《计算机安全设计方案》《安全管理中心设计方案》《安全管理体系设计方案》《信息安全资产梳理表》《信息系统梳理表》《信息系统漏洞扫描报告》《信息系统漏洞扫描清单》《安全产品运行状态基线》《应用系统渗透测试报告》《信息安全安全整改报告》《安全风险评估报告》《风险威胁报告》《流量监控报告》《安全值守授权书》《安全值守任务清单》《安全值守日报》《XXX 事件应急响应报告》《应急演练方案》《XX 安全事件应急演练报告》《XX 重要时期安全保障服务报告》《安全培训相关文档》《安全运维报告》《XX 设备安装调试报告》《XX 设备试运行报告》《初验报告》《终验报告》等。

中标人根据以上交付文档，建立省戒毒管理局网络安全知识库，定期更新完善。

4.2 提交文件形式及版权要求

4.2.1 提交件形式

本项目最终咨询成果将以电子文档并纸质文件提交。

1.电子文档：所有电子文档中标人应以PDF文件格式及WORD文件格式提交。

2.纸质文件：中标人应在项目完成时，将本项目所有文档、资料汇集成册交付给采购人，所有文件要求用中文书写或有完整的中文注释。验收后，中标人按国家、省以及采购人档案管理要求，向采购人提供装订成册的纸质文档至少 1 套，电子文档1套。

4.2.2 资产归属

1.本合同不会引起任何已申请、登记的知识产权所有权的转移。

2. 供应商需承诺，本合同所涉服务成果的知识产权归属按下列第（2）种方式处理：

（1）成交供应商为履行本合同义务所形成的服务成果的知识产权归采购人所有。

（2）采购人基于本合同约定委托中标人定制开发的产品、程序、服务，以及定制的方案、规划、制度性文件等的知识产权归采购人、中标人共同所有，中标人应按采购人书面要求交付该共有部分的成果；中标人在共有部分的基础上进行二次研究的及对二次研究形成的产品、程序等财产进行处置的，需经采购人书面同意，二次研究所形成的产品、程序、服务，以及方案、规划、规范性文件等的知识产权归研究者所有，共有部分仍归采购人、中标人共同所有。

3.本合同所涉及的数据、系统、数据服务所有权归省戒毒管理局所有。中标人只能用于履行本合同之义务。

4. 供应商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。

4.2.3 其他要求

供应商须书面承诺，必须基于广东省“数字政府”网络安全体系建设总体规划思路及广东省“数字政府”网络安全体系建设运营实践经验开展安全服务，并遵循采购人所制定的相关管理办法和要求，根据相关指引提供安全服务。

5 工期、项目管理及其他服务要求

5.1 项目工期进度要求

本项目属于省戒毒管理局网络安全驻点服务及安全产品采购实施建设实施项目，驻点服务总服务周期 2 年。

时间要求：中标通知书发出后 5 天内发起合同签订流程，产品安装调试（含总体联调）2 周，安全服务周期 2 年。签署合同后 30 天内交付安全服务实施方案；以上天数定义为日历日。安全服务内容按照 2 年为一个服务周期提交相关项目成果物。

5.2 组织实施要求

为使项目按质、按量、按时及有序实施，供应商应按照成熟的项目管理模式及配套管理办法要求，建立完善、稳定的项目团队、内部组织管理方式及管理机构、协调机制、技术基础，支撑保障要求及其他相关要求。在项目日常管理和条件保障方面，从行政组织、后勤保障和支撑条件各方面创造良好的服务环境，确保项目的顺利实施。

5.3 质量保证要求

为保证本项目能按时高质的顺利完成，规避项目风险或将风险降至最低程度，中标人应建立项目质量管理体系，包括但不限于质量目标、质量指标、岗位责任、问题处理计划、质量评价、整改完善等内容，并建立奖惩制度。

5.4 人员管理

5.4.1 项目经理要求

供应商须书面承诺，如在项目实际执行过程中发生项目经理不能按采购文件要求胜任相关工作的，采购人有权要求更换项目经理，供应商必须在两周内调整为符合采购文件要求且能胜任相关工作的项目经理并到位开展工作，否则采购人有权终止合同并报相关管理部门进行处理。应指派固定的团队为本项目提供专业服务，服务团队成员不得少于 5 人。

本项目需配备项目经理进行沟通协调、工作安排和项目汇报。配备专业的远程专家服务团队，支持驻场人员进行现场工作的实施解决。协助驻场人员进行其他网络及信息安全相关工作。

在成交供应商项目组成员应严格遵守采购方的相关工作管理规定，如有违反规定的，经采购方通报成交供应商后，将按采购方的有关规定予以处理。

5.4.2 驻场人员工作职责

提供相应的驻场安全服务，为省戒毒管理局局机关提供安全管理检查和现场安全值守工作，并指导下属单位的安全工作，协助局机关落实相关安全政策以及相关要求。

1.负责省戒毒管理局安全设备及安全检测系统的日常运维，包括运行状态日检、检测，对安全设备及安全监测系统的策略调优、每天对安全设备日志信息和安全监测系统告警信息进行深入分析，及时发现安全威胁，并进行验证、处置及报告。

2.结合省戒毒管理局实际业务发展及安全现状，协助对网络及信息安全进行持续的风险评估，以风险结果为依据，协助进行应急预案及省戒毒管理局体系建设的补充完善。

3.对外部发生的信息安全事件(如系统或软件高危漏洞、病毒变种等)，快速分析，结合省戒毒管理局实际情况提供处置方案并协助实施，以防同类事件在省戒毒管理局内部发生。

4.故障处理时限：上班时间（周一至周五 8：30～17:30）以及周末、节假日、值班期间，5 分钟之内到达故障现场，2 小时内解决并完成服务需求；工作日其余时间（除周一至周五 8：30～17:30 以外的时间）要求 1 小时内到达现场，3 小时内解决并完成服务需求；遇到紧急、特殊的服务要求应立即提供服务至解决问题为止；与二线专家建立快速响应通道，及时对安全事件的进行分析和反馈，提升安全运营工作效率。

5.开展现场安全值守、安全运营体系建设、风险评估服务、安全加固服务、安全应急服务、漏洞扫描服务、应用系统渗透测试、安全攻防演练服务、安全重保服务等。

6.驻场安全工程师在服务期间需要完成局机关科技部门交办的其他安全工作任务，根据工作需要对基层场所特别是省直戒毒单位进行相关的网络安全分析、漏洞扫描、风险评估等工作，及时为基层单位提供网络安全应急技术指导和支撑服务。因特殊情况需要，如需驻场安全工程师赶赴基层场所特别是省直戒毒单位提供现场技术支援的，由省局统一安排车辆，成交供应商不得以任何形式向省戒毒管理局收取任何费用。

5.4.3 驻场人员管理其他要求

1.驻场服务人员必须与采购方签订保密承诺书。

2.驻场服务人员须提供三年内无违法犯罪记录，五年内无刑事处罚记录并加盖公章；须提供身份证复印件、资格证明复印件以及社保证明复印件加盖公章。

3.驻场服务人员须严格遵守本单位考勤制度，平日上下班时间;上午 8：30-12：00，下午 13：00-17：30。国庆、两会、春节、重要节假日（如清明、五一、中秋、端午等）、重要会议、极重要业务服务时间段以及局机关要求的期间：上午 8：30-次日 8:30，轮班人员按交接班对应时间签到考勤。如有请假应提前通知项目负责人，做好值班调整安排，不得影响正常值班。

4.驻场服务人员须与项目负责人或管理人员良好沟通，服从领导以及本单位的规则制度；

5.驻场服务人员须有良好的工作态度以及责任心，积极主动完成工作，并有一定的学习能力。

6.成交供应商须提供驻场服务人员日常工作流程与考核标准给省戒毒管理局做管理参考，省戒毒管理局可对驻场安全工程师进行考核，省戒毒管理局有权要求变更驻场安全工程师，提供驻场服务的厂商必须在省戒毒管理局要求的期限内补齐满足要求的驻场安全工程师。

7.驻场服务人员应自觉履行岗位职责，严格遵照成交供应商安全服务操作流程与标准，按要求定期向采购人汇报工作进展与问题，成交供应商须保障一线人员与二线资源的协调沟通。

8.未经省戒毒管理局书面授权，驻场服务人员不得有任何越权行为，如擅自授权其它服务厂商等，否则由此产生的一切后果由成交供应商承担。构成犯罪的，移交司法机关处理。

5.5 设备验收调试要求

5.5.1 设备验收调试总体要求

成交供应商必须向省戒毒管理局提供本项目采购的所有硬件的安装和维护服务的全部内容，并在需要的时候配合设备使用单位完成整个系统的网络联调工作。若本项目采购的设备产品等方面的配置或要求中出现不合理或不完整的问题时，成交供应商有责任和义务在投标文件中提出补充修改方案并征得省戒毒管理局同意后付诸实施。

对成交供应商要求：

1.要求成交供应商必须具有良好信誉和相关实力的技术队伍。

2.成交供应商应本着认真负责态度，组织技术队伍，做好整体方案，并书面提出长期保修、维护、服务以及今后技术支持的措施计划和承诺。

3.自系统安装工作一开始，成交供应商应允许采购单位的工作人员一起参与系统的安装、测试、诊断及解决遇到的问题等各项工作。

设备安装工艺要求：

1.施工前必须做好详细的施工计划和施工方案，经审批后实施，并严格执行，确保整个项目在有效时间内保质、保量的完成；

2.进行与原有系统的对接工作，应避免工作时间施工，必须在施工完成后对现场进行及时恢复，确保工作时间正常使用；

3.要做好原有设备保护处理，防止损坏；

4.项目经理必须具有丰富的网络安全经验，能协调好现场的各种资源、控制现场的施工进度，做好进度管理、质量管理。

减少施工过程对省戒毒管理局正常办公的影响，每日施工完毕必须对施工现场卫生进行清洁并回复原样。

5.5.2 测试验收要求

成交供应商应根据所提交的验收方案和实施办法，自行组织设备和人员，并在使用单位监查下现场进行测试和验收。

测试方式

成交供应商必须向建设单位提供本项目采购的所有硬件的安装和维护服务的全部内容，并在需要的时候配合设备使用单位完成整个系统的网络联调和测试工作。

测试主要目的是网络安全运营相关系统的支撑能力及运行能力。系统安装完成后，按照系统要求的基本功能逐一测试。

若省戒毒管理局涉及的设备产品或服务配置要求等方面存在不合理或不完整的情况，成交供应

商有责任和义务提出补充修改方案并征得省戒毒管理局同意后付诸实施，否则必须完全按用户需求执行。

测试和验收

成交供应商应根据所提交的验收方案和实施办法，自行组织设备和人员，并在使用单位监查下现场进行测试和验收。

1.开箱检验

（1）所有设备、器材在开箱时必须完好，无破损。配置与装箱单相符。数量、质量及性能不低于合同要求。

（2）拆箱后，成交供应商应对其全部产品、零件、配件、用户许可证书、资料、介质造册登记，并与装箱单对比，如有出入应立即书面记录，由供货商解决，如影响安装则按合同有关条款处理。登记册作为验收文档之一。

2.系统测试

系统安装完成后，按照系统要求的基本功能逐一测试。

（1）单项测试：单项产品安装完成后，由成交供应商进行产品自身性能的测试。设备通电测试应单台进行，所有设备通电自检正常后，才能相互联结。

（2）系统联机测试：系统安装完成后，由成交供应商和设备使用单位对所有采购的产品进行联网运行，并进行相应的联机测试。

（3）系统功能测试：对网络安全运营相关系统配置及应用等功能进行详细测试。

（3）系统整体运行情况：系统运行正常，联机测试通过。

（4）如商检或系统测试中发现设备性能指标或功能上不符合标书和合同时，将被看作性能不合格，设备使用单位有权拒收并要求赔偿。

（5）成交供应商应负责在项目验收时将系统的全部有关产品说明书、原厂家安装手册、技术文件、资料、及安装、验收报告等文档交付设备使用单位。

3.产品验收要求

（1）要求对全部设备、产品、型号、规格、数量、外型、外观、包装及资料、文件（如装箱单、保修单、随箱介质等）的验收。

（2）凡列入《中华人民共和国实施强制性产品认证的产品目录》的产品在验收时出具 CCC 认证证书复印件，并以在产品外部加施认证标志作为验收依据之一。

（3）成交供应商应负责在项目验收时将系统的全部有关产品说明书、原厂家安装手册、技术文件、资料、及安装、验收报告等文档汇集成册交付设备使用单位和监理单位。

5.5.3 验收标准

采购人同时对服务的质量和安全设备的部署情况进行验收。项目验收按照广东省财政投资信息化建设项目验收的有关规定执行。项目验收的具体组织工作由项目采购人承担。

本项目的验收应符合广东省信息化项目相关验收管理办法的要求，同时应遵循下列标准：

1.实现合同和根据招标文件所编写的投标文件中列举的全部工作内容。

2.验收项目包括按照合同和根据招标文件所编写的投标文件中所标明的调研报告、运营方案、培训教材和使用说明书。

3.服务期间，成交供应商应按照合同、招标文件的要求和投标文件的服务承诺提供稳定、可靠、优质的服务，定期提交《项目进度报告》。服务期满后，提交《服务总结报告》。采购人收到《服务总结报告》15 个工作日内启动流程对报告进行审核，审核完成后开展验收，出具最终验收报告。

5.6 安全保密

成交供应商向采购方签订《保密责任书》，同时成交供应商向采购方提供成交供应商所有服务人员的基本资料，《保密责任书》和服务人员基本资料作为合同附件；同时，成交供应商服务人员向采购方签订《保密承诺书》。

成交供应商及项目组工作人员在本项目实施过程中，应严格遵守采购方有关规定和要求。在工作中使用和产生的各类纸质或电子文档资料均归采购方所有。成交供应商对接触到、掌握到的采购方工作状况、文件资料、数据信息、技术装备等应严格保守秘密，未经采购方许可，不得记录、存储、复制、泄漏、外传等，或用于履行本合同之外的其他用途。

成交供应商负责确保其工作人员或受雇第三方严格履行本项目安全保密义务，如在项目实施过程中或项目验收后，成交供应商或其工作人员、受雇第三方违反本项目安全保密义务，特别是出现因成交供应商或其工作人员、受雇第三方原因造成采购方发生信息安全保密或信息泄露问题，采购方有权视情况按相关法律、法规、规章、制度和本合同，追究成交供应商和相关人员的相应责任，并要求赔偿由此造成的损失。

5.7 付款方式说明

付款方式：采用银行转账、支票等形式。成交供应商请款时，应根据财务管理规定要求，提供合法有效的发票、项目合同复印件等相关资料并经采购人核实。

付款时间为：采购人在收到付款申请 10 个工作日内提交审核，经审核符合支付条件后（如遇法定节假日，则审批时间相应顺延）按照相关的程序办理资金拨付。

成交供应商承诺在采购人办理以上各期付款的支付手续前，为采购人出具等额的符合国家规定的发票，成交供应商迟延提供发票的，采购人有权迟延付款；

本合同约定的付款期限仅为采购人向财政申请付款的时间，不包括采购人正常办理支付报批手续的时间，由于审批迟延导致的逾期付款采购人不承担违约责任。

1.第一期款：合同签订生效后 10 个工作日内，成交供应商向采购人报送请款资料，申请支付合同总金额 40%。经采购人审核后，申请办理付款。

2.第二期款：驻场服务满 1 年后 10 个工作日内，成交供应商向采购人提交服务 1 年的阶段性成果物报告并报送请款资料，申请支付合同中总金额 30%。经采购人审核后，申请办理付款。

3.第三期款：驻场服务满 2 年后 10 个工作日内，成交供应商向采购人提交服务内容的成果物报告和总结并通过采购人组织的项目终验后，报送请款资料，申请支付合同总金额 30%。经采购人审核后，申请办理付款。

4.第四期款：安全产品正常使用且满 3 年，如无发生因质量问题扣款，质保期到后，采购人 10 个工作日内将质量保证金无息支付给成交供应商。

合同签订生效后 15 个工作日内，成交供应商向采购人缴纳合同金额 5%的履约保证金，项目终验后，该款转为质量保证金。

第三部分 合同草案

合 同 草 案

甲　　方：_____

乙　　方：_____

签约地点：_____

签订日期：　　年　　月　　日

甲　　方：广东省戒毒管理局

电　　话：　　传　真：　　地　址：

乙　　方：_____

电　　话：　　传　真：　　地　址：

根据 2020 年省戒毒局机关网络安全项目 的采购结果，按照《中华人民共和国政府采购法》、《中华人民共和国政府采购法实施条例》、《合同法》的规定，经双方协商，本着平等互利和诚实信用的原则，一致同意签订本合同如下。

一、 合同金额

合同金额为（大写）：_____元（￥_____元）人民币。

二、 服务范围

甲方聘请乙方提供以下服务：

1. 本合同项下的服务指_____。

2. .....

3. .....

三、 甲方乙方的权利和义务

（一） 甲方的权利和义务

（二） 乙方的权利和义务

四、 服务期间（项目完成期限）

委托服务期间自_____年_____月至_____年_____月止。

五、 付款方式

因甲方使用的是财政资金，甲方在前款规定的付款时间为向政府采购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甲方已经按期支付。

六、 知识产权产权归属

乙方应保证本项目的技术、服务或其任何一部分不会产生因第三方提出侵犯其专利权、商标权或其他知识产权而引起的法律和经济纠纷；如因第三方提出其专利权、商标权或其他知识产权

的侵权之诉，则一切法律责任由乙方承担。

七、 保密

项目实施过程中至乙方正式向甲方交付技术文档资料时止，乙方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，由于乙方过错导致的上述资料泄密的，乙方必须承担一切责任。项目完成后，甲、乙双方均有责任对本项目的技术保密承担责任。

1）未经乙方事先书面同意，甲方不得将由乙方为本合同提供的条文、规格、计划、图纸、模型、样品或资料提供给与本合同无关的任何第三方，不得将其用于履行本合同之外的其它用途。即使向与履行本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。

2）除了合同本身之外，上款所列举的任何物件均是乙方的财产。如果乙方有要求，甲方在完成合同后应将这些物件及全部复制件还给乙方。

八、 违约责任与赔偿损失

1）乙方提供的服务不符合磋商文件、响应文件或本合同规定的，甲方有权拒收，并且乙方须向甲方方支付本合同总价 5%的违约金。

2）乙方未能按本合同规定的交货时间提供服务，从逾期之日起每日按本合同总价 3‰的数额向甲方支付违约金；逾期半个月以上的，甲方有权终止合同，由此造成的甲方经济损失由乙方承担。

3）甲方无正当理由拒收接受服务，到期拒付服务款项的，甲方向乙方偿付本合同总的 5%的违约金。甲方人逾期付款，则每日按本合同总价的 3‰向乙方偿付违约金。

4）其它违约责任按《中华人民共和国合同法》处理。

九、 争端的解决

合同执行过程中发生的任何争议，如双方不能通过友好协商解决，按相关法律法规处理。

十、 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。

十一、 税费

在中国境内、外发生的与本合同执行有关的一切税费均由乙方负担。

十二、 其它

1）本合同所有附件、磋商文件、响应文件、成交通知书均为合同的有效组成部分，与本合同具有同等法律效力。

2）在执行本合同的过程中，所有经双方签署确认的文件（包括会议纪要、补充协议、往来信函）即成为本合同的有效组成部分。

3）如一方地址、电话、传真号码有变更，应在变更当日内书面通知对方，否则，应承担相应责任。

4）除甲方事先书面同意外，乙方不得部分或全部转让其应履行的合同项下的义务。

十三、 合同生效

1）本合同在甲乙双方法人代表或其授权代表签字盖章后生效。

2）合同一式____份，其中甲方____份，乙方____份，监管部门壹份，采购代理机构壹份。

甲方（盖章）：	乙方（盖章）：
法定代表/授权代表（签字）：	法定代表/授权代表（签字）：
日期：	日期：
邮政编码：	邮政编码：
开户名称：	开户名称：
开户银行：	开户银行：
开户账号：	开户账号:

注： 此为合同草案，可根据磋商情况进行变更！

第四部分 评审办法

1. 磋商小组

1.1 本次磋商按照磋商须知前附表第 9 项规定依法组建磋商小组（达到公开招标数额的项目磋商小组成员为五人以上单数）。

1.2 磋商小组所有成员集中对响应文件进行审查，与每个供应商分别进行先商务技术条件后价格的磋商，本次磋商采用一轮磋商，两次报价形式进行。最后报价提交时间视磋商进程由磋商小组决定。磋商小组也可视实际情况确定磋商轮次及报价次数，并提交评审报告及推荐成交供应商。

1.3 磋商小组名单在磋商结果确定前严格保密。

2. 评审方法：综合评分法。

先进行资格、符合性评审的第一阶段审查，不通过第一阶段审查的供应商，其响应文件作无效处理，不进入磋商阶段。磋商完成后，进行资格、符合性评审的第二阶段审查，然后进行详细评审。

3. 评审程序

1.1 **确定磋商次序**

按照供应商递交首次磋商响应文件的先后顺序作为磋商的先后顺序。

1.2 **磋商小组确认磋商文件**

1.3 **资格、符合性评审**

磋商小组对每个供应商的响应文件进行资格、符合性评审。评审细则详见“附表一：资格、符合性评审表”。**对不通过第一阶段审查的供应商，由磋商小组或采购人代表将集体意见现场及时告知该供应商，其响应文件作无效处理，不参与磋商。**

1.4 **磋商**

3.4.1 磋商文件未发生实质性变动的：

磋商小组集中与每个供应商分别进行磋商，并形成磋商纪要。磋商的内容主要是对响应文件的澄清、修正、补充、确认等。供应商磋商结束后，填写《磋商纪要》，在该文件上注明最后报价及有关承诺。《磋商纪要》是响应文件的有效组成部分。如磋商小组没有对磋商文件作实质性变动增加新的需求，后一轮报价不得高于前一轮报价，否则将按响应无效处理。

3.4.2 磋商文件发生实质性变动的：

（1）书面通知变更内容

在磋商过程中，磋商小组可以根据磋商文件和磋商情况实质性变动采购需求中的技术、服务要求以及合同草案条款，但不得变动磋商文件中的其他内容。实质性变动的内容，经采购人代表确认后，由磋商小组书面通知所有供应商。对磋商文件作出的实质性变动是磋商文件的有效组成部分。

（2）磋商

磋商小组集中与接受磋商文件变更的每个供应商分别进行磋商，并形成磋商纪要。磋商的内容主要是对响应文件的澄清、修正、补充、确认等。不接受磋商文件变更的供应商，视为自动退出磋商，其响应文件作无效处理。

（3）重新提交响应文件（含报价）

供应商应当按照磋商文件的变动情况和磋商小组的要求重新提交响应文件（指磋商结束后，在规定时间内填写《磋商纪要》，在该文件上注明最后报价及有关承诺，并提交）。最终报价时间视磋商进程由磋商小组决定。《磋商纪要》是响应文件的有效组成部分，须由其法定代表人或授权代表签字或印鉴或者加盖公章。由授权代表签字或印鉴的，应当附法定代表人授权书。供应商为自然人的，应当由本人签字或印鉴并附身份证明。

★供应商未在规定时间内提交最终报价的，视为退出磋商，其响应文件作无效处理。

1.5 **最终报价的详细报价的确定**

供应商应在最终报价表中详细填写各项单价。若只填写总价不填报单价，则视为供应商同意按照下浮率 b%对首次报价表中的单价进行统一下浮。

下浮率 b%的计算方法=1-最终报价总价/首次报价总价

当采购需求发生修改或变动导致供应商的最终报价总价高于首次报价总价的，供应商应当在最终报价表中详细填写各项单价。

1.6 **公布最终报价**

除非在磋商中磋商小组调整或修改采购需求内容，否则采购人不接受高于前面轮次磋商报价的最终报价。最终报价内容现场公布。

1.7 **最终方案评审**

经磋商确定最终采购需求和提交最后报价的供应商后，由磋商小组采用综合评分法对提交最后报价的供应商的响应文件和最后报价进行综合评分（即技术、商务及价格的详细评审）。

- 资格、符合性评审表（详见附表一）
- 技术评审表（详见附表二）
- 商务评审表（详见附表三）
- 价格评审（详见附表四）

3.7.1 比较与评价

磋商小组按磋商文件中规定的评审方法和标准，对通过第一、第二阶段资格、符合性评审的响应文件进行商务和技术评估，综合比较与评价。技术、商务、价格部分分值分配如下：

评分项目	技术评分	商务评分	价格评分	合 计
权重	50%	30%	20%	100%
分值	50分	30分	20分	100 分

具体量化打分标准如下：

（1）技术、商务评分

磋商小组分别对各供应商的技术、商务响应文件中的各项内容进行评议比较，详细对比其技术、商务方案等各种因素方面是否满足磋商文件的要求。在技术、商务评审表的相应项各自记名打分。

（2）技术商务得分统计

将所有磋商小组的技术评分的算术平均值即为每个有效供应商的技术得分（四舍五入后，精确到 0.01）。

将所有磋商小组的商务评分的算术平均值即为每个有效供应商的商务得分（四舍五入后，精确到 0.01）。

将技术得分、商务得分相加得出商务技术得分。

（3）价格核准和评分

A. 价格的核准

如果磋商小组发现响应供应商的最终报价明显低于其他通过资格、符合性评审供应商的报价，有可能影响产品质量或者不能诚信履约的，将要求其在磋商现场在磋商小组规定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，磋商小组将其作为响应无效处理。

磋商小组先对入围供应商的最后报价进行复核，审查其是否有计算上的错误，修正错误的原则如下

响应文件的大写金额和小写金额不一致的，以大写金额为准；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；单价金额小数点有明显错位的，应以总价为准，并修改单价；对不同文字文本响应文件的解释发生异议的，以中文文本为准。

按上述修正错误的方法调整后的最后报价，对供应商具有约束力。如果供应商不接受修正后的价格，则其响应文件作无效处理。

B. 小型和微型企业产品价格扣除条款

供应商为小型或微型企业（包括成员均为小型或微型企业的联合体）且报价产品/服务含小型或微型企业产品/服务时，报价给予 K1 的价格扣除（K1 的取值为 6%），即：评审价＝核实价-小微企业产品核实价×K1 ；

供应商为大中型企业和其他自然人、法人或者其他组织与小型、微型企业组成的联合体，且联合体协议中约定小型、微型企业的协议合同金额（必须为本企业承担的服务）占到联合体协议合同总金额 30%以上的，对联合体报价给予 K2 的价格扣除（K2 的取值为 2%），即：评审价＝核实价-小微企业产品核实价×K2；

本条款所称小型或微型企业应当符合以下条件：符合《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300 号）规定的对小型或微型企业的划分标准，并且提供本企业承担的服务；

组成联合体的大中型企业和其他自然人、法人或者其他组织，与联合体中的小型、微型企业

之间不得存在投资关系；

参加政府采购活动的中小企业应当提供《中小微企业声明函》。符合残疾人福利性单位认定条件的，应当提供《残疾人福利性单位声明函》（详见第五部分 响应文件格式第四章）。符合监狱企业单位认定条件的，应当提供由省级以上监狱管理局、戒毒管理局(含新疆生产建设兵团)出具的属于监狱企业的证明文件。

监狱企业、残疾人福利性单位视同小型、微型企业，享受以上价格扣除政策。

监狱企业、残疾人福利性单位本身属于小型、微型企业的，不重复享受政策。

C. 节能环保产品价格扣除条款

b) 所投产品(针对非政府强制采购产品)获得有效期内的节能产品认证证书的，节能产品报价占总报价比例在 80%或以上的，对节能产品的价格给予 2%的扣除，在 80%以下的，对节能产品的价格给予 1%的扣除，用扣除后的价格参与评审。（提供节能产品认证证书）。

c) 所投产品(针对非政府强制采购产品)获得有效期内的环境标志产品认证证书的，环境标志产品报价占总报价比例在 80%或以上的，对环境标志产品的价格给予 2%的扣除，在 80%以下的，对环境标志产品的价格给予 1%的扣除，用扣除后的价格参与评审。（提供环境标志产品认证证书）。

对属于强制采购的节能产品，节能要求作为实质性响应指标，不再享受评审优惠。

D. 价格评分

磋商小组对入围的供应商的最后价格进行修正得出评审价。综合评分法中的价格分统一采用低价优先法计算，即满足磋商文件要求（通过资格、符合性评审）且价格最低的有效最后报价（指修正后的价格，下同）为磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算：

磋商报价得分＝（磋商基准价 / 最后磋商报价）x 价格权值x 100（精确到0.01）。

因落实政府采购政策进行价格调整的，以调整后的价格计算磋商基准价和最后磋商报价。

因落实政府采购政策进行价格调整的，以调整后的价格计算磋商基准价和磋商报价。

4. 推荐成交候选人名单

详见磋商须知前附表第 11 项。

5. 确定成交供应商

采购人将根据评审结果，确定成交供应商。采购代理机构受采购人委托在规定的媒体上发布成交公告，同时向成交供应商发出书面《成交通知书》，向所有未成交供应商发出《成交结果通知书》。

附表一：

资格、符合性评审表

审查内容			供应商
第一阶段审查（磋商前）	符合磋商文件规定的资格要求		
	保证金按要求提交		
	符合磋商有效期		
	响应文件按照磋商文件规定要求签署、盖章	资格声明函	
		报价函	
		法定代表人证明书或法定代表人授权书	
		首次报价一览表	
		首次报价详细报价表	
		实质性响应一览表	
		报价响应与磋商文件差异一览表	
第二阶段审查（磋商后）	**最终报价未超过本项目最高限价（或超出了最高限价，采购人仍能接受）**		
	完全满足磋商文件中 “★”标注的条款（若磋商文件发生实质性变动的，本条将针对供应商重新提交的响应文件进行评审）		
	未出现有关法律、法规、规章或磋商文件规定的属于响应无效的情形		
结论	是否实质性响应磋商文件（写“是”或“否”）		

注：

1、每一项符合要求的打“○”，对不符合要求的打“×”，并在结论栏中简要说明原因。

2、不通过第一阶段审查的供应商，其响应文件作无效处理，不进入磋商阶段。

附表二：技术评审表

序号	评审项目	评分细则	单项分数/权重	供应商得分
1	重要条款响应	对于需求中的重要条款“▲”进行响应，每个得 1.5 分。最高的 27 分。	27	
2	技术方案	根据供应商提供的技术方案进行评审，具体要求如下： 提供的技术方案能满足采购人的要求，并且针对以下内容有对应的章节进行详细描述 1.整体架构设计：需要详细介绍整体架构设计情况，内容需要包括但不限于： （1）整体架构图设计图；（2）设计说明；（3）系统内包含的各个组件说明； 2.病毒、恶意代码及木马防护：需要详细介绍病毒、恶意代码及木马防护情况，内容需要包括但不限于： （1）病毒更新模式；（2）私有云查杀平台； 3.需要详细介绍补丁管理情况，内容需要包括但不限于： （1）补丁管理流程；（2）补丁更新方式；（3）补丁分发控制手段； 4.运维管理支撑：需要详细介绍运维管理支撑情况，内容需要包括不限于： （1）非法外联控制；（2）应用程序控制；（3）网络安全防护；(4）硬件外设控制；（5）策略应用时段管理； 5. 桌面安全加固： 需要详细介绍桌面安全加固设置情况，内容需要包括不限于： （1）针对桌面系统的账号密码的加固；（2）针对本地安全策略的加固；（3）针对屏保与壁纸的加固；（4）针对浏览器安全的加固； 6.资产管理：需要详细介绍资产管理情况，内容需要包括不限于 （1）终端软、硬件资产统计管理；（2）终端软、硬件变更管理；（3）终端插件管理； 7.移动存储介质管理：需要详细介绍移动存储介质注册及授权管理过程情况，内容需要包括不限于： （1）授权管理；（2）外出管理；（3）挂失管理；（4）例外管理； 8.终端安全态势大屏分析：提供可视化能力界面，界面能够呈现终端大数据内容可基于内容做相关分析，方案中提供相应产品功能配图说明： （1）安装率展示；（2）正常率展示；（3）合规率展示；（4）实名率展示。 针对以上八项逐项打分，满足的一项得 1.5 分，不满足或未响应的得 0 分，累计最高得 12 分。	12	
		方案全面，应答精准透彻得 4 分，方案比较全面，应答准确得 3 分。有基本的方案，应答基本准确得 2 分。方案片面或应答不准确得 1 分，无不得分。	4	

3	需求理解能力	依据各供应商需求理解能力进行比较。 对招标文件的内容、要求理解透彻，投标文件结构清晰，内容完整，表述（含截图）清晰、严谨、合理；实施方案完整、可行、实用，完全满足并优于采购需求，得 4 分；理解一般，结构一般，内容一般，表述（含截图）一般，基本满足采购需求，得 2 分；理解不够透彻，结构不太清晰，内容不太完整，表述（含截图）不清晰，不能完全满足采购需求，得 1 分；未提供，得 0 分。	4	
4	服务要求	依据各供应商项目实施方案中服务相关内容进行评审。 给出了详细的服务方案，完全满足采购人要求，得 3 分；服务方案一般，不太详细，不能完全满足采购人要求，得 1 分；未提供，得 0 分。	3	
合计			50	

附表三：商务评审表

序号	评审项目	评分细则	单项分数/权重	投标人得分
1	供应商资质要求	1.具有质量管理体系认证证书（1 分） 2.具有信息安全管理体系认证证书（1 分） 3.具有服务管理体系认证证书（1 分） 4. CMM/CMMI 体系三级证书或以上（1 分） 5.具有信息系统安全集成服务资质认证证书（CCRC）一级得 3 分，二级得 2 分，三级得 1 分；无得 0 分。 提供相应证书复印件并加盖供应商公章。	7	
2	同类项目业绩	2017 年 1 月 1 日至投标截止之日止，供应商承接同类项目业绩，每提供一个得 1 分。本项累计最高得 4 分； 注：上述项目业绩须在投标文件中同时附上合同复印件加盖供应商公章。	4	
3	终端安全产品厂家资质要求	拥有国家信息安全漏洞库技术支撑单位证书，一级得 2 分，二级得 1 分，三级得 0.5 分；无得 0 分；提供相应证书复印件并加盖供应商公章。	2	
		拥有国家互联网应急中心网络安全信息通报单位证书，得 1 分；无得 0 分；提供相应证书复印件并加盖供应商公章；	1	
		国家规划布局内重点软件企业证书，得 1 分；无得 0 分；提供相应证书复印件并加盖供应商公章	1	
		拥有 CCRC 中国网络安全审查技术与认证中心（原为中国信息安全认证中心）信息安全服务资质-安全运维服务资质一级得 2 分，二级得 1 分，三级得 0.5 分；无得 0 分；提供相应证书复印件并加盖供应商公章	2	
		终端安全产品厂商二线支撑团队拟投入的项目经理具备： （1）注册信息安全专业人员（CISP）证书（1 分）； （2）PMP 证书（1 分）； （3）信息系统项目管理师证书（1 分）； （4）学历硕士（或以上）证书（1 分）。 以上证书每个提供一个得 1 分。 供应商需提供为上述“拟投入的项目经理”购买的投标截止时间为止近 1 年内任意连续 3 个月的社保证明（代缴个税税单或参加社会保险的《投保单》或《社会保险参保人员证明》等证明均可）。如果供应商成立时间或该人员入职不足 3 个月，则提供人员入职证明及入职时间至今的社保证明。提供相应证书和证明材料复印件并加盖供应商公章。	4	

4	拟投入人员资质要求	1.供应商拟投入项目负责人具备： （1）注册信息安全专业人员（CISP）证书（1 分）； （2）信息系统项目管理师证书（1 分）； （3）学历硕士（或以上）证书（1 分）； （4）系统分析师证书（1 分）； （5）2017 年以来完成过的信息化项目经验（1 分）。 供应商需提供为“拟投入的项目负责人”购买的投标截止时间为止近 1 年内任意连续 3 个月的社保证明（代缴个税税单或参加社会保险的《投保单》或《社会保险参保人员证明》等证明均可）。如果供应商成立时间或该人员入职不足 3 个月，则提供人员入职证明及入职时间至今的社保证明。提供相应证书和证明材料复印件并加盖供应商公章。	5	
		2.除项目负责人外的其他人员具备： （1）信息安全保障人员认证证书（1 分）； （2）ITIL 认证项目管理师证书（1 分）； （3）注册信息安全专业人员（CISP）证书（1 分）； （4）信息安全等级保护安全建设专业技术人员证书（1 分）。 供应商需提供为“除项目负责人外的其他人员”购买的投标截止时间为止近 1 年内任意连续 3 个月的社保证明（代缴个税税单或参加社会保险的《投保单》或《社会保险参保人员证明》等证明均可）。如果供应商成立时间或该人员入职不足 3 个月，则提供人员入职证明及入职时间至今的社保证明。提供相应证书和证明材料复印件并加盖供应商公章。	4	
合计			30	

附表四：

价格评审表

序号	评审项目	评议内容
1	价格	磋商小组对入围的供应商的最后价格进行修正得出评审价。综合评分法中的价格分统一采用低价优先法计算，即满足磋商文件要求（通过资格、符合性评审）且价格最低的有效最后报价（指修正后的价格，下同）为磋商基准价，其价格分为满分。其他供应商的价格分统一按照下列公式计算： 磋商报价得分＝（磋商基准价／最后磋商报价）x 价格权值x 100（精确到0.01）。 因落实政府采购政策进行价格调整的，以调整后的价格计算磋商基准价和最后磋商报价。

第五部分　响应文件格式

响应文件包装信封或外包装格式参考

项目编号： 440000-202009-202001-0041
项目名称： 2020 年省戒毒局机关网络安全项目

响 应 文 件

□ 正本

□ 副本

□ 保证金信封

供应商名称:（盖单位章）

供应商地址:

供应商名称:

（在规定的投标截止时间之前不得启封）

响应文件封面格式参考

项目编号：440000-202009-202001-0041
项目名称：2020 年省戒毒局机关网络安全项目

响 应 文 件

口 正本

口 副本

供应商名称:（盖单位章）

供应商地址:

第一章 目录

类型名称	序号	文件名称	页码	备注
索引	1	**资格性、符合性审查自查表**		
	2	**评审要素响应资料表**		
资格审查文件（加盖公章）	1	**资格声明函（按规定格式盖章签署，否则将导致不能通过资格审查）**		
	1.1	提供最新的供应商营业执照（或事业单位法人证书，或社会团体法人登记证书，或执业许可证）副本复印件；如供应商为自然人的需提供自然人身份证明；如国家另有规定的，则从其规定。若以不具有独立承担民事责任能力的分支机构磋商，须取得具有法人资格的总公司的授权书，并提供总公司营业执照副本复印件。		
	1.2	供应商应当具有良好的商业信誉和健全的财务会计制度，提供以下证明之一：①提供 2018 年年度（或 2019 年年度）年度审计报告或企业所得税年度汇算清缴报告（适用于在上一年度前成立的法人或其他组织）；② 2020 年任一季度或任一月的财务报表，内容含盖资产负债表和利润表和现金流量表（适用在上一年度或本财务年度成立的法人或其他组织）；③基本户开户银行出具的资信证明，并提供开户许可证（适用于法人或其他组织）； ④中国人民银行出具的个人信用报告（适用于自然人）。		
	1.3	提供 2019 年（或 2020 年）任意一个月的依法缴纳税收的证明（如纳税凭证）复印件，如依法免税的，应提供相应文件证明其依法免税；（其中税种不能为社会保险基金）；供应商成立不满三个月的，可不提供缴纳税收的证明。		

	1.4	提供 2019 年（或 2020 年）任意一个月的依法缴纳社会保险的证明（如缴费凭证）复印件，如依法不需要缴纳社会保障资金的，应提供相应文件证明其依法不需要缴纳社会保障资金；供应商成立不满三个月的，可不提供缴纳社会保险的证明。		
	2	**供应商认为必要的材料。**		
商务部分（加盖公章）	1	**报价函（按规定格式盖章签署，否则将导致响应无效）**		
	2	**法定代表人证明书或法定代表人授权委托书（按规定格式盖章签署，否则将导致响应无效）**		
	3	**首次报价一览表（按规定格式盖章签署，否则将导致响应无效）**		
	4	**首次报价详细报价表（按规定格式盖章签署，否则将导致响应无效）**		
	5	**政策适用性说明**		
	6	**中小微企业声明函（可选）**		
	7	**残疾人福利性单位声明函（可选）**		
	8	**实质性响应一览表（按规定格式盖章签署，否则将导致响应无效）**		
	9	**磋商响应与磋商文件差异一览表（按规定格式盖章签署，否则将导致响应无效）**		
	10	**供应商基本情况表**		
	11	**项目经理/项目负责人简历表**		
	12	**拟为本项目配置的人员情况表**		
	13	**类似项目业绩一览表**		
	14	**磋商保证金退还说明**		
	15	**采购代理服务费承诺书**		
	16	**供应商认为必要的其他商务资料**		
	17	**银行保函（已通过其他方式提交保证金的，无须提供）**		
	18	**政府采购磋商担保函（已通过其他方式提交保证金的，无须提供）**		
	19	**联合体共同磋商协议书（如项目允许联合体参与，联合体各方需签订）**		
技术部分（加盖公章）	20	**详见《第五章 响应文件技术部分》**		
	21	**供应商认为必要的其他技术资料**		

第二章 索引

2-1 资格性、符合性审查自查表

评审内容		磋商文件要求	自查结论	证明资料
资格性检查	供应商的资格要求	按磋商公告中所列供应商资格	□通过 □不通过	见响应文件第（）页
	保证金(磋商保证金交纳凭证)	金额详见磋商须知前附表（转账、汇款的提供复印件加盖公章）	□通过 □不通过	见响应文件第（）页
符合性审查	磋商有效期	报价函（供应商的报价有效期为自提交首次响应文件截止之日起 90 日）	□通过 □不通过	见响应文件第（）页
	最高限价	最终报价没有超出最高限价	□通过 □不通过	见响应文件第（）页
	响应文件签署合格	响应文件按照磋商文件规定要求签署、盖章	□通过 □不通过	见响应文件第（）页
	磋商文件中“★”标注的条款	满足磋商文件中“★”标注的条款	□通过 □不通过	见响应文件第（）页
	其他	未出现有关法律、法规、规章或磋商文件规定的属于响应无效的情形	□通过 □不通过	见响应文件第（）页

注：以上材料将作为供应商资格性、符合性审核的重要内容之一，供应商应严格按照其内容及序列要求在响应文件中对应如实提供,对缺漏和不符合项将会直接导致响应无效!请在对应的 □ 打“√”。

2-2 评审要素响应资料表

商务评审分项	商务评审细则	证明文件
		见响应文件第（）页
		见响应文件第（）页
		见响应文件第（）页
		见响应文件第（）页
		见响应文件第（）页
		见响应文件第（）页
……	……	见响应文件第（）页
技术评审分项	**技术评审细则**	**证明文件**
		见响应文件第（）页
		见响应文件第（）页
		见响应文件第（）页
		见响应文件第（）页
		见响应文件第（）页
		见响应文件第（）页
……	……	见响应文件第（）页

注：1、供应商应根据《技术评审表》和《商务评审表》的各项内容填写此表，表格可延长。

2、按评审项的顺序填写。

第三章 资格审查文件

3-1 资格声明函

广东志正招标有限公司：

关于贵公司的 2020 年省戒毒局机关网络安全项目 （项目编号：440000-202009-202001-0041 ）的竞争性磋商公告，本单位（企业）自愿参加磋商，本单位具备《中华人民共和国政府采购法》第二十二条规定的条件，现承诺如下：

本单位具备《中华人民共和国政府采购法》第二十二条资格条件，并已清楚磋商文件的要求及有关文件规定。

本单位的法定代表人或单位负责人与所参投的本采购项目包组的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。

根据《中华人民共和国政府采购法实施条例》的规定，本单位清楚：如为本采购项目包组提供整体设计、规范编制或者项目管理、监理、检测等服务的供应商，不得再参加该采购项目包组的其他采购活动。否则，由此所造成的损失、不良后果及法律责任，一律由我单位承担。

本单位具有履行合同所必需的设备和专业技术能力，且参加政府采购活动前 3 年内在经营活动中没有重大违法记录。否则，由此所造成的损失、不良后果及法律责任，一律由我单位承担。

本次招标采购活动中，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，一律由我单位承担。

供应商名称（并加盖法人公章）：

供应商法定代表人或其委托人签名或印鉴：

日期：_____年___月___日

附件：

1.1 提供最新的供应商营业执照（或事业单位法人证书，或社会团体法人登记证书，或执业许可证）副本复印件。如供应商为自然人的需提供自然人身份证明。若以不具有独立承担民事责任能力的分支机构磋商，须取得具有法人资格的总公司的授权书，并提供总公司营业执照副本复印件。

1.2 供应商应当具有良好的商业信誉和健全的财务会计制度，提供以下证明之一：①提供 2018 年年度（或 2019 年年度）年度审计报告或企业所得税年度汇算清缴报告（适用于在上一年度前成立的法人或其他组织）；② 2020 年任一季度或任一月的财务报表，内容含盖资产负债表和利润表和现金流量表（适用在上一年度或本财务年度成立的法人或其他组织）；③基本户开户银行出具的资信证明，并提供开户许可证（适用于法人或其他组织）； ④中国人民银行出具的个人信用报告（适用于自然人）。

1.3 提供 2019 年（或 2020 年）任意一个月的依法缴纳税收的证明（如纳税凭证）复印件，如依法免税的，应提供相应文件证明其依法免税；（其中税种不能为社会保险基金）；供应商成立不满三个月的，可不提供缴纳税收的证明。

1.4 提供 2019 年（或 2020 年）任意一个月的依法缴纳社会保险的证明（如缴费凭证）复印件，如依法不需要缴纳社会保障资金的，应提供相应文件证明其依法不需要缴纳社会保障资金；供应商成立不满三个月的，可不提供缴纳社会保险的证明。

3-2 符合“供应商资格”要求的其他证明文件

附件 1：供应商认为必要的其他材料，如已经成功领取采购文件的证明材料（含采购代理机构邮件发送采购文件电子版的截图或者采购代理机构开具的本次采购文件购买的发票）

第四章 响应文件商务部分

4-1 报价函

致：广东志正招标有限公司

根据贵方为 2020 年省戒毒局机关网络安全项目 （项目编号：440000-202009-202001-0041 ）的竞争性磋商公告，本人代表供应商 （供应商名称） 参加磋商，并提交响应文件。

据此函，本人宣布同意如下：

1. 我方郑重承诺：磋商总报价包含用户需求说明的所有产品功能和服务内容，漏报的单价或每单价报价中漏报、少报的费用，视为此项费用已隐含在磋商总报价中，成交后不再向采购人收取任何费用。
2. 供应商已详细审查全部磋商文件，包括修改文件（如有的话）以及全部参考资料和有关附件。我们完全理解并同意放弃对这方面有不明及误解的权利。
3. 供应商的报价自响应文件提交截止之日起有效期为 90 天。
4. 如果在规定的提交响应文件截止时间后，供应商在磋商有效期内撤回响应文件，同意贵方不退还磋商保证金。
5. 供应商同意提供按照贵方可能要求的与我方报价有关的一切数据或资料，理解贵方不一定要接受最低价的报价或收到的任何报价。
6. 与本报价有关的一切正式往来通讯请寄：

地址： 邮编：

电话： 传真：

供应商代表姓名、职务（印刷体）：_____

供应商名称：（并加盖法人公章）

供应商法定代表人或其委托人签字或印鉴：_____

日期：____年___月___日

注：法定代表人委托全权代表人，需附法定代表人签字或印鉴的授权书。

4-2 法定代表人证明书/法定代表人授权书格式

法定代表人证明书和法定代表人授权书按以下格式填写，如由法定代表人参加磋商并签署响应文件，需提供法定代表人证明书，否则需提供法定代表人证明书和法定代表人授权书。

法定代表人证明书

_____同志，现任我单位_____职务，为法定代表人，特此证明。

有效日期：_____年___月___日至_____年___月___日 签发日期：_____年___月___日

附：

经济性质：

主营（产）：

兼营（产）：

供应商名称：（并加盖法人公章）

地址：

日期：

法定代表人 **有效期内的**居民身份证复印件（正面） 粘贴处	法定代表人 **有效期内的**居民身份证复印件（反面） 粘贴处

法定代表人授权书

致:广东志正招标有限公司

本授权书声明：注册于_____（国家或地区）的_____（供应商名称）的在下面签字的 _____（法定代表人姓名、职务）代表本单位授权在下面签字（或盖印鉴）的_____（被授权人的姓名、职务）为本单位的合法代表人，就 2020 年省戒毒局机关网络安全项目 （项目编号：_____）的磋商和合同执行，以我方的名义处理一切与之有关的事宜。

本授权书于 _____年____月____日签字（或盖印鉴）生效，特此声明。

供应商名称(并加盖法人公章)：

地　　址：

法定代表人（签名或印鉴)：

职　　务：

被授权人（签名或印鉴)：

职　　务：

被授权人（授权代表） **有效期内的**居民身份证复印件（正面） 粘贴处	被授权人（授权代表） **有效期内的**居民身份证复印件（反面） 粘贴处

4-3 首次报价一览表

项目编号：

项目名称	首次报价	备注
2020 年省戒毒局机关网络安全项目	大写：人民币_____元整	
	小写：¥_____元整	

注：1.本表格中的报价应等于详细报价表中的总报价。

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

日期：

4-4 首次报价详细报价表

项目编号： 金额单位：元（人民币）

序号	分项名称	数量	单价	是否小型/微型企业产品/服务（是/否）	分项报价
	……				
总报价：					
小型/微型企业产品/服务价格合计：					

（此表可延长）

注：

1. 总报价中必须包含磋商文件中要求的相关服务内容的全部费用，金额单位为元。
2. 如果分项报价的汇总与总报价不一致的，以分项报价的汇总为准。
3. 所投货物/服务为小型或微型企业产品的，请在上表标注，填写小型/微型企业产品/服务价格合计一项(非小型/微型企业产品/服务此项标注“--”)，并提供附表《中小微企业声明函》。
4. 最终报价的详细报价的确定。供应商应在最终报价表中详细填写各项单价，如只填写总价不填报单价，则视为供应商同意按照下浮率 b%对首次报价表中的单价进行统一下浮。
   下浮率 b%的计算方法=1-最终报价总价/首次报价总价

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

4-5 政策适用性说明

产品适用政府采购政策情况表

<table>
<tr><td rowspan="11">中小企业扶持政策</td><td colspan="5">如属所列情形的，请在括号内打“√”：
（ ）小型、微型企业投标且全部提供本企业制造的产品。
（ ）小型、微型企业投标且部分提供本企业制造的产品，请填写下表内容：</td></tr>
<tr><td>产品名称（品牌、型号）</td><td colspan="2">制造商</td><td>制造商
企业类型</td><td>金额</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="4">本企业小型、微型企业产品金额合计①</td><td></td></tr>
<tr><td colspan="5">（ ）小型、微型企业投标且提供其它小型、微型企业产品的，请填写下表内容：</td></tr>
<tr><td>产品名称（品牌、型号）</td><td colspan="2">制造商</td><td>制造商
企业类型</td><td>金额</td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td></td><td colspan="2"></td><td></td><td></td></tr>
<tr><td colspan="4">其它企业小型、微型企业产品金额合计②</td><td></td></tr>
<tr><td colspan="4">小型、微型企业产品金额总计（①+②）</td><td></td></tr>
<tr><td rowspan="6">节能产品</td><td>产品名称（品牌、型号）</td><td>制造商</td><td>强制/优先采购品目</td><td>认证证书编号</td><td>金额</td></tr>
<tr><td></td><td></td><td>强制品目</td><td></td><td></td></tr>
<tr><td></td><td></td><td>优先品目</td><td></td><td></td></tr>
<tr><td colspan="4">节能产品金额合计</td><td></td></tr>
<tr><td colspan="4">比重（优先采购节能产品金额/投标总价）</td><td>%</td></tr>
<tr><td colspan="5">节能产品证明材料见第___至___页。</td></tr>
<tr><td rowspan="2">环境标志产品</td><td>产品名称（品牌、型号）</td><td>制造商</td><td colspan="2">认证证书编号</td><td>金额</td></tr>
<tr><td></td><td></td><td colspan="2"></td><td></td></tr>
</table>

	环境标志产品金额合计			
	比重（环境标志产品金额/投标总价）			%
	环境标志产品证明材料见第___至___页。			

填报要求：

1、本表的产品名称、规格型号和注册商标、金额应与《报价明细表》一致。

2、制造商为小型或微型企业时才需要填“制造商企业类型”栏，填写内容为“小型”或“微型”。

3、节能产品、环境标志产品必须是《节能产品政府采购清单》或《环境产品政府采购清单》所列品目范围内，且由国家确定的认证机构出具、处于有效期之内的节能产品、环境标志产品认证证书的产品。（需附上相关认证证书）

4、请供应商正确填写本表，所填内容将作为评审的依据。其内容或数据应与对应的证明资料相符，如果不一致，可能导致该项无法获得相关政策优惠。

5、政策优惠得分按照下浮率 b%对首次报价的产品适用政府采购政策情况表中的单价进行统一下浮。

下浮率 b%的计算方法=1-最终报价总价/首次报价总价。

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

日期：

附表 1：中小微企业声明函（中小微型企业适用；事业单位、民办非企业单位参与磋商的，其本身不作为扶持对象）

中小微企业声明函

本单位郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库〔2011〕181 号）的规定，本单位为_____（请填写：中型、小型、微型）企业。即，本单位同时满足以下条件：

1.根据《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业〔2011〕300 号）规定的划分标准，本单位为_____（请填写：中型、小型、微型）企业。

2.本单位参加_____单位的_____项目采购活动提供本企业制造的货物，由本企业承担工程、提供服务，或者提供其他_____（请填写：中型、小型、微型）企业制造的货物。本条所称货物不包括使用大型企业注册商标的货物。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

若提供其他小微企业制造的货物，必须同时提供如下该小微企业的声明函。

小微企业声明函（制造商）

本公司郑重声明，根据《政府采购促进中小企业发展暂行办法》（财库[2011]181 号）的规定和《工业和信息化部、国家统计局、国家发展和改革委员会、财政部关于印发中小企业划型标准规定的通知》（工信部联企业[2011]300 号）规定的划分标准：第四条第_____项_____行业，本公司（此处填写营业收入或从业人员的具体数据），为_____（请填写：中型、小型、微型）企业。

本公司对上述声明的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

附表 2：残疾人福利性单位声明函

残疾人福利性单位声明函

本单位郑重声明，根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕 141 号）的规定，本单位为符合条件的残疾人福利性单位，且本单位参加_____单位的_____项目采购活动提供本单位制造的货物（由本单位承担工程/提供服务），或者提供其他残疾人福利性单位制造的货物（不包括使用非残疾人福利性单位注册商标的货物）。

本单位对上述声明的真实性负责。如有虚假，将依法承担相应责任。

单位名称（盖章）：

日 期：

注：根据《财政部 民政部 中国残疾人联合会关于促进残疾人就业政府采购政策的通知》（财库〔2017〕141 号）的规定，符合条件的残疾人福利性单位在参加政府采购活动时，按以上格式提供《残疾人福利性单位声明函》，视同小型、微型企业，享受评审中价格扣除等促进中小企业发展的政府采购政策，残疾人福利性单位属于小型、微型企业的，不重复享受政策。

4-6 实质性响应一览表

项目名称： 项目编号：

序号	磋商文件要求	供应商响应情况描述	供应商应答（完全响应/正偏离/负偏离）	对应响应文件位置及页码
1	磋商保证金：按磋商须知前附表要求提交			
2	（预算金额）：人民币 151.7 万元			
3	磋商有效期：从磋商截止之日起 90 日内			
4	磋商文件签署和盖章符合要求			
5	本项目不接受备选方案，不接受有任何选择或具有附加条件的报价，磋商响应文件的报价只允许唯一方案报价。否则，磋商小组将对其作无效处理。			
6	磋商文件中标注“★”的条款			

注：如磋商文件中标有“★”的内容，请在上表填写，并作出一一响应。若有一项带“★”的指标要求未响应或不满足，其响应文件作无效处理。

（此表可延长）

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

日期：

4-7 报价响应与磋商文件差异一览表

供应商对磋商文件中 “▲”标注条款的响应情况

序号	磋商文件中“▲”标注的内容	供应商响应情况描述	对采购文件的偏离说明（正偏离/完全响应/负偏离）	对应响应文件位置及页码
	……			

说明：

1.请供应商将磋商文件中“▲”标注的相关要求的响应情况按顺序逐条列入此表。

2.此表可延长。

3.磋商文件若无“▲”标注的条款，则上表留空。

供应商对用户需求的响应情况（标 “▲”的条款除外）

序号	磋商文件要求	供应商响应情况描述	对采购文件的偏离说明（正偏离/完全响应/负偏离）	对应响应文件位置及页码
	……			

说明：

1.把用户需求相关要求的响应情况逐条列入此表。

2.按用户需求的顺序填写。

3.此表可延长。

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

日期：

4-8 供应商基本情况表

一、供应商基本情况

1、供应商名称：_____ 电话号码：_____

2、地　　址：_____ 传　　真：_____

3、注册资金：_____ 经济性质：_____

4、供应商开户账号资料

银行名称及账号：_____

开户地址：_____

二、供应商简介

（自行描述）

三、供应商财务情况

年份	年营业总值	总净利	资产负债率

四、供应商获得的资质和获奖证明文件

证书名称	发证单位	证书等级	证书有效期

所有证明文件需提供复印件（加盖公章）

五、其他

1、参加政府采购活动前三年内，在经营活动中的重大违法记录（须如实填写，若对此进行隐瞒，

尔后又被采购人或采购代理机构发现，或被它人举证成立，其磋商资格将被取消）。

时 间	**受处理的原因** （注明采购项目名称及处理原因）	**处理的内容** （如受到禁止一段时期参加全国范围内某种项目的采购活动的，同时说明解禁时间）	**备 注**

2、其他供应商认为有必要提供的其他证明有关技术、资金实力的资质材料，所有证明文件需提供复印件（加盖公章）

供应商标记样本 （即 LOGO，如无,无须标记）	供应商公章样本

我/我们声明以上所述是正确无误的，您有权进行您认为必要的所有调查。

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

日期：

4-9 项目经理/项目负责人简历表

姓名		性别		年龄	
职务		职称		学历	
办公电话		住宅电话		移动电话	
参加工作时间		从事项目经理/负责人年限			
具有认证资质					
从事过的项目列表					
采购单位	项目名称	项目规模	日期	项目验收情况	

注：提供相关资质、资格证明文件复印件，及在本单位任职的外部证明材料（如加盖所在地区政府有关部门印章的打印日期在本项目提交响应文件截止日之前六个月以内任一月的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等。

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

日期：

4-10 拟为本项目配置的人员情况表

序号	姓名	年龄	学历	获得有关的资质证书	经验年限	主要资历、经验及承担过的项目	拟在本项目担任的工作

注：提供相关资质、资格证明文件复印件，及在本单位任职的外部证明材料（如加盖所在地区政府有关部门印章的打印日期在本项目提交响应文件截止日之前六个月以内任一月的《投保单》或《社会保险参保人员证明》，或单位代缴个人所得税税单等。

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

日期：

4-11 类似项目一览表

序号	业主名称	项目名称	合同金额	签约及完成时间	验收情况	单位联系人及电话

（此表可延长）

注：需提供合同复印件。

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

日期：

4-12 保证金退还说明

致： 广东志正招标有限公司

我方为 2020 年省戒毒局机关网络安全项目 （项目编号：440000-202009-202001-0041）磋商所提交的保证金_____元，请贵公司退还时划到下列账户：

收款单位：

开户银行：

账　　号：

联系人：

联系人电话：

供应商名称(并加盖公章)：

供应商法定代表人或其委托人签名或印鉴：_____

日期：

4-13 采购代理服务费承诺书

致：**广东志正招标有限公司：**

如果我方在贵公司组织的 2020 年省戒毒局机关网络安全项目 （项目编号：_____）磋商中获成交，我方保证在收取《成交通知书》后，按磋商文件规定向贵公司交纳采购代理服务费。

我方如违约，愿凭贵公司开出的违约通知，按采购代理服务费的 200%接受处罚，从我方提交的磋商保证金中支付；以银行保函（或《政府采购磋商担保函》）方式提交磋商保证金时，同意和要求磋商保函开立银行（或开立《政府采购磋商担保函》的担保机构）应广东志正招标有限公司的要求办理支付手续；不足部分由采购人在支付我方的成交合同款中代为扣付，并愿承担全部由此引起的法律责任。

特此承诺！

供应商法定名称（公章）；

供应商法定地址：

供应商授权代表（签名或印鉴）：

电　　话：

传　　真：

承诺日期：

以下磋商保函、政府采购磋商担保函、联合体共同磋商协议书格式文件由供应商根据需要选用。

4-14 磋商保函（已通过其他方式提交保证金的，无须提供）

（不符合磋商文件要求的保函有被拒收的风险）

开具日期： 年 月 日

不可撤销保函第_____号

致：**广东志正招标有限公司**

本保函作为_____*(供应商名称)*_____(以下简称供应商)响应采购项目编号 440000-202009-202001-0041 的 2020 年省戒毒局机关网络安全项目 采购项目的磋商邀请提供的磋商保证金，_____（*开具银行名称*）_____在此无条件及不可撤销地具结保证并承诺，本行或其后继者或受让人一旦收到贵方提出的下述任何一种情况的书面通知（贵方不需要说明理由，不需要提供证明），立即无条件地向贵方支付人民币（大写）_____元整［保证金金额］((小写)￥_____元 ）：

1. 从提交首次响应文件截止之日起到磋商有效期满前，供应商撤回响应文件；
2. 供应商未能按成交通知书的要求与采购人签订合同；
3. 供应商未能及时按磋商文件及成交通知书的要求交纳采购代理服务费；
4. 成交供应商未能按《供应商须知》的要求在规定期限内提交履约保证金。

本保函自出具之日起至该磋商有效期满后 30 天内持续有效，除非贵方提前终止或解除本保函。如果贵方和供应商同意需延长本保函有效期，只需在到期日前书面通知本行，本保函在任何延长的有效期内保持有效。本保函适用于中华人民共和国法律并按其进行解释。

银行名称（打印）(公章)：

银行地址： 邮政编码：

联系电话： 传真号：

法定代表人或其授权的代理人亲笔签字或印鉴：

法定代表人或其授权的代理人姓名和职务（打印）：姓名_____职务_____

4-15 政府采购磋商担保函（已通过其他方式提交保证金的，无须提供）

_____（采购人或采购代理机构）：

鉴于_____（以下简称‘供应商’）拟参加 2020 年省戒毒局机关网络安全项目_____（项目编号：_____）（以下简称‘本项目’）磋商，根据本项目磋商文件，供应商参加磋商时应向贵方交纳磋商保证金，且可以磋商担保函的形式交纳磋商保证金。应供应商的申请，我方以保证的方式向贵方提供如下磋商保证金担保：

一、保证责任的情形及保证金额

（一）在供应商出现下列情形之一时，我方承担保证责任：

1．获得成交资格后供应商无正当理由不与采购人或者采购代理机构签订《政府采购合同》；

2．磋商文件规定的供应商应当缴纳保证金的其他情形。

（二）我方承担保证责任的最高金额为人民币_____元（大写_____），即本项目的磋商保证金金额。

二、保证的方式及保证期间

我方保证的方式为：连带责任保证。

我方的保证期间为：自本保函生效之日起____个月止。

三、承担保证责任的程序

1．贵方要求我方承担保证责任的，应在本保函保证期间内向我方发出书面索赔通知。索赔通知应写明要求索赔的金额，支付款项应到达的账号，并附有证明供应商发生我方应承担保证责任情形的事实材料。

2．我方在收到索赔通知及相关证明材料后，在_____个工作日内进行审查，符合应承担保证责任情形的，我方应按照贵方的要求代供应商向贵方支付磋商保证金。

四、保证责任的终止

1．保证期间届满贵方未向我方书面主张保证责任的，自保证期间届满次日起，我方保证责任自动终止。

2．我方按照本保函向你贵方履行了保证责任后，自我方向你贵方支付款项（支付款项从我方账户划出）之日起，保证责任终止。

3．按照法律法规的规定或出现我方保证责任终止的其它情形的，我方在本保函项下的保证责任亦终止。

五、免责条款

1．依照法律规定或贵方与供应商的另行约定，全部或者部分免除供应商磋商保证金义务时，

我方亦免除相应的保证责任。

2．因贵方原因致使供应商发生本保函第一条第（一）款约定情形的，我方不承担保证责任。

3．因不可抗力造成供应商发生本保函第一条约定情形的，我方不承担保证责任。

4．贵方或其他有权机关对磋商文件进行任何澄清或修改，加重我方保证责任的，我方对加重部分不承担保证责任，但该澄清或修改经我方事先书面同意的除外。

六、争议的解决

因本保函发生的纠纷，由你我双方协商解决，协商不成的，通过诉讼程序解决，诉讼管辖地法院为_____法院。

七、保函的生效

本保函自我方加盖公章之日起生效。

保证人：（公章）

年 月 日

备注：此为政府采购磋商担保函样本，仅供参考。供应商可根据实际情况自行提供，但不能偏离且不限于以上实质性内容！

4-16 联合体共同磋商协议书（如联合体参与磋商，需提供）

（联合体各方名称）在 2020 年省戒毒局机关网络安全项目（项目编号：）中组成联合体，共同参加磋商。就本项目有关事宜，经各方充分协商一致，达成如下协议：

一、由为本次磋商联合体主体方，为协办方，组成联合体共同进行本项目的磋商工作。

二、联合体以一个供应商的身份共同参加本项目的磋商，成交后，联合体各方共同与采购人签订合同，就本项目对采购人承担连带责任。

三、联合体授权主体方负责本项目的一切组织、协调工作，主体方在报价、合同磋商过程中所签署的一切文件和处理的与本次磋商有关的一切事务,联合体各方均予以承认并承担法律责任。

四、主体方 负责 工作，协办方负责工作。具体工作范围、工作内容以合同为准。

五、联合体成员为（请填写：小型、微型）企业，将承担合同总金额%的工作内容**（联合体成员中有小型、微型企业时适用）**。

六、各方的责任、权利和义务的详细内容和规定在成交后经各方协商后报采购人同意另行签署协议或者合同。

七、联合体各方不得再以自己的名义在本项目中单独提交响应文件，联合体项目责任人不能作为其他联合体或单独供应商的项目组成员。如因发生上述问题而导致联合体报价无效的，联合体其他成员可追究违约责任。

八、联合体如因违约过失责任而导致采购人经济损失或被索赔时，本联合体任何一方均同意无条件优先清偿采购人的一切债务和经济赔偿。

九、本协议在自签署之日起生效，有效期内有效，如获成交资格，合同有效期延续至合同履行完毕之日。如联合体未获成交资格，本协议自动废止。

主体方全称：（公章）	协办方全称：（公章）
法定代表人姓名：（签名或印鉴）	法定代表人姓名：（签名或印鉴）
地址：	地址：
邮政编码：	邮政编码：
联系电话：	联系电话：
签署日期：	签署日期：

备注：联合体各方成员须在本协议上共同盖章和签署。

第五章 响应文件技术部分

建议包括以下内容：

对项目特点的认识和理解

对项目重点、难点分析

项目实施服务方案

进度计划安排及保证进度的承诺

保证服务质量的措施、出现异常情况下的补救措施及服务承诺

供应商认为必要的其他技术资料

附件：政府采购履约担保函（提交磋商响应文件时无需提供）

政府采购履约担保函

编号：

_____（采购人）：

鉴于你方与_____（以下简称供应商）于___年__月__日签定编号为_____的《_____政府采购合同》(以下简称主合同),且依据该合同的约定,供应商应在____年____月日前向你方交纳履约保证金，且可以履约担保函的形式交纳履约保证金。应供应商的申请，我方以保证的方式向你方提供如下履约保证金担保：

一、保证责任的情形及保证金额

（一）在供应商出现下列情形之一时，我方承担保证责任：

1．将成交项目转让给他人，或者在响应文件中未说明，且未经采购招标机构人同意，将成交项目分包给他人的；

2．主合同约定的应当缴纳履约保证金的情形:

（1）未按主合同约定的质量、数量和期限供应货物/提供服务/完成工程的；

（2）_____。

（二）我方的保证范围是主合同约定的合同价款总额的_____%数额为_____元（大写_____），币种为_____。（即主合同履约保证金金额）

二、保证的方式及保证期间

我方保证的方式为：连带责任保证。

我方保证的期间为：自本合同生效之日起至供应商按照主合同约定的供货/完工期限届满后日内。

如果供应商未按主合同约定向贵方供应货物/提供服务/完成工程的，由我方在保证金额内向你方支付上述款项。

三、承担保证责任的程序

1．你方要求我方承担保证责任的，应在本保函保证期间内向我方发出书面索赔通知。索赔通知应写明要求索赔的金额，支付款项应到达的帐号。并附有证明供应商违约事实的证明材料。

如果你方与供应商因货物质量问题产生争议，你方还需同时提供_____部门出具的质量检测报告，或经诉讼（仲裁）程序裁决后的裁决书、调解书，本保证人即按照检测结果或裁决书、调解书决定是否承担保证责任。

2． 我方收到你方的书面索赔通知及相应证明材料，在_____工作日内进行核定后按照本保函

的承诺承担保证责任。

四、保证责任的终止

1．保证期间届满你方未向我方书面主张保证责任的，自保证期间届满次日起，我方保证责任自动终止。保证期间届满前，主合同约定的货物\工程\服务全部验收合格的，自验收合格日起，我方保证责任自动终止。

2．我方按照本保函向你方履行了保证责任后，自我方向你方支付款项（支付款项从我方账户划出）之日起，保证责任即终止。

3．按照法律法规的规定或出现应终止我方保证责任的其它情形的，我方在本保函项下的保证责任亦终止。

4．你方与供应商修改主合同，加重我方保证责任的，我方对加重部分不承担保证责任，但该等修改事先经我方书面同意的除外；你方与供应商修改主合同履行期限，我方保证期间仍依修改前的履行期限计算，但该等修改事先经我方书面同意的除外。

五、免责条款

1．因你方违反主合同约定致使供应商不能履行义务的，我方不承担保证责任。

2．依照法律法规的规定或你方与供应商的另行约定，全部或者部分免除供应商应缴纳的保证金义务的，我方亦免除相应的保证责任。

3．因不可抗力造成供应商不能履行供货义务的，我方不承担保证责任。

六、争议的解决

因本保函发生的纠纷，由你我双方协商解决，协商不成的，通过诉讼程序解决，诉讼管辖地法院为_____法院。

七、保函的生效

本保函自我方加盖公章之日起生效。

保证人：（公章）

年 月 日