代理机构内部编号：SJJCZB2025017

松江区“雪亮工程”综治分平台安全加固升级扩容采购项目

招标文件

采 购 人：中共上海市松江区委政法委员会

集中采购机构：上海市松江区政府采购中心

2025年08月29日

2025年08月29日

目　录

第一章　投标邀请

项目概况

松江区“雪亮工程”综治分平台安全加固升级扩容招标项目的潜在投标人应在上海政府采购网获取招标文件，并于 2025-09-25 10:00:00（北京时间）前递交投标文件。

一、项目基本情况

项目编号：**310117000250828131621-17268790**

项目名称：**松江区“雪亮工程”综治分平台安全加固升级扩容**

预算编号：1725-000173812，1725-K00003603

预算金额（元）：**11858902.00 元（国库资金 11858902.00 元；自筹资金：0 元）**

最高限价（元）：**包 1-11858902.00 元**

采购需求：

包名称：**松江区“雪亮工程”综治分平台安全加固升级扩容**

数量：2

预算金额（元）：**11858902.00 元**

简要规格描述或项目基本概况介绍、用途：**本项目采购态势分析与安全运营系统、防火墙、安全审计、堡垒机等安全设备，按照信息系统安全等级保护三级标准完善松江区“雪亮工程”社会面（社区）公共安全视频监控平台的网络和数据安全防范能力，同时结合综治实际工作的需要采购物联感知数据接入平台系统及相关配套设备实现对物联感知数据的统一管理和应用。**

合同履约期限：**合同签订后 180 天之内完成。**

本项目**不允许**接受联合体投标。

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：本项目面向大、中、小、微型等各类供应商采购。

3.本项目的特定资格要求：

1、符合《中华人民共和国政府采购法》第二十二条的规定。

2、未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）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。

3、本项目不接受联合体投标。

三、获取招标文件

时间：2025-09-01 至 2025-09-08，每天上午 00:00:00~12:00:00，下午 12:00:00~23:59:59（北京时间，法定节假日除外）

地点：上海政府采购网

方式：网上获取

售价（元）：0

四、提交投标文件截止时间、开标时间和地点

提交投标文件截止时间：2025-09-25 10:00:00（北京时间）

投标地点：上海政府采购网（www.zfcg.sh.gov.cn）

开标时间：2025-09-25 10:00:00

开标地点：上海政府采购网（www.zfcg.sh.gov.cn）

五、公告期限

自本公告发布之日起 5 个工作日。

六、其他补充事宜

七、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：**中共上海市松江区委政法委员会**

地 址：**上海市松江区园中路 1 号**

联系方式：021-37739396

2.采购代理机构信息

名 称：**上海市松江区政府采购中心**

地 址：**上海市松江区松礼路（地铁 9 号线上海松江站 2 号口）上海市松江区政务服务中心 3 楼 3203 室**

联系方式：57746172

3.项目联系方式

项目联系人：**单老师**

电话：57746172

第二章　　投标人须知

前附表

一、项目情况

项目名称:**松江区“雪亮工程”综治分平台安全加固升级扩容**

项目编号：详见投标邀请

项目地址：详见投标邀请

项目内容：详见投标邀请

采购预算：详见投标邀请

采购预算说明：本项目采购预算为 11858902.00 元人民币，超过采购预算的报价不予接受。

采购标的对应的中小企业划分标准所属行业：工业。

二、招标人

采购人

名称：**中共上海市松江区委政法委员会**

地址：**上海市松江区园中路 1 号**

联系人：**欧阳老师**

电话：**021-37739396**

传真：**021-37735470**

集中采购机构

名称：**上海市松江区政府采购中心**

地址：**上海市松江区松礼路（地铁 9 号线上海松江站 2 号口）上海市松江区政务服务中心 3 楼 3203 室**

联系人：**单老师**

电话：**57746172**

传真：**67743657**

三、合格供应商条件

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：本项目面向大、中、小、微型等各类供应商采购。

3.本项目的特定资格要求：

1、符合《中华人民共和国政府采购法》第二十二条的规定。

2、未被“信用中国”（www.creditchina.gov.cn）、中国政府采购网（www.ccgp.gov.cn）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。

3、本项目不接受联合体投标。

四、招标有关事项

1、招标答疑会：不召开

2、踏勘现场：不集中组织

3、投标有效期：自开标之日起 90 日

4、投标保证金：不收取

5、投标截止时间：详见投标邀请（招标公告）或延期公告（如果有的话）

6、递交投标文件方式和网址

投标文件递交方式：由投标人在上海市政府采购云平台（门户网站：上海政府采购网）提交。

投标文件递交网址：http://www.zfcg.sh.gov.cn

7、开标时间和开标地点网址：

开标时间：同投标截止时间

开标网址：上海市政府采购云平台（门户网站：上海政府采购网，网址：http://www.zfcg.sh.gov.cn)。

8、评标委员会的组建：详见第五章《评标方法与程序》。

9、评标方法：详见第五章《评标方法与程序》

10、中标人推荐办法：详见第五章《评标方法与程序》

五、其它事项

1、付款方式：详见第四章《招标需求》

2、质量保证期：详见第四章《招标需求》

3、交付日期：详见第四章《招标需求》

4、转让与分包：详见第四章《招标需求》

5、履约保证金：不收取

六、说明

根据上海市财政局《关于上海市政府采购云平台第三批单位上线运行的通知》的规定，本项目采购相关活动在由市财政局建设和维护的上海市政府采购云平台（简称：采购云平台，门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）进行。供应商应根据《上海市电子政府采购管理暂行办法》等有关规定和要求执行。供应商在采购云平台的有关操作方法可以参照采购云平台中的“操作须知”专栏的有关内容和操作要求办理。

投标人应在投标截止时间前尽早加密上传投标文件，电话通知招标人进行签收，并及时查看招标人在电子采购平台上的签收情况，打印签收回执，以免因临近投标截止时间上传造成招标人无法在开标前完成签收的情形。未签收的投标文件视为投标未完成。

投标人须知

一、总则

1．概述

1．1 根据《中华人民共和国政府采购法》、《中华人民共和国招标投标法》等有关法律、法规和规章的规定，本采购项目已具备招标条件。

1．2 本招标文件仅适用于《投标邀请（招标公告）》和《投标人须知》前附表中所述采购项目的招标采购。

1．3 招标文件的解释权属于《投标邀请（招标公告）》和《投标人须知》前附表中所述的招标人。

1．4 参与招标投标活动的所有各方，对在参与招标投标过程中获悉的国家、商业和技术秘密以及其它依法应当保密的内容，均负有保密义务，违者应对由此造成的后果承担全部法律责任。

1.5 根据上海市财政局《关于上海市政府采购云平台第三批单位上线运行的通知》的规定，本项目招投标相关活动在上海市政府采购云平台（门户网站：上海政府采购网，网址：www.zfcg.sh.gov.cn）进行。

2．定义

2．1 “采购项目”系指招标人在招标文件里描述的所需采购的货物和相关服务。

2．2 “货物”系指投标人按招标文件规定，须向采购人提供的各种形态和种类的物品，包括一切设备、产品、机械、仪器仪表、备品备件、工具、手册等有关技术资料和原材料等。

2．3 “相关服务”系指招标文件规定投标人须承担的与其所提供货物相关的运输、就位、安装、调试、技术协助、校准、培训、技术指导以及其他类似的义务。

2．4“招标人”系指《投标人须知》前附表中所述的组织本次招标的集中采购机构和采购人。

2．5“投标人”系指从招标人处按规定获取招标文件，并按照招标文件向招标人提交投标文件的供应商。

2．6 “中标人”系指中标的投标人。

2．7 “甲方”系指采购人。

2．8 “乙方”系指中标并向采购人提供货物和相关服务的投标人。

2．9 招标文件中凡标有“★”的条款均系实质性要求条款。

2.10“采购云平台”系指上海市政府采购云平台，门户网站为上海政府采购网（www.zfcg.sh.gov.cn），是由市财政局建设和维护。

3．合格的投标人

3.1 符合《投标邀请（招标公告）》和《投标人须知》前附表中规定的合格投标人所必须具备的资格条件和特定条件。

3.2 《投标邀请（招标公告）》和《投标人须知》前附表规定接受联合体投标的，除应符合本章第 3.1 项要求外，还应遵守以下规定：

（1）联合体各方应按招标文件提供的格式签订联合体协议书，明确联合体各方权利义务、合同份额；联合体协议书应当明确联合体主办方、由主办方代表联合体参加采购活动；

（2）联合体中有同类资质的供应商按联合体分工承担相同工作的，应当按照资质等级较低的供应商确定资质等级；

（3）招标人根据采购项目的特殊要求规定投标人特定条件的，联合体各方中至少应当有一方符合采购规定的特定条件。

（4）联合体各方不得再单独参加或者与其他供应商另外组成联合体参加同一合同项下的政府采购活动。

4．合格的货物和相关服务

4．1 投标人对所提供的货物应当享有合法的所有权，没有侵犯任何第三方的知识产权、技术秘密等权利，而且不存在任何抵押、留置、查封等产权瑕疵。

4．2 投标人提供的货物应当是全新的、未使用过的，货物和相关服务应当符合招标文件的要求，并且其质量完全符合国家标准、行业标准或地方标准，均有标准的以高（严格）者为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合采购目的的特定标准确定。

4.3 投标人应当说明投标货物的来源地，如投标的货物非投标人生产或制造的，则应当按照《招标需求》的要求提供其从合法途径获得该货物的相关证明。

5．投标费用

不论投标的结果如何，投标人均应自行承担所有与投标有关的全部费用，招标人在任何情况下均无义务和责任承担这些费用。

6． 信息发布

本采购项目需要公开的有关信息，包括招标公告、招标文件澄清或修改公告、中标公告以及延长投标截止时间等与招标活动有关的通知，招标人均将通过“上海政府采购网”（http://www.zfcg.sh.gov.cn）和“松江区门户网”（ http://www.songjiang.gov.cn）公开发布。投标人在参与本采购项目招投标活动期间，请及时关注以上媒体上的相关信息，投标人因没有及时关注而未能如期获取相关信息，及因此所产生的一切后果和责任，由投标人自行承担，招标人在任何情况下均不对此承担任何责任。

7．询问与质疑

7．1 投标人对招标活动事项有疑问的，可以向招标人提出询问。询问可以采取电话、电子邮件、当面或书面等形式。对投标人的询问，招标人将依法及时作出答复，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7．2 投标人认为招标文件、招标过程或中标结果使自己的合法权益受到损害的，可以在知道或者应知其权益受到损害之日起七个工作日内，以书面形式向招标人提出质疑。其中，对招标文件的质疑，应当在其收到招标文件之日（以采购云平台显示的报名时间为准）起七个工作日内提出；对招标过程的质疑，应当在各招标程序环节结束之日起七个工作日内提出；对中标结果的质疑，应当在中标公告期限届满之日起七个工作日内提出。

投标人应当在法定质疑期内一次性提出针对同一采购程序环节的质疑，超过次数的质疑将不予受理。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。

7. 3 投标人可以委托代理人进行质疑。代理人提出质疑应当提交投标人签署的授权委托书，并提供相应的身份证明。授权委托书应当载明代理人的姓名或者名称、代理事项、具体权限、期限和相关事项。投标人为自然人的，应当由本人签字；投标人为法人或者其他组织的，应当由法定代表人、主要负责人签字或者盖章，并加盖公章。

7.4 投标人提出质疑应当提交质疑函和必要的证明材料。质疑函应当包括下列内容：

（1）供应商的姓名或者名称、地址、邮编、联系人及联系电话；

（2）质疑项目的名称、编号；

（3）具体、明确的质疑事项和与质疑事项相关的请求；

（4）事实依据；

（5）必要的法律依据；

（6）提出质疑的日期。

投标人为自然人的，应当由本人签字；投标人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者盖章，并加盖公章。

质疑函应当按照财政部制定的范本填写，范本格式可通过中国政府采购网（http://www.ccgp.gov.cn）右侧的“下载专区”下载。

7.5 投标人提起询问和质疑，应当按照《政府采购质疑和投诉办法》（财政部令第 94 号）的规定办理。质疑函或授权委托书的内容不符合《投标人须知》第 7.3 条和第 7.4 条规定的，招标人将当场一次性告知投标人需要补正的事项，投标人超过法定质疑期未按要求补正并重新提交的，视为放弃质疑。

质疑函的递交应当采取当面递交形式，质疑联系部门：上海市松江区政府采购中心，联系电话：021-57746172，地址：上海市松江区松礼路（地铁 9 号线上海松江站 2 号口）上海市松江区政务服务中心 3 楼 3203 室。

7. 6 招标人将在收到投标人的书面质疑后七个工作日内作出答复，并以书面形式通知提出质疑的投标人和其他有关投标人，但答复的内容不涉及商业秘密或者依法应当保密的内容。

7. 7 对投标人询问或质疑的答复将导致招标文件变更或者影响招标活动继续进行的，招标人将通知提出询问或质疑的投标人，并在原招标公告发布媒体上发布变更公告。

8. 公平竞争和诚实信用

8. 1 投标人在本招标项目的竞争中应自觉遵循公平竞争和诚实信用原则，不得存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为。“腐败行为”是指提供、给予任何有价值的东西来影响采购人员在采购过程或合同实施过程中的行为；“欺诈行为”是指为了影响采购过程或合同实施过程而提供虚假材料，谎报、隐瞒事实的行为，包括投标人之间串通投标等。

8. 2 如果有证据表明投标人在本招标项目的竞争中存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为，招标人将拒绝其投标，并将报告政府采购监管部门查处；中标后发现的，中标人须参照《中华人民共和国消费者权益保护法》第 55 条之条文描述方式双倍赔偿采购人，且民事赔偿并不免除违法投标人的行政与刑事责任。

8.3 招标人将在开标后至评标前，通过“信用中国”网站(www.creditchina.gov.cn)、中国政府采购网(www.ccgp.gov.cn)查询相关投标人信用记录，并对供应商信用记录进行甄别，对列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单、中国政府采购网(www.ccgp.gov.cn)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，将拒绝其参与政府采购活动。以上信用查询记录，招标人将打印查询结果页面后与其他采购文件一并保存。

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，将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. 其他

本《投标人须知》的条款如与《投标邀请》 、 《招标需求》和《评标方法与程序》就同一内容的表述不一致的，以《投标邀请》 、 《招标需求》和《评标方法与程序》中规定的内容为准。

二、招标文件

10. 招标文件构成

10．1 招标文件由以下部分组成：

（1）投标邀请（招标公告）

（2）投标人须知

（3）政府采购政策功能

（4）招标需求

（5）评标方法与程序

（6）投标文件有关格式

（7）合同书格式和合同条款

（8）本项目招标文件的澄清、答复、修改、补充内容（如有的话）。

10．2 投标人应仔细阅读招标文件的所有内容，并按照招标文件的要求提交投标文件。如果投标人没有按照招标文件要求提交全部资料，或者投标文件没有对招标文件在各方面作出实质性响应，则投标有可能被认定为无效标，其风险由投标人自行承担。

10．3、投标人应认真了解本次招标的具体工作要求、工作范围以及职责，了解一切可能影响投标报价的资料。一经中标，不得以不完全了解项目要求、项目情况等为借口而提出额外补偿等要求，否则，由此引起的一切后果由中标人负责。

10．4、投标人应按照招标文件规定的日程安排，准时参加项目招投标有关活动。

11. 招标文件的澄清和修改

11．1 任何要求对招标文件进行澄清的投标人，均应在投标截止期 15 天以前，按《投标邀请（招标公告）》中的地址以书面形式（必须加盖投标人单位公章）通知招标人。

11．2 对在投标截止期 15 天以前收到的澄清要求，招标人需要对招标文件进行澄清、答复的；或者在投标截止前的任何时候，招标人需要对招标文件进行补充或修改的，招标人将会通过“上

海政府采购网”以澄清或修改公告形式发布,并通过采购云平台发送至已下载招标文件的供应商工作区。如果澄清或更正的内容可能影响投标文件编制的，且澄清或修改公告发布时间距投标截止时间不足 15 天的，则相应延长投标截止时间。延长后的具体投标截止时间以最后发布的澄清或修改公告中的规定为准。

11．3 澄清或修改公告的内容为招标文件的组成部分。当招标文件与澄清或修改公告就同一内容的表述不一致时，以最后发出的文件内容为准。

11．4 招标文件的澄清、答复、修改或补充都应由集中采购机构以澄清或修改公告形式发布和通知，除此以外的其他任何澄清、修改方式及澄清、修改内容均属无效，不得作为投标的依据，否则，由此导致的风险由投标人自行承担，招标人不承担任何责任。

11．5 招标人召开答疑会的，所有投标人应根据招标文件或者招标人通知的要求参加答疑会。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。

12．踏勘现场

12．1 招标人组织踏勘现场的，所有投标人应按《投标人须知》前附表规定的时间、地点前往参加踏勘现场活动。投标人如不参加，其风险由投标人自行承担，招标人不承担任何责任。招标人不组织踏勘现场的，投标人可以自行决定是否踏勘现场，投标人需要踏勘现场的，招标人应为投标人踏勘现场提供一定方便，投标人进行现场踏勘时应当服从招标人的安排。

12．2 投标人踏勘现场发生的费用由其自理。

12．3 招标人在现场介绍情况时，应当公平、公正、客观，不带任何倾向性或误导性。

12．4 招标人在踏勘现场中口头介绍的情况，除招标人事后形成书面记录、并以澄清或修改公告的形式发布、构成招标文件的组成部分以外，其他内容仅供投标人在编制投标文件时参考，招标人不对投标人据此作出的判断和决策负责。

三、投标文件

13． 投标的语言及计量单位

13.1 投标人提交的投标文件以及投标人与招标人就有关投标事宜的所有来往书面文件均应使用中文。除签名、盖章、专用名称等特殊情形外，以中文以外的文字表述的投标文件视同未提供。

13．2 投标计量单位，招标文件已有明确规定的，使用招标文件规定的计量单位；招标文件没有规定的，一律采用中华人民共和国法定计量单位（货币单位：人民币元）。

14．投标有效期

14．1 投标文件应从开标之日起，在《投标人须知》前附表规定的投标有效期内有效。投标有效期比招标文件规定短的属于非实质性响应，将被认定为无效投标。

14．2 在特殊情况下，在原投标有效期期满之前，招标人可书面征求投标人同意延长投标有效期。

14．3 中标人的投标文件作为项目合同的附件，其有效期至中标人全部合同义务履行完毕为止。

15． 投标文件构成

15．1 投标文件由商务响应文件（包括相关证明文件）和技术响应文件二部分构成。

15. 2 商务响应文件（包括相关证明文件）和技术响应文件具体应包含的内容，以第四章《招标需求》规定为准。

16． 商务响应文件

16．1 商务响应文件由以下部分组成：

（1）《投标函》

（2）《开标一览表》（在采购云平台填写）

（3）《投标报价分类明细表》等相关报价表格详见第六章《投标文件有关格式》

（4）《资格审查要求表》

（5）《符合性要求表》

（6）《商务要求响应表》

（7）第四章《招标需求》规定的其他内容

（8）相关证明文件（投标人应按照《招标需求》所规定的内容提交相关证明文件，以证明其有资格参加投标和中标后有能力履行合同）

17． 投标函

17．1 投标人应按照招标文件中提供的格式完整地填写《投标函》。

17．2 投标人不按照招标文件中提供的格式填写《投标函》，或者填写不完整的，评标时将按照第五章《评标方法与程序》中的相关规定予以扣分。

17．3 投标文件中未提供《投标函》的，为无效投标。

18． 开标一览表

18．1 投标人应按照招标文件的要求和采购云平台提供的投标文件格式完整地填写《开标一览表》，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

18.2 《开标一览表》是为了便于招标人开标，《开标一览表》内容在开标时将当众公布。

18.3 投标人未按照招标文件的要求和采购云平台提供的投标文件格式完整地填写《开标一览表》、或者未提供《开标一览表》，导致其开标不成功的，其责任和风险由投标人自行承担。

19． 投标报价

19．1 投标人应当按照国家和上海市有关行业管理服务收费的相关规定，结合自身服务水平和承受能力进行报价。投标报价应是履行合同的最终价格，除《招标需求》中另有说明外，投标报价应当是投标人为提供本项目所要求的全部管理服务所发生的一切成本、税费和利润，包括人工（含工资、社会统筹保险金、加班工资、工作餐、相关福利、关于人员聘用的费用等）、设备、国家规定检测、外发包、材料（含辅材）、管理、税费及利润等。

19．2 报价依据：

（1）本招标文件所要求的服务内容、服务期限、工作范围和要求；

（2）本招标文件明确的服务标准及考核方式；

（3）其他投标人认为应考虑的因素。

19．3 投标人提供的服务应当符合国家和上海市有关法律、法规和标准规范，满足合同约定的服务内容和质量等要求。投标人不得违反标准规范规定或合同约定，通过降低服务质量、减少服务内容等手段进行恶性竞争，扰乱正常市场秩序。

19．4 除《招标需求》中说明并允许外，投标的每一种服务的单项报价以及采购项目的投标总价均只允许有一个报价，任何有选择的报价，招标人对于其投标均将予以拒绝。

19．5 投标报价应是固定不变的，不得以任何理由予以变更。任何可变的或者附有条件的投标报价，招标人均将予以拒绝。

19．6 投标人应按照招标文件第六章提供的格式完整地填写各类报价分类明细表，说明其拟提供服务的内容、数量、价格、时间、价格构成等。

19．7 投标应以人民币报价。

20． 资格性审查及符合性要求表

20．1 投标人应当按照招标文件所提供格式，逐项填写并提交《资格审查要求表》以及《符合性要求表》，以证明其投标符合招标文件规定的所有合格投标人资格条件及实质性要求。

20．2 投标文件中未提供《资格审查要求表》或《符合性要求表》的，为无效投标。

21．技术响应文件

21．1 投标人应按照《招标需求》的要求编制并提交技术响应文件，对招标人的技术需求全面完整地做出响应并编制服务方案，以证明其投标的服务符合招标文件规定。

21．2 技术响应文件可以是文字资料、表格、图纸和数据等各项资料，其内容应包括但不限于人力、物力等资源的投入以及服务内容、方式、手段、措施、质量保证及建议等。

22． 投标文件的编制和签署

22．1 投标人应按照招标文件和采购云平台要求的格式填写相关内容。

22．2 投标文件中凡招标文件要求签署、盖章之处，均应显示投标人的法定代表人或法定代表人正式授权的代表签署字样及投标人的公章。投标人名称及公章应显示全称。如果是由法定代表人授权代表签署投标文件，则应当按招标文件提供的格式出具《法定代表人授权委托书》（如投标人自拟授权书格式，则其授权书内容应当实质性符合招标文件提供的《法定代表人授权委托书》格式之内容）并将其附在投标文件中。投标文件若有修改错漏之处，须在修改错漏之处同样显示出投标人公章或者由法定代表人或法定代表人授权代表签署字样。投标文件因字迹潦草或表达不清所引起的后果由投标人自负。

其中对《投标函》 、《法定代表人授权委托书》 、《资格审查要求表》 、《符合性要求表》以及《财务状况及税收、社会保障资金缴纳情况声明函》，投标人未按照上述要求显示公章的，其投标无效。

22．3 建设节约型社会是我国落实科学发展观的一项重大决策，也是政府采购应尽的义务和职责，需要政府采购各方当事人在采购活动中共同践行。目前，少数投标人制作的投标文件存在编写繁琐、内容重复的问题，既增加了制作成本，浪费了宝贵的资源，也增加了评审成本，影响了评审效率。为进一步落实建设节约型社会的要求，提请投标人在制作投标文件时注意下列事项：

（1）评标委员会主要是依据投标文件中技术、质量以及售后服务等指标来进行评定。因此，投标文件应根据招标文件的要求进行制作，内容简洁明了，编排合理有序，与招标文件内容无关或不符合招标文件要求的资料不要编入投标文件。

（2）投标文件应规范，应按照规定格式要求规范填写，扫描文件应清晰简洁、上传文件应规范。

四、投标文件的递交

23. 投标文件的递交

23.1 投标人应按照招标文件规定，参考第六章投标文件有关格式，在采购云平台中按照要求填写和上传所有投标内容。投标的有关事项应根据采购云平台规定的要求办理。

23.2 投标文件中含有公章，防伪标志和彩色底纹类文件（如《投标函》、营业执照、身份证、认证证书等）应清晰显示。如因上传、扫描、格式等原因导致评审时受到影响，由投标人承担相应责任。

招标人认为必要时，可以要求投标人提供文件原件进行核对，投标人必须按时提供，否则投标人须接受可能对其不利的评标结果，并且招标人将对该投标人进行调查，发现有弄虚作假或欺诈行为的按有关规定进行处理。

23.3 投标人应充分考虑到网上投标可能会发生的技术故障、操作失误和相应的风险。对因网上投标的任何技术故障、操作失误造成投标人投标内容缺漏、不一致或投标失败的，招标人不承担任何责任。

24. 投标截止时间

24.1 投标人必须在《投标邀请（招标公告）》规定的网上投标截止时间前将投标文件在采购云平台中上传并正式投标。

24.2 在招标人按《投标人须知》规定酌情延长投标截止期的情况下，招标人和投标人受投标截止期制约的所有权利和义务均应延长至新的截止时间。

24.3 在投标截止时间后上传的任何投标文件，招标人均将拒绝接收。

25. 投标文件的修改和撤回

在投标截止时间之前，投标人可以对在采购云平台已提交的投标文件进行修改和撤回。有关事项应根据采购云平台规定的要求办理。

五、开标

26. 开标

26. 1 招标人将按《投标邀请》或《延期公告》（如果有的话）中规定的时间在采购云平台上组织公开开标。

26.2 开标程序在采购云平台进行，所有上传投标文件的供应商应登录采购云平台参加开标。开标主要流程为签到、解密、唱标和签名，每一步骤均应按照采购云平台的规定进行操作。

26. 3 投标截止，采购云平台显示开标后，投标人进行签到操作，投标人签到完成后，由招标人解除采购云平台对投标文件的加密。投标人应在规定时间内使用数字证书对其投标文件解密。签到和解密的操作时长分别为半小时，投标人应在规定时间内完成上述签到或解密操作，逾期未

完成签到或解密的投标人，其投标将作无效标处理。因系统原因导致投标人无法在上述要求时间内完成签到或解密的除外。

如采购云平台开标程序有变化的，以最新的操作程序为准。

26．4 投标文件解密后，采购云平台根据各投标人填写的《开标一览表》的内容自动汇总生成《开标记录表》。

投标人应及时使用数字证书对《开标记录表》内容进行签名确认，投标人因自身原因未作出确认的视为其确认《开标记录表》内容。

六、评标

27． 评标委员会

27．1 招标人将依法组建评标委员会，评标委员会由采购人代表和上海市政府采购评审专家组成，其中专家的人数不少于评标委员会成员总数的三分之二。

27．2 评标委员会负责对投标文件进行评审和比较，并向招标人推荐中标候选人。

28． 投标文件的资格审查及符合性审查

28．1 开标后，招标人将依据法律法规和招标文件的《投标人须知》、《资格审查要求表》，对投标人进行资格审查。确定符合资格的投标人不少于 3 家的，将组织评标委员会进行评标。

28．2 在详细评标之前，评标委员会要对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。评标委员会只根据投标文件本身的内容来判定投标文件的响应性，而不寻求外部的证据。

28．3 符合性审查未通过的投标文件不参加进一步的评审，投标人不得通过修正或撤销不符合要求的偏离或保留从而使其投标成为实质上响应的投标。

28．4 开标后招标人拒绝投标人主动提交的任何澄清与补正。

28．5 招标人可以接受投标文件中不构成实质性偏差的小的不正规、不一致或不规范的内容。

29． 投标文件内容不一致的修正

29．1 投标文件报价出现前后不一致的，按照下列规定修正：

（1）《开标记录表》报价与投标文件中报价不一致的，以《开标记录表》为准；

（2）大写金额和小写金额不一致的，以大写金额为准；

（3）单价金额小数点或者百分比有明显错位的，以开标记录表的总价为准，并修改单价；

（4）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。

同时出现两种以上不一致的，按照上述规定的顺序修正。修正后的报价经投标人确认后产生约束力，投标人不确认的，其投标无效。

29．2 《开标记录表》内容与投标文件中相应内容不一致的，以《开标记录表》为准。

29．3 投标文件中如果有其他与评审有关的因素前后不一致的，将按不利于出错投标人的原则进行处理，即对于不一致的内容，评标时按照对出错投标人不利的情形进行评分；如出错投标人中标，签订合同时按照对出错投标人不利、对采购人有利的条件签约。

30． 投标文件的澄清

30．1 对于投标文件中含义不明确或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清。投标人应按照招标人通知的时间和地点委派授权代表向评标委员会作出说明或答复。

30．2 投标人对澄清问题的说明或答复，还应以书面形式提交给招标人，并应由投标人授权代表签字。

30．3　投标人的澄清文件是其投标文件的组成部分。

30．4　投标人的澄清不得超出投标文件的范围或者改变其投标文件的实质性内容，不得通过澄清而使进行澄清的投标人在评标中更加有利。

31．投标文件的评价与比较

31．1　评标委员会只对被确定为实质上响应招标文件要求的投标文件进行评价和比较。

31．2　评标委员会根据《评标方法与程序》中规定的方法进行评标，并向招标人提交书面评标报告和推荐中标候选人。

32．　评标的有关要求

32．1 评标委员会应当公平、公正、客观，不带任何倾向性，评标委员会成员及参与评标的有关工作人员不得私下与投标人接触。

32．2 评标过程严格保密。凡是属于审查、澄清、评价和比较有关的资料以及授标建议等，所有知情人均不得向投标人或其他无关的人员透露。

32．3 任何单位和个人都不得干扰、影响评标活动的正常进行。投标人在评标过程中所进行的试图影响评标结果的一切不符合法律或招标规定的活动，都可能导致其投标被拒绝。

32．4 招标人和评标委员会均无义务向投标人做出有关评标的任何解释。

七、定标

33．确认中标人

除了《投标人须知》第 36 条规定的招标失败情况之外，采购人将根据评标委员会推荐的中标候选人及排序情况，依法确认本采购项目的中标人。

34．　中标公告及中标和未中标通知

34．1 采购人确认中标人后，招标人将在两个工作日内通过“上海政府采购网” 和“松江区门户网”发布中标公告，公告期限为一个工作日。

34.2 中标公告发布同时，招标人将及时向中标人发出《中标通知书》通知中标，向其他未中标人发出《中标结果通知书》。《中标通知书》对招标人和投标人均具有法律约束力。

35．投标文件的处理

所有在开标会上被接受的投标文件都将作为档案保存,不论中标与否，招标人均不退回投标文件。

36．招标失败

在投标截止后，参加投标的投标人不足三家；在资格审查时，发现符合资格条件的投标人不足三家的；或者在评标时，发现对招标文件做出实质性响应的投标人不足三家，评标委员会确定为招标失败的，招标人将通过“上海政府采购网” 和“松江区门户网”发布招标失败公告。

八、授予合同

37. 合同授予

除了中标人无法履行合同义务之外，招标人将把合同授予根据《投标人须知》第 33 条规定所确定的中标人。

38. 签订合同

中标人与采购人应当在《中标通知书》发出之日起 30 日内签订政府采购合同。

39. 其他

采购云平台有关操作方法可以参考采购云平台（网址：www.zfcg.sh.gov.cn）中的“操作须知”专栏。

第三章　政府采购政策功能

根据政府采购法，政府采购应当有助于实现国家的经济和社会发展政策目标，包括保护环境，扶持不发达地区和少数民族地区，促进中小企业发展等。

列入财政部、发展改革委发布的《节能产品政府采购品目清单》中强制采购类别的产品，按照规定实行强制采购；列入财政部、发展改革委、生态环境部发布的《节能产品政府采购品目清单》和《环境标志产品政府采购品目清单》中优先采购类别的产品，按规定实行优先采购。

中小企业按照《政府采购促进中小企业发展管理办法》享受中小企业扶持政策，对预留份额项目专门面向中小企业采购，对非预留份额采购项目按照规定享受价格扣除优惠政策。中小企业应提供《中小企业声明函》。享受扶持政策获得政府采购合同的，小微企业不得将合同分包给大中型企业，中型企业不得将合同分包给大型企业。

在政府采购活动中，监狱企业和残疾人福利性单位视同小微企业，监狱企业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，残疾人福利性单位应当提供《残疾人福利性单位声明函》。

如果有国家或者上海市规定政府采购应当强制采购或优先采购的其他产品和服务，按照其规定实行强制采购或优先采购。

第四章　招标需求

一、项目概述

见附件

二、项目内容及要求

见附件

三、商务要求：

类别	要求
投标有效期	自开标之日起 90 日
质量保证期	自最终验收合格之日起软件和硬件均不少于 36 个月的免费质量保修期
交付日期	合同签订后 180 天内
付款方式	合同签订后支付 30%、货物到齐开箱验收合格后支付 30%、完成机房迁建满足试运行条件后支付 28%、通过第三方测评完成项目终验后支付 12%。
转让与分包	本项目合同不得转让与分包

四、投标文件的编制要求

投标人应按照第二章《投标人须知》的相关要求及采购云平台要求编制网上投标文件，其中投标文件应包括下列内容（不限于下列）：

1. 商务响应文件由以下部分组成：

（1）《投标函》

（2）《开标一览表》（在采购云平台填写）

（3）《投标报价分类明细表》

（4）《资格审查要求表》

（5）《符合性要求表》

（6）《商务要求响应表》

（7）《法定代表人授权委托书》（含法定代表人身份证、被授权人身份证复印件）

（8）投标人营业执照（或事业单位、社会团体法人证书）

（9）财务状况及税收、社会保障资金缴纳情况声明函

（10）享受政府采购优惠政策的相关证明材料，包括：中小企业声明函、监狱企业证明文件、残疾人福利性单位声明函等（中标人为中小企业、残疾人福利性单位的，其声明函将随中标结果同时公告）

（11）投标人基本情况简介

2．技术响应文件由以下部分组成：

（1）项目经理情况表；

（2）主要管理、技术人员配备及同类项目工作经历、职业资格汇总表；

（3）软硬件产品技术要求比对明细表；

（4）针对本项目的需求理解；

（5）方案设计；

（6）实施方案；

（7）售后服务方案；

（8)开标日前半年内任意一个月投标人为项目经理和项目组主要人员依法缴纳社会保障资金的证明材料；

（9）按照本招标文件要求提供的其他技术性资料以及投标人需要说明的其他事项。

以上各类响应文件格式详见招标文件第六章《投标文件有关格式》（格式自拟除外）。

第五章　评标方法与程序

一、资格审查

招标人将依据法律法规和招标文件的《投标人须知》、《资格审查要求表》，对投标人进行资格审查。确定符合资格的投标人不少于 3 家的，将组织评标委员会进行评标。

二、投标无效情形

1、投标文件不符合《资格审查要求表》以及《符合性要求表》所列任何情形之一的，将被认定为无效投标。

2、单位负责人或法定代表人为同一人，或者存在直接控股、管理关系的不同供应商，参加同一包件或者未划分包件的同一项目投标的，相关投标均无效。

3、除上述以及政府采购法律法规、规章、《投标人须知》所规定的投标无效情形外，投标文件有其他不符合招标文件要求的均作为评标时的考虑因素，而不导致投标无效。

三、评标方法与程序

1、评标方法

根据《中华人民共和国政府采购法》及政府采购相关规定，结合项目特点，本项目采用“综合评分法”评标，总分为 100 分。

2、评标委员会

2.1 本项目具体评标事务由评标委员会负责，评标委员会由 7 人组成，其中采购人代表不多于成员总数的三分之一，其余为政府采购评审专家，采购代表不参加评标的，则评委会成员均由评审专家组成。招标人将按照相关规定，从上海市政府采购评审专家库中随机抽取评审专家。

2.2 评标委员会成员应坚持客观、公正、审慎的原则，依据投标文件对招标文件响应情况、投标文件编制情况等，按照《投标评分细则》逐项进行综合、科学、客观评分。

3、评标程序

本项目评标工作程序如下：

3.1 符合性审查。评标委员会应当对符合资格的投标人的投标文件进行符合性审查，以确定其是否满足招标文件的实质性要求。

3.2 澄清有关问题。对投标文件中含义不明确或者有明显文字和计算错误的内容，评标委员会应当以书面形式要求投标人作出必要的澄清、说明或者纠正。投标人的澄清、说明或者补正应当采用书面形式，由其授权的代表签字，不得超出投标文件的范围或者改变投标文件的实质性内容，也不得通过澄清而使进行澄清的投标人在评标中更加有利。

3.3 比较与评分。评标委员会按招标文件规定的《投标评分细则》，对符合性审查合格的投标文件进行评分。

3.4 推荐中标候选供应商名单。各评委按照评标办法对每个投标人进行独立评分，再计算平均分值，评标委员会按照每个投标人最终平均得分的高低依次排名，推荐得分最高者为第一中标候选人，依此类推。得分相同的，按投标报价由低到高顺序排列。得分且投标报价相同的并列。

投标文件满足招标文件全部实质性要求，且按照评审因素的量化指标评审得分最高的投标人为排名第一的中标候选人。如果评审得分仍相同，则由评标委员会按照少数服从多数原则投票表决。

3.5 提供的本项目核心产品为相同品牌产品且通过资格审查、符合性审查的不同投标人参加同一合同项下投标的，按一家投标人计算，评审后得分最高的提供同品牌核心产品的投标人获得中标人推荐资格；评审得分相同的，报价最低的投标人获得中标人推荐资格，其他同品牌投标人不作为中标候选人。

4、评分细则

本项目具体评分细则如下：

4.1 投标价格分按照以下方式进行计算：

（1）价格评分：报价分＝价格分值×（评标基准价/评审价）

（2）评标基准价：是经符合性检查合格（技术、商务基本符合要求，无重大缺、漏项）满足招标文件要求且投标价格最低的投标报价。

（3）评审价：投标报价无缺漏项的，投标报价即评审价；投标报价有缺漏项的，其投标报价也即评审价，缺漏项的费用视为已包括在其投标报价中。

（4）非预留份额专门面向中小企业采购的项目或包件，对小微企业报价给予**10%**的扣除，用扣除后的价格参与评审；非预留份额专门面向中小企业采购且接受联合体投标或者允许分包的项目或包件，对于联合协议或者分包意向协议中约定小微企业的合同份额占到合同总金额30%以上的投标人，给予其报价4%的扣除，用扣除后的价格参与评审。以联合体形式参加政府采购活动，联合体各方均为中小企业的，联合体视同中小企业，其中，联合体各方均为小微企业的，联合体视同小微企业。组成联合体或者接受分包的小微企业与联合体内其他企业、分包企业之间存在直接控股、管理关系的，不享受价格扣除优惠政策。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。中小企业投标应提供《中小企业声明函》。

（5）评标委员会认为投标人的报价明显低于其他通过符合性审查投标人的报价，有可能影响产品质量或者不能诚信履约的，应当要求其在评标现场合理的时间内提供书面说明，必要时提交相关证明材料；投标人不能证明其报价合理性的，评标委员会应当将其作为无效投标处理。

4.2 投标文件其他评分因素及分值设置等详见《投标评分细则》。

投标评分细则（100分）

序号	评审内容	评审因素	类别	评审标准	分值
1	报价得分	报价得分	客观分	报价得分=（评标基准价／投标报价）×30%×100。	30
2	需求理解	需求理解	主观	投标人结合项目背景、项目定位等，对相关业务、功能、性能、安全、服务等内容进行需求的分析和理解。	3

		重难点分析	分	投标人能否根据项目目标、项目现状等，对机房迁建及系统集成过程中的重点、难点的进行分析。	3
3	兼容性对接及测评承诺	兼容性对接及测评承诺	客观分	根据“**8、兼容性对接及测评承诺**”要求，是否提供物联感知数据接入平台软硬一体机无缝对接承诺函，提供承诺函得 4 分，未完整承诺或未承诺本项不得分。	4
				根据“**8、兼容性对接及测评承诺**”要求，是否提供态势分析与安全运营系统实现统一监管承诺函，提供承诺函得 4 分，未完整承诺或未承诺本项不得分。	4
				根据“**8、兼容性对接及测评承诺**”要求，是否提供配合用户方进行安全测评及等级保护测评工作承诺函，提供承诺函得 4 分，未完整承诺或未承诺本项不得分。	4
4	技术指标偏离度	技术指标偏离度	客观分	按照“**9、#号项指标汇总**”对#号重要参数逐个响应，#号重要参数每负偏离一项或未完整提供佐证材料的扣 2 分。	14
5	实施方案	进度管理	主观分	投标人根据项目要求是否提供进度计划，包括但不限于项目进度管理、过程管理节点计划、保障措施组织方案等是否满足招标要求。	4
		机房迁建	主观分	投标人能否根据机房迁建要求提供了整体风险评估、设备迁移实施方案及数据安全保障措施等，是否满足招标要求。	4
		集成方案	主观分	投标人能否根据项目特性提供了集成方案，包括机房部署规划、网络拓扑、综合布线、系统对接及实施保障措施，是否满足招标要求。	4
		质量管理	主观分	投标人是否提供了针对本项目的项目质量管理方案，包括但不限于项目质量保证体系、项目质量控制方法、项目质量保障措施，提供的方案是否满足项目各阶段的质量管理需求。	4
		项目经理	客观分	项目经理具有信息系统项目管理师资格证书的得 2 分。（上述人员提供有效的国家有关职能部门颁发的职业资格证书复印件，及投标人为其开标日前三个月内任意一个月缴纳社会保障资金的证明材料，未完整提供证明材料的本项不得分）。	2
6	售后服务	售后服务体系	主观分	投标人是否提供了售后服务体系，是否包含服务组织架构、服务流程与标准以及技术支持与资源等内容，是否能够满足采购需求。	4
		应急保障措施	主观分	投标人是否提供了应急保障方案，包括针对本项目的应急处理保障方案，在应急保障处置中，能否根据事件紧急重要情况，提供不同等级的服务，专业设备落实计划等是否满足采购需求。	4
		培训方案	主观分	投标人是否提供了针对项目各类人员制定培训方案，包括培训资料、培训方式、培训内容等，是否满足采购需求。	4
		驻场服务承诺	客观分	投标人是否提供 3 年质保期内不少于 3 人的驻场服务人员的承诺函（格式自拟），提供承诺函得 4 分，未提供的不得分。	4

7	业绩	业绩	客观分	提供合同签订日期为2021年1月1日至开标之日计算机及网络设备集成项目业绩。投标人需提供项目的合同扫描件，扫描件中需体现合同的签约主体、项目名称及内容、签订时间、合同金额、交付日期等合同要素的相关内容，否则将不予认可。每提供一个有效业绩得1分，最高得4分，未提供的不得分。	4

第六章　　投标文件有关格式

一、商务响应文件有关格式

1、投标函格式

致：上海市松江区政府采购中心

根据贵方_____（项目名称、招标编号）采购的招标公告及投标邀请，_____（姓名和职务）被正式授权代表投标人_____（投标人名称、地址），按照采购云平台规定向贵方提交投标文件1份。

据此函，投标人兹宣布同意如下：

1.按招标文件规定，我方的投标总价为_____（大写）元人民币。

2.我方已详细研究了全部招标文件，包括招标文件的澄清和修改文件（如果有的话）、参考资料及有关附件，我们已完全理解并接受招标文件的各项规定和要求，对招标文件的合理性、合法性不再有异议。

3.投标有效期为自开标之日起_____日。

4.如我方中标，投标文件将作为本项目合同的组成部分，直至合同履行完毕止均保持有效，我方将按招标文件及政府采购法律、法规的规定，承担完成合同的全部责任和义务。

5.我方同意向贵方提供贵方可能进一步要求的与本投标有关的一切证据或资料。

6.我方完全理解贵方不一定要接受最低报价的投标或其他任何投标。

7.我方已充分考虑到投标期间网上投标可能会发生的技术故障、操作失误和相应的风险，并对因网上投标的任何技术故障、操作失误造成投标内容缺漏、不一致或投标失败的，承担全部责任。

8. 我方同意开标内容以采购云平台开标时的《开标记录表》内容为准。我方授权代表将及时使用数字证书对《开标记录表》中与我方有关的内容进行签名确认，授权代表未进行确认的，视为我方对开标记录内容无异议。

9.为便于贵方公正、择优地确定中标人及其投标货物和相关服务，我方就本次投标有关事项郑重声明如下：

（1）我方向贵方提交的所有投标文件、资料都是准确的和真实的。

（2）以上事项如有虚假或隐瞒，我方愿意承担一切后果，并不再寻求任何旨在减轻或免除法律责任的辩解。

地址：
电话、传真：
邮政编码：
开户银行：
银行账号：
投标人授权代表签名：
投标人名称（公章）：
日期：　　年　　月　　日

2、开标一览表格式

开标一览表格式见采购云平台，并在该平台填写。

松江区“雪亮工程”综治分平台安全加固升级扩容包 1

交付日期	质量保证期	投标总价(总价、元)

填写说明：

（1）所有价格均系用人民币表示，单位为元，精确到分。

（2）交付日期是指合同生效后多少天完成送货上门、就位、安装、调试、培训直至验收合格。

（3）质量保证期是指自货物按合同规定验收合格之日起多少个月。

（4）投标人应按照《招标需求》和《投标人须知》的要求报价。

3、投标报价汇总表格式

项目名称：
项目编号：

序号	费用名称	报价（元）	备注
1	硬件购置费		详见明细（ ）
2	成品软件购置费		详见明细（ ）
3	安全产品购置费		详见明细（ ）
4	安全服务费		详见明细（ ）
5	其他服务费		详见明细（ ）
报价合计			

说明：（1）投标人应编制报价明细表并随本表一起提供。
（2）本表合计总价应与开标一览表报价相等。

投标人授权代表签字：
投标人（公章）：
日　期：　　年　　月

4、报价分类明细表格式

项目名称：

项目编号：

（一）设备费 单位：元（人民币）

序号	设备名称	规格型号	品牌/产地	数量	单位	单价	合价	备注
合计								

（二）材料费 单位：元（人民币）

序号	材料名称	规格型号	品牌/产地	数量	单位	单价	合价	备注
合计								

（三）伴随服务费（包括运输费、安装费、调试费、人员培训费等其他费用）

单位：元（人民币）

费用类别	价格	备注
运输费		
安装费		
调试费		
驻场费		
培训费		
其他		
合计		

投标总价＝（一）+（二）+（三）

投标人授权代表签字：

投标人（公章）：

日　期：　　年　　月

5、资格审查要求表

项目名称：

项目编号：

松江区“雪亮工程”综治分平台安全加固升级扩容资格审查要求包 1

序号	类型	审查要求	要求说明	项目级/包级
1	自定义	法定基本条件	1．符合《中华人民共和国政府采购法》第二十二条规定的条件：营业执照（或事业单位、社会团体法人证书）；提供财务状况及税收、社会保障资金缴纳情况声明函。 2.未被列入“信用中国”网站(www.creditchina.gov.cn)失信被执行人名单、重大税收违法案件当事人名单和中国政府采购网(www.ccgp.gov.cn)政府采购严重违法失信行为记录名单的供应商。	包 1
2	自定义	联合体投标	本项目不接受联合体投标。	包 1
3	自定义	大中小微企业	本项目面向大、中、小、微型等各类供应商采购。	包 1

投标人授权代表签字：

投标人（公章）：

日期：　　年　　月　　日

6、符合性要求表

项目名称：
项目编号：

项目内容	具备的条件说明（要求）	投标检查项(响应内容说明(是/否))	详细内容所对应电子投标文件名称与页次	备注
法定代表人授权	1．在投标文件由法定代表人授权代表签字（或盖章）的情况下，应按招标文件规定格式提供法定代表人授权委托书。 2．按招标文件要求提供法定代表人身份证、被授权人身份证。			
投标文件密封、签署等要求	符合招标文件规定： 1．投标文件按招标文件规定格式提供《投标函》、《开标一览表》、《资格审查要求表》以及《符合性要求表》。 2．投标文件按招标文件要求密封（适用于纸质投标项目），电子投标文件须经电子加密（投标文件上传成功后，系统即自动加密）。			
投标报价	1．不得进行选择性报价（投标报价应是唯一的，招标文件要求提供备选方案的除外）。 2．不得进行可变的或者附有条件的投标报价。 3．投标报价不得超出招标文件标明的采购预算金额/项目最高限价。 4．不得低于成本报价。 5．投标报价有缺漏项的，缺漏项部分的报价按照其他投标人相同项的最高报价计算，计算出的缺漏项部分报价不得超过投标报价的 10%。			
商务要求	1．投标有效期、交付日期、质量保证期、付款条件满足招标文件要求。 2．合同不得转让与分包。			
进口产品	本项目不接受进口产品。			
“★”要求	符合技术规范、技术标准和《招标需求》质量标准，或者符合招标文件中标“★”的技术、性能及其它要求的。			
公平竞争和诚实信用	不得存在腐败、欺诈或其他严重违背公平竞争和诚实信用原则、扰乱政府采购正常秩序的行为。			

投标人授权代表签字：
投标人（公章）：
日期：　　年　　月　　日

7、商务响应表格式

项目名称：
项目编号：

项目	招标文件要求	是否响应	投标人的承诺或说明
投标有效期			
质量保证期			
交付日期			
付款方式			
转让与分包			

投标人授权代表签字：
投标人（公章）：
日期：　　年　　月　　日

8、法定代表人授权委托书格式

致：上海市松江区政府采购中心

我_____（姓名）系注册于_____（地址）的_____（投标人名称，以下简称我方）的法定代表人，现代表我方授权委托我方在职职工_____（姓名，职务）以我方的名义参加贵中心_____项目的投标活动，由其代表我方全权办理针对上述项目的投标、开标、投标文件澄清、签约等一切具体事务，并签署全部有关的文件、协议及合同。

我方对被授权人的签名事项负全部责任。

在贵中心收到我方撤销授权的书面通知以前，本授权书一直有效。被授权人在授权书有效期内签署的所有文件不因授权的撤销而失效。

被授权人无转委托权，特此委托。

法定代表人身份证复印件 （有照片一面）	被授权人身份证复印件 （有照片一面）
投标人（公章）： 法定代表人（签字或盖章）： 电话： 传真： 日期：	受托人（签字）： 身份证号码： 电话： 传真： 日期：

9、中小企业声明函

本公司（联合体）郑重声明，根据《政府采购促进中小企业发展管理办法》（财库〔2020〕46 号）的规定，本公司（联合体）参加 （单位名称） 的 （项目名称） 采购活动，服务全部由符合政策要求的中小企业承接。相关企业（含联合体中的中小企业、签订分包意向协议的中小企业）的具体情况如下：

1. （物联感知数据接入平台软硬一体机-PC 服务器-综治平台汇聚扩容），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

2. （物联感知数据库-PC 服务器-综治平台汇聚扩容），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

3. （视频国标网关（扩容）-PC 服务器-综治平台汇聚扩容），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

4. （一机一档数据治理平台（扩容）-PC 服务器-综治平台汇聚扩容），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

5. （运维平台（升级）-PC 服务器-综治平台汇聚扩容），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

6. （核心交换机-网络设备-街镇边界与核心），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

7. （汇聚交换机-网络设备-街镇边界与核心），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

8. （万兆光模块-网络设备-街镇边界与核心），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

9. （终端威胁防御系统 （EDR）-机架式服务器-安全管理区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

10. （数据防泄漏系统-机架式服务器-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

11. （信息数字证书认证系统-机架式服务器-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

12. （下一代防火墙-工具软件-横向安全边界区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

13. （下一代防火墙-工具软件-街镇边界与核心），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

14. （下一代防火墙-工具软件-互联网出口边界），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

15. （下一代防火墙-工具软件-应用系统区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

16. （下一代防火墙-工具软件-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

17. （终端威胁防御系统 （EDR）-工具软件-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

18. （终端威胁防御系统 （EDR）-操作系统-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

19. （终端威胁防御系统 （EDR）-工具软件-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

20. （终端威胁防御系统 （EDR）-工具软件-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

21. （终端威胁防御系统 （EDR）-终端威胁防御系统 （EDR）-安全管理区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

22. （漏洞扫描-工具软件-安全管理），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

23. （数据防泄漏系统-工具软件-安全管理区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

24. （数据防泄漏系统-操作系统-安全管理区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

25. （信息数字证书认证系统-工具软件-安全管理区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

26. （信息数字证书认证系统-数据库-安全管理区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

27. （信息数字证书认证系统-中间间-安全管理区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

28. （信息数字证书认证系统-操作系统-安全管理区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

29. （下一代防火墙-防火墙-横向安全边界区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

30. （入侵防御系统-入侵防御产品（IPS）-横向安全边界区），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

31. （下一代防火墙-防火墙-街镇边界与核心），属于 工业 ；承接企业为 （企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于 （中型企业、小型企业、微型企业）；

32. （入侵防御系统-入侵防御产品（IPS）-街镇边界与核心），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

33. （统一安全接入网关系统（管理平台）-安全隔离与信息交换产品-街镇边界与核心），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为万元，属于（中型企业、小型企业、微型企业）；

34. （统一安全接入网关系统（核心侧）-安全隔离与信息交换产品-街镇边界与核心），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

35. （统一安全接入网关系统（街镇侧 1）-安全隔离与信息交换产品-街镇边界与核心），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为万元，属于（中型企业、小型企业、微型企业）；

36. （统一安全接入网关系统（街镇侧 2）-安全隔离与信息交换产品-街镇边界与核心），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为万元，属于（中型企业、小型企业、微型企业）；

37. （下一代防火墙-防火墙-互联网出口边界），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

38. （入侵防御系统-入侵防御产品（IPS）-互联网出口边界），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

39. （抗 DDOS 系统-抗拒绝服务系统产品-互联网出口边界），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

40. （抗 DDOS 系统（千兆板卡扩容）-抗拒绝服务系统产品-互联网出口边界），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

41. （下一代防火墙-防火墙-应用系统区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

42. （入侵防御系统-入侵防御产品（IPS）-应用系统区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

43. （Web 应用防护系统-WEB 应用防火墙产品-应用系统区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

44. （下一代防火墙-防火墙-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

45. （数据库审计-安全审计产品-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

46. （堡垒机-安全隔离与信息交换产品-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

47. （日志审计-安全审计产品-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

48. （漏洞扫描-网络脆弱性扫描产品-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

49. （态势分析与安全运营系统-安全管理平台产品-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

50. （态势分析与安全运营系统（日志源 License）-安全管理平台产品-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

51. （备份一体机-数据安全-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

52. （备份一体机（存储扩展）-数据安全-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

53. （网络审计系统-安全审计产品-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

54. （数据防泄漏系统（终端 DLP 代理许可）-访问控制-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

55. （信息数字证书认证系统（智能密码钥匙）-统一身份认证-安全管理区），属于 工业 ；承接企业为（企业名称），从业人员____人，营业收入为____万元，资产总额为____万元，属于（中型企业、小型企业、微型企业）；

以上企业，不属于大企业的分支机构，不存在控股股东为大企业的情形，也不存在与大企业的负责人为同一人的情形。

本企业对上述声明内容的真实性负责。如有虚假，将依法承担相应责任。

企业名称（盖章）：

日 期：

说明：（1）本声明函所称中小企业，是指在中华人民共和国境内依法设立，依据国务院批准的中小企业划分标准确定的中型企业、小型企业和微型企业，但与大企业的负责人为同一人，或者与大企业存在直接控股、管理关系的除外。符合中小企业划分标准的个体工商户，在政府采购活动中视同中小企业。事业单位、团体组织等非企业性质的政府采购供应商，不属于中小企业划型标准确定的中小企业，不得按《关于印发中小企业划型标准规定的通知》规定声明为中小微企业，也不适用《政府采购促进中小企业发展管理办法》。

（2）本声明函所称服务由中小企业承接，是指提供服务的人员为中小企业依照《中华人民共和国劳动合同法》订立劳动合同的从业人员，否则不享受中小企业扶持政策。

（3）从业人员、营业收入、资产总额填报上一年度数据，无上一年度数据的新成立企业可不填报。

（4）采购标的对应的中小企业划分标准所属行业，以招标文件第二章《投标人须知》规定为准。

（5）投标人未按照上述格式正确填写《中小企业声明函》的，视为未提供《中小企业声明函》，不享受中小企业扶持政策。

注：行业划型标准：（二）工业。从业人员 1000 人以下或营业收入 40000 万元以下的为中小微型企业。其中，从业人员 300 人及以上，且营业收入 2000 万元及以上的为中型企业；从业人员 20 人及以上，且营业收入 300 万元及以上的为小型企业；从业人员 20 人以下或营业收入 300 万元以下的为微型企业。

10、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，本单位安置残疾人___人，占本单位在职职工人数比例___%，符合残疾人福利性单位条件，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：

说明：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》享受政府采购支持政策的残疾人福利性单位应当同时满足以下条件：

（1）安置的残疾人占本单位在职职工人数的比例不低于 25%（含 25%），并且安置的残疾人人数不少于 10 人（含 10 人）；

（2）依法与安置的每位残疾人签订了一年以上（含一年）的劳动合同或服务协议；

（3）为安置的每位残疾人按月足额缴纳了基本养老保险、基本医疗保险、失业保险、工伤保险和生育保险等社会保险费；

（4）通过银行等金融机构向安置的每位残疾人，按月支付了不低于单位所在区县适用的经省级人民政府批准的月最低工资标准的工资；

（5）提供本单位制造的货物、承担的工程或者服务（以下简称产品），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）。

中标人为残疾人福利性单位的，本声明函将随中标结果同时公告。

如投标人不符合残疾人福利性单位条件，无需填写本声明。

11、财务状况及税收、社会保障资金缴纳情况声明函

我方（供应商名称）符合《中华人民共和国政府采购法》第二十二条第一款第（二）项、第（四）项规定条件，具体包括：

1.具有健全的财务会计制度；

2.有依法缴纳税收和社会保障资金的良好记录。

特此声明。

我方对上述声明的真实性负责。如有虚假，将依法承担相应责任。

供应商名称（公章）

日期：

二、技术响应文件有关表格格式

1、项目经理情况表

项目名称：
项目编号：

姓　名		出生年月		文化程度		毕业时间
毕业院校及专业			从事同类项目工作年限			联系方式
职业资格			技术职称			聘任时间
主要工作经历： 主要管理服务项目： 主要工作特点： 主要工作业绩： 胜任本项目经理的理由						

投标人授权代表签字：
投标人（公章）：
日期：　　年　　月　　日

2、主要管理、技术人员配备及同类项目工作经历、职业资格汇总表

项目名称：

项目编号：

项目组成员姓名	年龄	在项目组中的岗位	学历和毕业时间	职称及职业资格	进入本单位时间	同类项目工作经历	联系方式

投标人授权代表签字：

投标人（公章）：

日　期：　　年　　月

3、软硬件产品技术要求比对明细表

项目名称：

项目编号：

序号	名称	采购参数	响应参数	偏离情况说明	证明材料所在页码
技术参数					
1					
2					
3					
4					
…					

投标人授权代表签字：

投标人（公章）：

日　期：　　年　　月

4、 物联感知数据接入平台软硬一体机对接承诺声明函

致：_____（招标人）

我公司（供应商名称）是按照中华人民共和国法律成立，主要营业地点设在（承诺方地址）。针对（投标人名称）参加（项目名称）、（项目编号）的投标活动，由我公司提供的以下设备：

1．物联感知数据接入平台软硬一体机

2．. . . . . .

以上所有设备均能支持前端智能门禁、视频抓拍图片等数据接入，兼容原有人脸分析算法平台、数据存储平台和运维管理平台的无缝对接，实现统一管理应用。完全符合甲方相关要求，保证其系统的兼容性和功能的完整性，否则将承担由此引起的一切后果和相应的法律责任。

特此承诺！

承诺人名称（盖章）：

日期：　　年　　月　　日

5、态势分析与安全运营系统兼容性承诺声明函

致：_____（招标人）

我公司（供应商名称）是按照中华人民共和国法律成立，主要营业地点设在（承诺方地址）。针对（投标人名称）参加（项目名称）、（项目编号）的投标活动，由我公司提供的以下设备：

1．态势分析与安全运营系统

2．. . . . . .

以上所有设备均能支持对各类安全设备、网络设备及终端的安全信息能力纳管，实现跨域设备动态感知、集中监控、基于统一策略的自动化联动响应与处置，实现统一监管。完全符合甲方相关要求，保证其系统的兼容性和功能的完整性，否则将承担由此引起的一切后果和相应的法律责任。

特此承诺！

承诺人名称（盖章）：

日期：　　年　　月　　日

6、测评承诺声明函

致：_____（招标人）

我司_____（公司名称）郑重承诺：

免费提供技术人员及资料，全程配合贵方完成安全测评及等保三级测评。并及时对测评中发现的问题立即整改。确保项目完成测评工作，否则将承担由此引起的一切后果和相应的法律责任。

特此承诺！

承诺人名称（盖章）：

日期：　　年　　月　　日

7、#号项指标技术要求比对明细表

序号	系统名称	产品名称	投标产品	投标型号	#重要参数指标	是否偏离	响应说明	应答证明材料所在章节	备注
1	安全产品购置	下一代防火墙			#支持链路连通性检查功能，支持通过DNS 解析、ARP 探测、PING 和 BFD 等方式对链路连通性进行探测；		提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告		
2					#支持策略匹配分析、策略冗余分析、风险端口分析，提供安全策略优化建议；		提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告		
3					#支持对 HTTP/SMTP/POP3/FTP/等协议进行病毒防御；		提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告		
4					#当主机故障时，双机切换时不丢包，并可实现双机部署下升级不断网；		提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告		
5	综治分平台安全加固	态势分析与安全运营系统			#支持攻击事件时间溯源轴展示匹配上的威胁建模模型信息，攻击手段显示模型名称，事件类型显示威胁建模设置的事件标签，覆盖的攻击阶段显示威胁建模设置的攻击链，安全处置建议显示威胁建模设置的处置建议		提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告		
6					#支持自定义弱密码字典的增删改查，可用于检测自定义的弱密码，弱密码字典支持对事件和密码进行筛选和检索		提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告		

7					#支持自定义攻击事件分析模型，至少包括：事件规则匹配模型、事件统计分析模型、事件关联分析模型；内置38种及以上安全事件分析模型，如冰蝎webshell通信、利用Sqlmap上传webshell、Acunetix安全工具扫描、APPSCAN工具扫描等		提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告		

第七章　合同书格式和合同条款

包 1 合同模板：

[合同中心-项目名称]合同

合同编号：［合同中心-合同编码］

合同双方：

甲方（买方）：**［合同中心-采购单位名称］**

地址：**［合同中心-采购单位所在地］**

邮政编码：**［合同中心-采购人单位邮编］**

电话：**［合同中心-采购单位联系人电话］**

传真：**［合同中心-采购人单位传真］**

联系人：**［合同中心-采购单位联系人］**

乙方（卖方）：**［合同中心-供应商名称］**

地址：**［合同中心-供应商所在地］**

邮政编码：**［合同中心-供应商单位邮编］**

电话：**［合同中心-供应商联系人电话］**

传真：**［合同中心-供应商单位传真］**

联系人：**［合同中心-供应商联系人］**

［合同中心-供应商银行名称］

［合同中心-供应商银行账号］

根据《中华人民共和国政府采购法》、《中华人民共和国民法典》之规定，本合同当事人在平等、自愿的基础上，经协商一致，同意按下述条款和条件签署本合同：

1. 乙方根据本合同的规定向甲方提供以下信息系统设备、应用软件和服务项目：

1.1 乙方所提供的 **［合同中心-项目名称］**

乙方所提供的信息系统设备、应用软件其来源应符合国家的有关规定，信息系统设备、应用软件的模块配置、功能、版本、数量、价格和交付日期等详见合同附件。

2. 合同价格、交货地点、交货时间和交货状态

2.1 合同价格

本合同价格为人民币**[合同中心-合同总价]**元整；大写**[合同中心-合同总价大写]**。

乙方为履行本合同而发生的所有费用均应包含在合同价中，甲方不再另行支付其它任何费用。

2.2 交付地点

本系统设备、应用软件和服务项目交付地点：采购人指定地点。

2.3 交付日期

本信息系统应用软件和服务项目的交付日期：详见投标文件。

3. 质量标准和要求

3.1 乙方所交付信息系统设备、应用软件的质量标准按照国家标准、行业标准，上述标准不一致的，以严格的标准为准。没有国家标准、行业标准和企业标准的，按照通常标准或者符合合同目的的特定标准确定。

3.2 乙方所交付的信息系统应用软件还应符合国家和上海市有关软件开发规定。

4. 权利瑕疵担保

4.1 乙方保证对其交付的信息系统应用软件享有合法的权利。

4.2 乙方保证在其交付的信息系统应用软件上不存在任何未曾向甲方透露的漏洞，后门等安全隐患。

4.3 乙方保证其所交付的信息系统应用软件没有侵犯任何第三人的知识产权和商业秘密等权利。

4.4 如甲方使用该信息系统应用软件构成上述侵权的，则由乙方承担全部责任。

5.交付、领受与验收

5.1 甲方应依据信息系统项目工程的条件和性质，根据乙方的要求向乙方提供信息系统的施工、安装和调试环境。如甲方未能在该时间内提供该施工和安装环境，乙方可相应顺延交付日期。如对乙方造成经济损失，甲方还应依本合同规定承担违约责任。

5.2 乙方应在进行每项交付前，以书面方式通知甲方。甲方应当在接到通知后安排接受交付。乙方在交付前应当根据附件中的检测标准对所交付的项目进行功能和运行检测，以确认交付项目符合本合同的规定。

5.3 乙方应按照合同及其附件所约定的内容进行交付，如果本合同约定甲方可以使用或拥有某软件源代码的，乙方应同时交付软件的源代码。所交付的文档与文件应当是可供人阅读的书面和电子文档。

5.4 甲方在领受交付项目后，应当对所交付项目进行检验，向乙方出具书面文件，以确认其符合本合同所约定信息系统设备及应用软件的模块、需求和功能、使用手册、维护手册。如有缺陷，应向乙方出具书面报告，陈述需要改进的缺陷。乙方应立即改进此项缺陷，并再次进行检测和评估，甲方应当再次检验并向乙方出具书面领受文件或递交缺陷报告。甲、乙双方将重复此项程序直至甲方领受或甲方依法或依约终止本合同为止。

5.5 自系统功能检测通过之日起，甲方拥有系统试运行权利。

5.6 如果由于乙方原因，导致系统在试运行期间出现故障或问题，乙方应及时排除该故障或问题。以上行为产生的费用均由乙方承担。

5.7 如果由于甲方原因，导致系统在试运行期间出现故障或问题，乙方应及时配合排除该方面的故障或问题。以上行为产生的相关费用均由甲方承担。

5.8 系统试运行完成后，甲方应及时进行系统验收。乙方应当以书面形式向甲方递交验收通知书，甲方在收到验收通知书后，确定具体日期，由双方按照本合同的规定完成系统验收。甲方有权委托第三方检测机构进行验收，对此乙方应当配合。

5.9 如果属于乙方原因致使系统未能通过验收，乙方应当排除故障，并自行承担相关费用，同时延长试运行期，直至系统完全符合验收标准。

5.10 如果属于甲方原因致使系统未能通过验收，甲方应在合理时间内排除故障，再次进行验收。如果属于故障之外的原因，除本合同规定的不可抗力外，甲方不愿或未能在规定的时间内完成验收，则由乙方单方面进行验收，并将验收报告提交甲方，即视为验收通过。

5.11 甲方根据信息系统应用软件模块和功能，对信息系统设备及应用软件验收合格后，甲方收取发票并在《验收单》上签署验收意见及加盖单位印章。

6.知识产权和保密

6.1 甲方委托开发软件的知识产权归甲方所有。乙方向甲方交付使用的信息系统应用软件已享有知识产权的，甲方在许可的范围内合理使用。

6.2 在本合同项下的任何权利和义务不因合同乙方发生收购、兼并、重组、分立而发生变化。如果发生上述情形，则本合同项下的权利随之转移至收购、兼并、重组后的企业继续履行合同，分立后成立的企业共同对甲方承担连带责任。

6.3 如果甲方或乙方提供的内容属于保密的，应签订保密协议，甲乙双方均有保密义务。

7. 付款

7.1 本合同以人民币付款（单位：元）。

7.2 本合同款项按照以下方式支付。

合同签订后支付 30%、货物到齐开箱验收合格后支付 30%、完成机房迁建满足试运行条件后支付 28%、通过第三方测评完成项目终验后支付 12%。

8. 辅助服务

8.1 乙方应提交所提供信息系统应用软件包括相应的每一模块技术文件，例如：操作手册、使用说明、维护手册和服务指南。这些文件应包装好随同项目交付一起交付给甲方发运。

8.2 乙方还应提供下列服务：

（1）现场移动、安装、调试、启动监督及技术支持；

（2）在质量保证期内对交付的信息系统设备、应用软件实施运行监督、维护、维修；

（3）乙方应根据项目实施的计划、进度和需要与客户的合理要求，及时安排对甲方的相关人员进行培训。培训目标为使受训者能够独立、熟练地完成操作，实现依据本合同所规定的信息化系统应用软件的目标和功能。

8.3 辅助服务的费用应包含在合同价中，甲方不再另行支付。

9. 系统保证和维护

9.1 在乙方所交付的信息系统设备、应用软件中，不得含有未经甲方许可的可以自动终止或妨碍系统运作的软件和硬件，否则，乙方应承担赔偿责任；

9.2 乙方所提供的软件，包括受甲方委托所开发的软件，如果需要经国家有关部门登记、备案、审批或许可的，乙方应当保证所提供的软件已经完成上述手续。

9.3 乙方保证，依据本合同向甲方提供的信息系统设备、应用软件及其附属产品不存在品质或工艺上的瑕疵，能够按照本合同所规定的技术规范、要求和功能进行正常运行。乙方保证其所提供的软件系统在当前情况下是最适合本项目的版本。

9.4 乙方自各项目交付验收通过之日起 详见投标文件质保期 内向甲方提供免费的保修和维护服务并对由于设计、开发的缺陷而产生的故障负责。在此期间如发生系统运作故障，或出现问题，乙方将按照售后服务的承诺（见合同附件）提供技术支持和维护服务。

9.5 在质量保证期内，如果信息系统应用软件的模块或功能与合同不符，或证实信息系统设备、应用软件是有缺陷的，包括潜在的缺陷或使用不符合要求的设计、开发等，甲方可以根据本合同第 10 条规定以书面形式向乙方提出补救措施或索赔。

9.6 乙方在约定的时间内未能弥补缺陷，甲方可采取必要的补救措施，但其风险和费用将由乙方承担，甲方根据合同规定对乙方行使的其他权利不受影响。

9.7 在维护期内如由于乙方的责任而需要对本信息系统应用软件中的模块予以更换或升级，则该部件的保修期应相应延长。

10. 补救措施和索赔

10.1 甲方有权根据质量检测部门出具的检验证书向乙方提出索赔。

10.2 在质量保证期内，如果乙方对缺陷产品负有责任而甲方提出索赔，乙方应按照甲方同意的下列一种或多种方式解决索赔事宜：

（1）乙方同意退货并将货款退还给甲方，由此发生的一切费用和损失由乙方承担。

（2）根据信息系统应用软件的功能模块状况以及甲方所遭受的损失，经过买卖双方商定降低信息系统应用软件的价格。

（3）乙方应在接到甲方通知后七天内负责采用符合合同规定的规格、质量和性能要求的新零件、部件和设备来更换有缺陷的部分或修补缺陷部分，其费用由乙方负担。同时，乙方应在约定的质量保证期基础上相应延长修补和/或更换件的质量保证期。

10.3 如果在甲方发出索赔通知后十天内乙方未作答复，上述索赔应视为已被乙方接受。如果乙方未能在甲方发出索赔通知后十天内或甲方同意延长的期限内，按照上述规定的任何一种方法采取补救措施，甲方有权从应付货款中扣除索赔金额，如不足以弥补甲方损失的，甲方有权进一步要求乙方赔偿。

11. 履约延误

11.1 乙方应按照合同规定的时间、地点交货和提供服务。

11.2 如乙方无正当理由而拖延交货，甲方有权解除合同并追究乙方的违约责任。

11.3 在履行合同过程中，如果乙方可能遇到妨碍按时交货和提供服务的情况时，应及时以书面形式将拖延的事实、可能拖延的期限和理由通知甲方。甲方在收到乙方通知后，应尽快对情况进行评价，并确定是否同意延长交货时间或延期提供服务。

12. 误期赔偿

12.1 除合同第 13 条规定外，如果乙方没有按照合同规定的时间交货和提供服务，甲方应从货款中扣除误期赔偿费而不影响合同项下的其他补救方法，赔偿费按每（周、天）赔偿迟交货物的交货价或延期服务的服务费用的百分之零点五（0.5%）计收，直至交货或提供服务为止。但误期赔偿费的最高限额不超过合同价的百分之五（5%）。（一周按七天计算，不足七天按一周计算。）一旦达到误期赔偿的最高限额，甲方可考虑终止合同。

13. 不可抗力

13.1 如果合同各方因不可抗力而导致合同实施延误或不能履行合同义务的话，不应该承担误期赔偿或不能履行合同义务的责任。

13.2 本条所述的“不可抗力”系指那些双方不可预见、不可避免、不可克服的事件，但不包括双方的违约或疏忽。这些事件包括但不限于：战争、严重火灾、洪水、台风、地震、国家政策的重大变化，以及双方商定的其他事件。

13.3 在不可抗力事件发生后，当事方应尽快以书面形式将不可抗力的情况和原因通知对方。合同各方应尽可能继续履行合同义务，并积极寻求采取合理的措施履行不受不可抗力影响的其他事项。合同各方应通过友好协商在合理的时间内达成进一步履行合同的协议。

14. 履约保证金

不收取。

15. 争端的解决

15.1 甲乙双方如在履行合同中发生纠纷，首先应友好协商，协商不成，甲乙双方均应向合同签订地起诉。

16. 违约终止合同

16.1 在甲方对乙方违约而采取的任何补救措施不受影响的情况下，甲方可在下列情况下向乙方发出书面通知书，提出终止部分或全部合同。

（1）如果乙方未能在合同规定的期限或甲方同意延长的期限内提供部分或全部信息系统应用软件。

（2）如果乙方未能履行合同规定的其它义务。

16.2 如果甲方根据上述 16.1 款的规定，终止了全部或部分合同，甲方可以依其认为适当的条件和方法购买与未交货的信息系统应用软件，乙方应对购买类似的信息系统应用软件所超出的那部分费用负责。但是，乙方应继续执行合同中未终止的部分。

16.3 如果乙方在履行合同过程中有不正当竞争行为，甲方有权解除合同，并按《中华人民共和国反不正当竞争法》之规定由有关部门追究其法律责任。

17. 破产终止合同

17.1 如果乙方丧失履约能力或被宣告破产，甲方可在任何时候以书面形式通知乙方终止合同而不给乙方补偿。该终止合同将不损害或影响甲方已经采取或将要采取任何行动或补救措施的权利。

18. 合同转让和分包

18.1 本项目合同不得转让与分包。

19. 合同生效

19.1 本合同在合同各方签字盖章后生效。

19.2 本合同一式贰份，甲乙双方各执一份。

20. 合同附件

20.1 本合同附件包括：招标文件、投标文件、补充协议（若有）

20.2 本合同附件与合同具有同等效力。

20.3 合同文件应能相互解释，互为说明。若合同文件之间有矛盾，则以最新的文件为准。

21. 合同修改

21.1 除了双方签署书面修改协议，并成为本合同不可分割的一部分之外，本合同条件不得有任何变化或修改。

签约各方：

甲方（盖章）:**[合同中心-采购单位名称]**	乙方（盖章）：**[合同中心-供应商名称]**
法定代表人或授权委托人（签章）：	法定代表人或授权委托人（签章）：
日期：**[合同中心-签订时间]**	日期：**[合同中心-签订时间]**

合同签订地点:网上签约

[合同中心-合同有效期]

附件：项目采购需求

1、项目概述

项目名称	松江区“雪亮工程”综治分平台安全加固升级扩容
采购内容	按照安全测评技术导向基于等保 2.0 三级合规要求，开展安全技术措施加固，结合综治实际工作的需要对网络及服务器等设备进行扩容，满足全区公共安全视频监控建设集约化、联网规范化、应用智能化等要求。
采购预算	本项目采购预算为 11858902.00 元人民币，超过采购预算的报价不予接受。

2、建设背景

近年来，在全国市域社会治理现代化试点工作指引要求下，各地政法部门按照政法委、综治办等上级领导部门要求，大力加强城乡公共安全视频监控系统、市域共享交换平台和联网共享体系建设，全面实现“纵向贯通、横向互联、共享共用、安全可靠”和“全域覆盖、全网共享、全时可用、全程可控”目标。

加大有关标准贯彻执行力度，全面推进公共安全视频监控点位建设规划上图，前端摄像机和以建平台的高清改造和智能升级。建设市域社会治理智能化综合平台，以地理信息系统（GIS）地图和统一标准地址库为基础，加快“人、地、物、事、组织”等社会治理基础要素数字化、标准化转型。

松江区“雪亮工程”综治分平台作为综治工作的信息化中心，是全区海量社会面资源汇聚、交互、提升实战应用价值的重要支撑中心，也是确保社会面安防设施设备建成后完好运行的保障中心。当前，全区社会面联网接入随着社会面智能安防建设的全面推进，使得前端设备联网总量急剧增加。

综治公共视频专网分布散、覆盖广、应用专，操作人员经常性不固定、前端设备体量庞大、社区监控室人员复杂等导致的信息安全问题日益突出，计划在接入准入、系统安全加固和管理制度上不断加强，以确保图像、信息和数据不外泄、不丢失，从根本上杜绝信息安全和网络攻击等事故的发生，保障平台稳如磐石。

根据《全国市域社会治理现代化试点工作指引》要求下，对“雪亮工程”区综治分平台中不能满足要求的网络及服务器等设备进行扩容规划，满足全区公共安全视频监控建设集约化、联网规范化、应用智能化等要求。

在严格落实关键信息基础设施安全保护制度和网络安全等级保护制度前提下，融合社会治理相关部门数据，做到全域感知、智辅决策，为各级部门开展社会治理工作赋能。

3、建设目标

按照信息系统安全等级保护三级标准完善松江区“雪亮工程”社会面（社区）公共安全视频监控平台的网络和数据安全防范能力，实时掌控数据安全风险，从根本上降低了关键基础设施、重要网络和数据安全，避免发生重大及以上网络安全事件。结合综治实际工作的需要对“雪亮工程”区综治分平台中无法满足要求的网络及服务器等设备进行扩容规划，满足全区公共安全视频监控建设集约化、联网规范化、应用智能化等要求。为开展信息交换共享提供高效、安全的网络接入和数据交换服务提供网络安全防护和数据安全防护，提升社会治安综合治理的科技化水平。

4、建设内容及现状

4.1 建设内容

本次招标为松江区“雪亮工程”综治分平台安全加固升级扩容项目包括相关材料供货、安全服务、机房迁建、安装、设备测试、系统集成、试运行、采购方相关人员的培训、质量保证期内免费保养维修等内容。本项目主要建设内容如下：

松江区“雪亮工程”综治分平台安全加固设备采购

松江区“雪亮工程”综治分平台物联数据汇聚升级扩容设备采购

松江区“雪亮工程”综治分平台安全加固升级扩容项目等级保护安全服务

松江区“雪亮工程”综治分平台新机房迁建及系统集成

4.2 综治分平台现状及规划

4.2.1 总体架构

松江区公共安全视频监控联网建设应用总体架构为“1+2+X”，全区一个共享平台，2 个分平台（GA

联网平台和 ZZ 应用平台），X 为各横向单位的视频监控子平台。采用树形网络结构用光缆点对点将 18 个纵向下级单位的平台进行级联，同时向 QGA 平台及 SZZ 平台提供接入接口，满足上级业务部门的联网要求。

综治分平台是实现系统内资源汇聚、联网，汇聚及资源应用，实现基于本级平台的资源汇聚和联网，主要和 QGA 分平台、松江区共享平台（QCY 平台）直连互通，并通过松江区共享平台与横向各单位数据资源平台联网实现数据共享等。

4.2.2 区综治分平台架构

区综治分平台主要分为中心管理功能、综治应用功能、联网功能、智能运维功能、流媒体转发功能、显示功能等。其系统架构如下图所示：

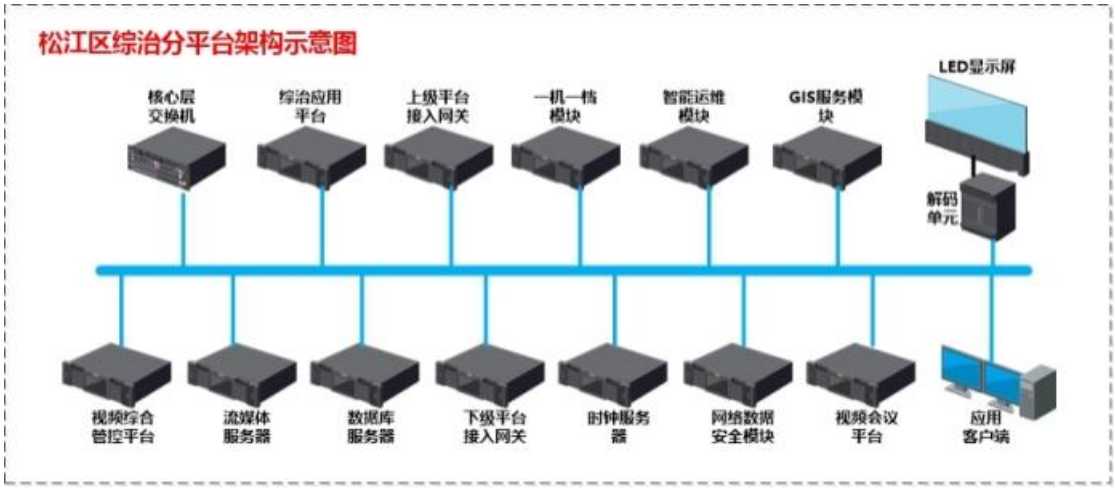

图 1 区综治平台联网系统架构图

4.2.3 网络拓扑

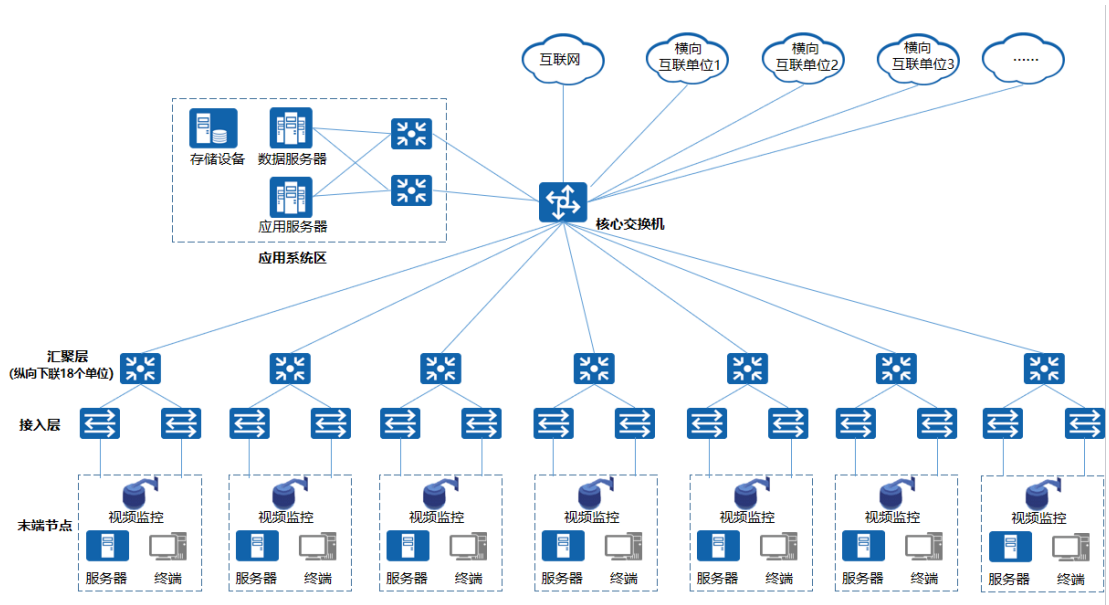

图 2 现有网络拓扑

4.2.4 现有设备

设备类型	单位	数量	品牌型号
应用服务器	台	168	主要设备为：大华 DH-DSS-C8101S2；大华 DH-NMS-B9100S3F；大华 DH-DSS-C8902S3A-1U；大华 DH-DSS-C9505A；大华 DH-DSS-C9400A；大华 DH-CSS7324S-VR
通用服	台	26	主要设备为：华为 RH2288V3

务器			
安全设备	台	6	主要设备为：华为 USG6620；华为 NIP6680
网络设备	台	27	主要设备为：华为 CE12808；华为 CE6855-48S6Q-HI；华为 CE5855-24T4S2Q-EI；华为 RH2288V3
视频会议设备	台	4	主要设备为：华平 AVCON MCU-AM2024W；华平 AVCON AMP-8；AVCON MAS16；华平 AVCON MRS 2000-0810

4.2.5 “雪亮工程”区综治分平台网络安全加固结构设计

“雪亮工程”区综治分平台网络安全加固结构设计拓扑图及安全域划分说明如下：

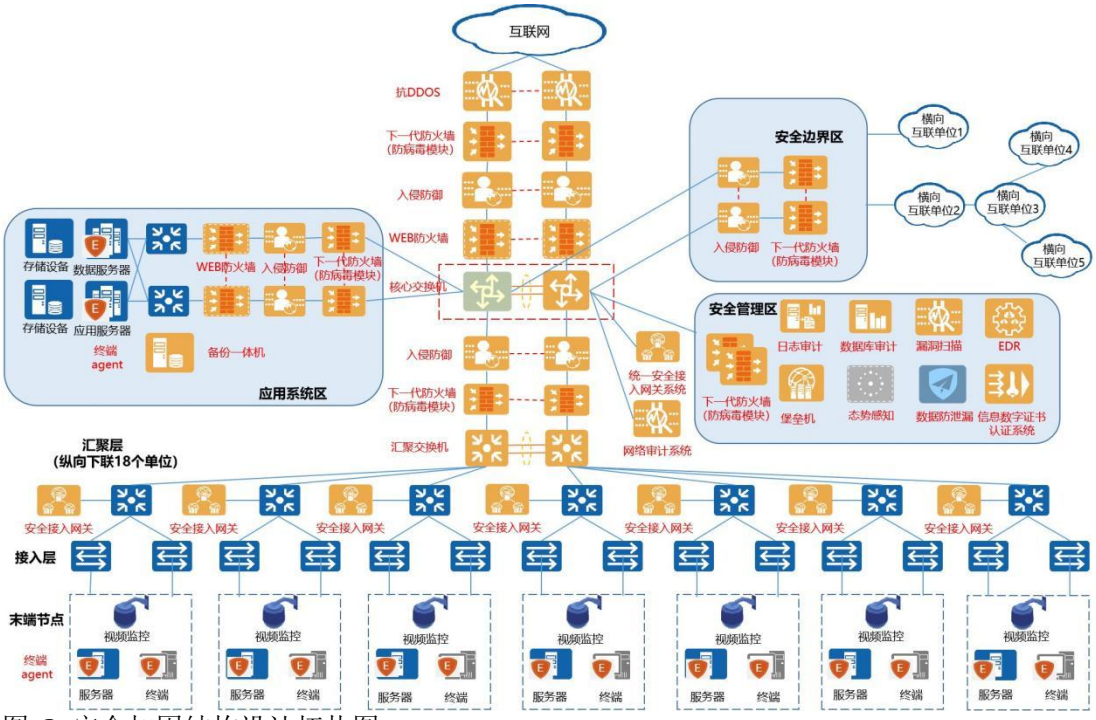

图 3 安全加固结构设计拓扑图

1）互联网出口区

双机部署抗 DDOS 系统、防火墙（含防病毒模块）、入侵防御系统、web 应用防护系统，功能开启后带宽需达到千兆（网络层万兆），对网络边界进行访问控制，对所有流经防火墙的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为；同时可以有效地缓解网站及 Web 应用系统面临如 0WASP TOP 10 中定义的常见威胁，并且可以快速地应对恶意攻击者对 Web 业务带来的冲击，实现 Web 业务应用安全与可靠交付。

2）应用系统区

双机部署防火墙（含防病毒模块）、入侵防御系统、web 应用防护系统，功能开启后带宽需达到千兆（网络层万兆）。对应用系统区边界进行访问控制和入侵防御，同时可以有效地缓解网站及 Web 应用系统面临如 0WASP TOP 10 中定义的常见威胁，并且可以快速地应对恶意攻击者对 Web 业务带来的冲击，实现 Web 业务应用安全与可靠交付。

3）核心交换区

在核心交换区新增 2 台核心交换机，满足等保 2.0 三级规划中对于关键节点设备的冗余要求。

在核心交换机部署统一安全接入网关系统，一方面满足约 2000 台终端 PC 和 800 台服务器接入需求；另一方面满足现网近 5W 摄像头以及近 3W 物联网终端的准入控制。

统一接入网关管理平台，通过主动探测方式形成 IPC 以及物联网设备的指纹库，包含设备 IP、MAC、设备类型等信息。同时对物联网设备进行漏洞防护，此外还能进行物联网设备的违规外联检测，检测是否存在无线 WIFI。

在核心区域旁路部署统一接入网关，通过主动探测、被动监听或者手动设置的方式形成设备指纹

库，包含设备 IP、MAC、设备类型等信息。非授权设备 IP、MAC 地址、设备类型在链路层被阻断，授权设备的 IP、MAC 地址、设备类型允许接入。
4）纵向下连 18 个单位
在 18 个下级单位的汇聚交换机部署 2 台防火墙（含防病毒模块），2 台入侵防御设备，对下属单位与核心区的网络边界进行访问控制，对所有流经防火墙的数据包按照严格的安全规则进行过滤，将所有不安全的或不符合安全规则的数据包屏蔽，杜绝越权访问，防止各类非法攻击行为。
在下级单位的服务器和 PC 中部署终端威胁防御系统软件，管理平台统一部署到本级数据中心机房，进行统一管理，agent 下沉到下级单位的 PC、服务器的主机上，防护网络层的病毒攻击。
在 18 个下级单位的汇聚交换机各旁路部署 1 台统一接入网关，通过主动探测、被动监听或者手动设置的方式形成设备指纹库，包含设备 IP、MAC、设备类型等信息。非授权设备 IP、MAC 地址、设备类型在链路层被阻断，授权设备的 IP、MAC 地址、设备类型允许接入。
5）安全边界区
考虑到 GA 神经元感知网的重要程度，以及和其他专网的边界，部署 2 台防火墙（含防病毒模块），部署 2 台入侵防御设备做访问控制与安全隔离。
6）安全管理区
部署 2 台防火墙（含防病毒模块），做访问控制与安全隔离。
部署态势分析与安全运营系统，该系统是智慧网络安全大脑的落地载体，也是整个安全保障体系实际落地方案。以安全大数据为基础，旨在从网络安全全局视角提升对安全威胁的发现识别、分析理解、响应处置能力，最终是为了决策和行动，目标是全面提升网络安全防护和响应能力。同时能够对接统一安全接入网关系统，对 IoT 进行网络安全监测、分析、展示与告警；并对 IoT 接入设备管理，新设备入网审批；下发指令联动准入控制设备踢出不可信设备。
为了满足等保的管理简化和合规性要求，部署日志审计系统，满足等保安全区域边界、安全计算环境、安全管理中心中所有对“安全审计”和“审计管理“的技术要求，同时满足《网络安全法》中“留存相关的网络日志不少于六个月”的法律要求。
在应用服务器前端部署数据库审计系统，满足等保技术要求中“安全审计”的要求，同时三级系统中数据库审计系统在等保测评时是重要的检查指标。该系统通过监控数据库的多重状态和通信内容，不仅能准确评估数据库所面临的风险，而且可以通过日志记录提供事后追查机制。主要功能包括：单双向审计、数据库自动发现、日志检索、风险告警、灵活策略配置、实时报表等。部署堡垒机设备，提供安全的信息传输路径，采用双因素认证，对网络中的安全设备或安全组件进行管理，满足等保技术要求中“安全审计”、“身份鉴别”、“集中管控”要求。同时堡垒机的部署能够简化安全运维工作，方便对运维操作的审计，降低因违规操作发生安全事件的风险。
部署漏洞扫描设备，定期对设备进行安全基线核查，并对网络中的资产进行漏洞扫描，找出不安全配置项进行整改加固，保障设备安全策略的有效性。
同时部署终端威胁防御系统，并在各个服务器和 PC 终端上安装 agent 围绕终端资产安全生命周期，通过预防、防御、检测、响应赋予终端更为细致的隔离策略、更为精准的查杀能力、更为持续的检测能力、更为快速的处置能力。
预防能力：提供对终端资产盘点、安全基线核查、智能微隔离、东西向流量可视等预防能力。
防御能力：提供对勒索软件、爆破入侵、后门上传、活跃僵尸程序等的实时防御能力。
检测能力：提供对恶意文件、入侵攻击、web 后门、热点事件的检测能力。
响应能力：支持全网威胁定位、一键文件隔离、一键主机隔离、设备联动响应机制。
部署备份一体机，对综治平台进行重要系统的备份和存储，满足等保 2.0 三级中对于关键数据的备份要求。
本次项目中部署网络审计系统，定期对网络系统的安全策略进行评估，确定系统的安全措施是否符合标准；检测网络系统是否存在未授权的访问或异常行为，对网络流量进行实时监控，发现和捕捉潜在的安全事件；对已发生的安全事件进行追踪和分析，找出事件发生的原因，为响应提供依据。
本次项目部署数据防泄漏系统，通过对 PC 上多种操作进行监听，对于所操作数据进行数据检测。从精确匹配的关键字到内容模糊查找，从基于文件内容到基于文件属性的检测，从被动的事件上报到主动拦截，全方位的数据安全防护措施能够真正的实现数据安全。尤其是设置打印水印功能、屏幕水印功能。可以提供有效依据快速追溯机密信息被拍摄外泄的来源信息。
部署信息数字证书认证系统，为软硬件平台提供数字证书认证服务。通过派发 USBkey 作为人员

信息认证因素，做到登录有记录，操作可追溯。

4.2.6“雪亮工程”区综治物联感知数据接入平台建设升级架构设计

物联感知数据接入平台升级架构说明如下：

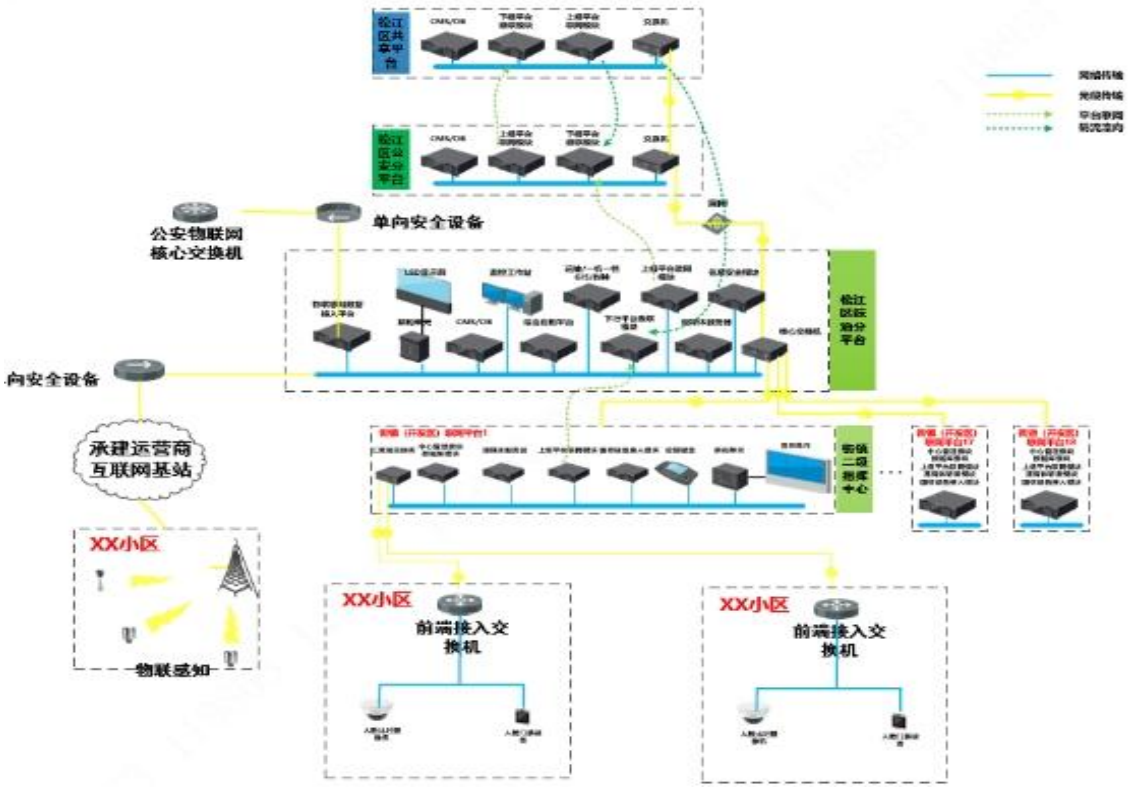

图 4 整体系统架构图

在原有(原有平台为大华 DH-DSS-C8101S2；大华 DH-NMS-B9100S3F 等)的区综治分平台一侧新增一套物联物联感知数据接入平台，前端物联网设备、人脸比对摄像机、人脸门禁等物联网感知设备按照 1400 等标准协议将数据接入综治物联感知数据接入平台实现统一管理和应用。

5、采购清单及参数要求

5.1 硬件购置

序号	功能模块	名称	配置要求	单位	数量	质保
1	综治平台汇聚扩容	物联感知数据接入平台软硬一体机	硬件要求： ★配置不低于 64G 内存，2 颗高性能国产 CPU，不低于 2.5GHZ（非超频），不少于 2 块 480G 固态硬盘，2 块 4T 硬盘，不少于 12 个硬盘槽位； 2.支持不低于 3 万路物联设备（包含门禁类数据通道）的接入，管理和应用能力； 3.支持不低于 1000 万张图片每天的转发及接收能力； 软件要求： 1.支持一站式门户管理，实现统一的鉴权、登录、资源管理体系； 2.支持服务集群，线性扩展平台的接入、存储和转发能力； 3.提供标准的平台开放接口； 4.支持统一运维，帮助用户管理设备，服务的状态以及快速安装部署；	套	1	3年

			5.支持通过 2 个不同模块分别接入抓拍数据及物联数据，可使用户快速区分； 6.支持图片通道和物联通道的接入； 7.支持对设备生命周期管理，包括设备增删改查、设备状态管理、设备冻结/解冻等管理操作；支持通过设备影子查询和存储设备属性值；支持查看设备信息、运行状态和服务调用明细情况；支持对设备设置分组、标签等操作；支持对设备进行批量增删改操作； 8.支持对系统内的资源进行标签管理，包括产品、设备、分组等，通过标签实现资源分类统一管理，支撑应用通过标签快速找到系统内相应的资源； 9.支持物联设备信息存储管理； 10.支持物模型数据存储管理； 11.支持产品信息、标签信息、分组信息，基础数据等信息的管理； 12.支持设备日志数据的存储查询管理； 13.支持创建泛协议实例、支持实例的安全管理、支持实例的接入管理，查看接入实例的详细信息、支持实例下的设备详情查看、支持泛协议 SDK 下载；			
2	综治平台汇聚扩容	物联感知数据库	硬件要求： ★配置不低于 2 块 4T 硬盘，3 块 480G 硬盘，不低于 128G 内存，不少于 4 个 GE 电口，不低于 2 颗国产化 ARM 架构，32 核，≥2.5GHz 2.支持横向扩展，单套支撑不少于 25 亿条数据量存储和分析，集群可支持 PB 级数据量的存储； 软件要求： 1.数据生命周期管理功能：支持用户自定义配置数据存储生命周期，自动按照配置信息保留指定时间范围内的数据； 2.数据冷热迁移功能：集群版特有的支持数据冷热迁移管理能力； 3.支持统一接入数据功能：针对实时流数据提供安全，可靠的数据传输平台，以消息流方式接入其他结构化数据； 4.支持车辆、人像、Mac、RFID、交通业务等数据实时接入，支持数据入库前运维上自动建表； 5.支持对数据库系统运维：支持服务启停、支持修改 IP 以及密码、支持数据库巡检；支持对数据库监控功能：支持监控系统运行情况，数据入库量统计，查询频率，支持智能诊断查询请求；提供数据管家功能：支持创建和管理数据接入任务，支持对数据表管理； 6.支持数据表分区自动管理，自动创建未来分区，自动删除过期分区； 7.支持 C、Java、R、Python、PL/pgSQL 语言的自定义函数； 8.数据均衡分布：支持多种业务数据存储在同一云数据库集群中，集群数据均衡； 9.支持与原有数据库兼容性；	套	1	3 年

3	综治平台汇聚扩容	视频国标网关（扩容）	硬件要求： ★不少于 2 颗 cpu，主频≥2.5GHz（非超频），不低于 32G 内存，2 块 4TB3.5 寸硬盘，1 块 480GSSD，4 个千兆网口； 2.不低于 2 万路视频级联和汇聚； 软件要求： 1.支持多平台多层次级联，跨域互联互通与资源共享； 2.支持联网标准协议 GB/T28181，具备符合上述协议的快速接入能力； 3.符合 GB/T28181-2011/GB/T28181-2016、公安机关视频监控系统联网标准符合性检测要求； 4.支持平台联网管理基本功能，资源共享与同步、实时预览、云台控制、录像检索/回放/下载、设备控制、报警处理等； 5.支持至少 3 级级联部署，最大可支持 16 个外域的接入； 6.项目部署中具备高度的开放性与兼容性，支持国内主流厂商视频监控系统的接入； 7.支持按域在线解析国标注册、心跳、订阅、实时业务、录像业务、平台业务报文，查看详情，支持根据任务状态、会话 ID、创建时间对业务请求进行筛选查询。点击查看按钮显示查看详情； 8.可接入原有网关集群，完成网关扩容；	套	3	3 年
4	综治平台汇聚扩容	一机一档数据治理平台（扩容）	硬件要求： ★不低于 2 颗 CPU，≥2.5GHZ（非超频），不少于 2 块 4T 硬盘； 2.支持不少于 3w 路设备信息管理； 软件要求： 1.同步联网平台通道支持同步联网平台通道、圈梁和实时消息同步； 2.支持扩展属性维护对通道进行扩展字段维护； 3.支持自定义标签支持自定义标签、新增、编辑、删除并将其应用到点位上； 4.支持列表查询列表数据过滤，组织、摄像头类型、关键字等； 5.支持扩展属性维护对通道进行扩展字段维护； 6.支持自定义标签支持自定义标签、新增、编辑、删除并将其应用到点位上； 7.支持列表查询列表数据过滤，组织、摄像头类型、关键字等； 8.支持条件筛选导出点位导出 excel，支持根据筛选条件导出点位信息； 9.支持导入点位信息，维护点位新增； 10.支持批量修改操作支持对点位信息进行批量修改，可根据组织、设备、对其下所有点位修改； 11.需要兼容原有一机一档管理平台；	套	1	3 年
5	综治平台汇聚扩容	运维平台（升级）	硬件要求： ★不低于 2 颗 CPU，≥2.5GHZ（非超频），不少于 2 块 4T 硬盘； 2.不低于 3 万路运维通道扩容； 软件要求： 1.支持对建设点位在线状态、视频点播、视频质量、录像	套	1	3 年

			完整性的检测，与编码设备、存储设备、门禁设备、服务器与交换机等设备核心运行指标的一体化监控，主动发现异常故障并告警，结合工单管理系统、运维统计及服务报告等实现业务闭环； 2.支持统计图片通道的通道总数、在线数、离线数、今日离线时长、在线率； 3.抓拍数据支持按照组织统计，统计数据包括通道总数、抓拍达标数、未知数、抓拍数据达标率、活跃、活跃率； 4.支持查看物联设备的在线状态、状态持续时长，并可按照在线状态、状态持续时长进行排序； 5.支持物联设备在线状态搜索，可按照资产名称、IP 地址、制造厂商、所属组织、在线状态检索监控信息； 6.抓拍数据支持按照组织统计，统计数据包括通道总数、抓拍达标数、未知数、抓拍数据达标率、活跃、活跃率； 7.抓拍数据达标性用于表征图片通道的结构化数据抓拍量是否达标，达标是与过去一段时间的每日抓拍量均值进行比较； 8.支持场景图片质量异常报警，包含清晰度异常报警、画面过暗报警、画面过亮报警、黑白图像报警、画面偏色报警、雪花屏报警、码流异常报警、画面黑屏报警、树叶遮挡报警、雾天报警、雨天报警、雪天报警； 9.支持对图片通道的抓拍图片是否可访问进行检测;可查看通道的图片可访问性(可访问、不可访问、未知)、图片可访问次数等信息； 10.可兼容原有综治运维平台；			
6	街镇边界与核心	核心交换机	硬件要求： 含交流/高压直流总装机箱,2*主控板,4*交换网板,4*3000W 交流&高压直流电源模块,满配风机盒；48 端口 10GE 以太网光接口板；36 端口 40GE 以太网光接口板；QSFP+-40G-高速电缆-5m-；QSFP+-40G-单模模块(1310nm,10km,LC)*2	台	2	3 年
7	街镇边界与核心	汇聚交换机	硬件要求： 含一体化总装机箱*1,主控板*2；4 端口万兆集群业务子卡*2；48 端口万兆以太网光接口板；2200W 交流电源模块*2；光模块-SFP+-850nm-1G~10G-10m*4	台	2	3 年
8	街镇边界与核心	万兆光模块	硬件要求： 万兆光模块-SFP+-10G-单模模块(1310nm,10km,LC）	个	20	3 年
9	安全管理区	终端威胁防御系统（EDR）	硬件要求： ★不少于 1 颗 32 核 CPU，2.0G/64G/240G/2T 企业级*2/标配三合一、红盘/三年质保、硬盘不回收	台	1	3 年
10	安全管理区	数据防泄漏系统	硬件要求： ★不少于 1 颗 32 核 CPU， 2.0G/64G/240G/2T 企业级*2 标配三合一、红盘/三年质保、硬盘不回收	台	1	3 年

11	安全管理区	信息数字证书认证系统	硬件要求： ★不少于 1 颗 32 核 CPU， 2.0G/64G/240G/2T 企业级*2/标配三合一、红盘/三年质保、硬盘不回收	台	1	3 年

5.2 成品软件购置

序号	功能模块	名称	配置要求	单位	数量	质保
1	横向安全边界区	下一代防火墙	软件要求： 增加防病毒功能共 3 年，包含病毒库升级，原设备不带，含专业版快速查杀病毒库不少于 1 年升级许可	套	2	3 年
2	街镇边界与核心	下一代防火墙	软件要求： 增加防病毒功能共 3 年，包含病毒库升级，原设备不带，含专业版快速查杀病毒库不少于 1 年升级许可	套	2	3 年
3	互联网出口边界	下一代防火墙	软件要求： 增加防病毒功能共 3 年，包含病毒库升级，原设备不带，含专业版快速查杀病毒库不少于 1 年升级许可	套	2	3 年
4	应用系统区	下一代防火墙	软件要求： 增加防病毒功能共 3 年，包含病毒库升级，原设备不带，含专业版快速查杀病毒库不少于 1 年升级许可	套	2	3 年
5	安全管理区	下一代防火墙	软件要求： 增加防病毒功能共 3 年，包含病毒库升级，原设备不带，含专业版快速查杀病毒库不少于 1 年升级许可	套	2	3 年
6	安全管理区	终端威胁防御系统（EDR）	软件要求： 1.采用 B/S 架构的管理控制中心，支持在国产化环境中部署，客户端支持国内外主流操作系统等环境中部署； 2.具备基因特征、人工智能、行为检测、云查杀多种引擎，且引擎可自定义配置； 3.提供 U 盘防护、ARP 防御、脚本防御、应用程序加固等实时防御功能； 4.支持勒索诱捕功能，诱饵文件可被实时监控，当勒索病毒对该文件进行攻击或加密操作时进行拦截；	套	1	3 年

			5.支持检测挖矿木马攻击行为，实时阻断挖矿木马挖矿行为； 6.支持 Powershell 和 VBScript 脚本防御，支持 Office、PDF、浏览器和视频播放器应用加固，防范无文件攻击和溢出攻击； 7.提供终端远程卸载、重启、关机、隔离能力，具备基线核查和自动加固、漏洞检测和自动修复、网络管控、进程管控、违规外联、外设管控、文件分发、远程协助、广告拦截、安全通告等功能； 8.支持对终端行为的全面监控与数据采集，包括终端进程、驱动、模块、网络连接、DNS 访问、浏览器 HTTP/HTTPS 访问、文件操作、外设操作、打印操作、注册表变更、账户操作、操作系统日志等 9.提供自身安全防护能力，防止恶意程序攻击，无法终止进程、修改文件、更改注册表内容； 10.支持对国内外主流操作系统、国产 CPU 等异构客户端的集中统一管理； 11.支持 IPV6 或 IPV4/IPV6 混合网络内部署和使用； 12.支持联动本次态势分析与安全运营系统，同步现网终端威胁信息，支持接收态势分析与运营系统下发的处置任务，对相应终端执行杀毒、桌管等命令			
7	安全管理区	终端威胁防御系统（EDR）	软件要求： ★操作系统需通过中国信息安全测评中心的安全可靠评测	套	1	3年
8	安全管理区	终端威胁防御系统（EDR）	软件要求： 1 个 LinuxServer 客户端防病毒功能授权，含 3 年升级服务。针对服务器操作系统进行病毒查杀，提供主动防御系统防护等功能。系统默认支持 LinuxServer。	个	500	3年
9	安全管理区	终端威胁防御系统（EDR）	软件要求： 1 个 WindowsServer 客户端防病毒功能授权，含 3 年升级服务。针对服务器操作系统进行病毒查杀，提供主动防御系统防护等功能。系统默认支持 WindowsServer。	个	100	3年
10	安全管理区	终端威胁防御系统（EDR）	软件要求： 1 个 Windows PC 客户端防病毒功能授权,含 3 年升级服务。防病毒的病毒查杀支持多引擎的协同工作对病毒、木马、恶意软件、引导区病毒、BIOS 病毒等进行查杀，提供主动防御系统防护等功能。客户端系统默认支持 Windows XP/VISTA/WIN7/WIN8/WIN10。	个	2000	3年
11	安全管理区	漏洞扫描	软件要求： 增加后二年规则库，原设备自带一年	套	2	3年

12	安全管理区	数据防泄漏系统	软件要求： 1.支持 B/S 管理，配置 2000 个客户端授权；支持屏幕水印功能，支持在屏幕水印上显示责任人、主机名、IP 地址、MAC 地址、登录用户、时间等信息，支持用户自定义显示内容； 2.服务端支持 CentOS、欧拉等环境，支持 Docker 部署方式；客户端支持 win7 及以上操作系统,支持麒麟、UOS 等国产操作系统； 3.支持统计普通终端和国产终端的在线数、离线数； 4.支持统计当日阻断事件、审计事件、事件总数； 5.支持统计阻断事件总数、审计事件总数、事件总数； 6.支持展示今日、近一周、近一月等周期的风险事件趋势； 7.支持统计终端所在的责任人、部门、IP、MAC 地址、计算机名、操作系统、客户端版本等信息； 8.支持以 excel 等格式导出终端信息列表； 9.支持可执行文件的执行方式选择，至少包括接收并运行、只接收、后台运行等 10.支持对即时通讯、邮件客户端、网盘客户端、浏览器上传、剪切板、打印、刻录、网络共享、移动存储、远程协助等外泄通道进行监控，支持对每个通道进行阻断、提示、审计等处理行为配置 11.支持记录敏感信息打印事件、刻录事件、邮件客户端传输事件、即时通讯传输事件、网络客户端传输事件、网络共享传输事件、浏览器上传事件、剪切板移动事件、移动存储事件、远程协助拷贝事件等类型日志； 12.支持记录时间、终端 ID、终端 IP、防御类型、数据类型、部门、计算机名称、MAC 地址、文件哈希值、文件路径、处置动作等详细信息； 13.支持以 excel 的形式进行安全日志导出；	套	1	3 年
13	安全管理区	数据防泄漏系统	软件要求： ★操作系统需通过中国信息安全测评中心的安全可靠评测	套	1	3 年
14	安全管理区	信息数字证书认证系统	软件要求： 由证书认证系统(CA)、证书注册系统(RA)、在线证 书状态查询系统(OCSP)、目录服务器(LDAP)、用户证书自助服务系统(User- Service，简称 US)等相关软件组成，可提供基于 SM2 密码算法的数字证书全生命周期 管理服务	套	1	3 年
15	安全管理区	信息数字证书认证系统	软件要求： 用于数据库部署（含 3 年授权） ★数据库需通过中国信息安全测评中心的安全可靠评测	套	1	3 年
16	安全管理区	信息数字证书认证系统	软件要求： 用于管理端软件部署	套	1	3 年

17	安全管理区	信息数字证书认证系统	软件要求： ★操作系统需通过中国信息安全测评中心的安全可靠评测	套	1	3年

5.3 安全产品购置

序号	功能模块	名称	配置要求	单位	数量	质保
1	横向安全边界区	下一代防火墙	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、4 个万兆光口，配置 4 个千兆多模光模块、4 个万兆多模光模块； 2.网络层吞吐量≥38Gbps，应用层吞吐量≥19Gbps，每秒新建连接速率≥260 万/秒，最大并发连接数≥6000 万； 软件要求： 1.支持根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口等条件配置链路负载算法； 2.支持通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置； 3.支持域名控制，支持对多级域名进行控制，域名对象支持通配符； 4.支持基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级，支持白名单； 5.支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，支持控制所有或单 IP 会话总数及单 IP 新建连接数； 6.支持基于 HTTP、FTP、TELNET、SMTP、POP3、IMAP 等协议的内容过滤策略； 7.支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理； 8.支持在 WEB 界面进行 PING、TRACEROUTE、TCP、HTTP、DNS 诊断方式；支持在 WEB 界面进行网络抓包，支持设置接口、IP、协议、端口、包数等过滤条件，抓包文件支持导出； 9.支持日志本地存储，支持对不同类型日志设置存储空间或存储时间；支持日志外发至多个 SYSLOG 服务器；	台	2	3年
2	横向安全边界区	入侵防御系统	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、6 个万兆光口，配置 4 个千兆多模光模块、6 个万兆多模光模块； 2.满检速率≥49Gbps，最大并发连接数≥1970 万；兼容国家信息安全漏洞库； 软件要求： 1.支持按照受害者、攻击者、威胁事件、攻击类型、攻击主机、受害主机、应用类型等维度进行综合分析；支持威胁事件的失陷/成功/尝试/失败等攻击结果、攻击事件级	台	2	3年

			别、攻击类型分布、攻击阶段、事件详情等信息；支持按照时间范围、攻击者 IP、事件类型、处置状态、来源、攻击者所属国家等条件综合分析攻击者信息。 2.支持入侵攻击检测，支持 10000 种漏洞规则，同时支持在界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则； 3.支持服务器非法外联检测，支持 DGA 恶意域名检测，支持 HTTP 隧道检测，支持违规应用检测； 4.支持对多种加密流量的分析检测； 5.支持独立的僵尸主机检测库，支持 10000 种以上的僵尸主机规则库； 6.支持带外管理,保障管理网络和业务网络相互隔离； 7.支持 SNMP V1/V2/V3/Trap 等标准网络管理协议； 8.支持规则库在线升级、离线升级； 9.支持通过 Syslog 或 Kafka 方式将日志数据发送给第三方平台；支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间； 10.支持手动导出和自动导出，支持导出 PDF、Word、HTML、Excel 等多种文件类型报表；			
3	街镇边界与核心	下一代防火墙	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、4 个万兆光口，配置 4 个千兆多模光模块、4 个万兆多模光模块； 2.网络层吞吐量≥38Gbps，应用层吞吐量≥19Gbps，每秒新建连接速率≥260 万/秒，最大并发连接数≥6000 万； 软件要求： 1.支持根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口等条件配置链路负载算法； 2.支持通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置； 3.支持域名控制，支持对多级域名进行控制，域名对象支持通配符； 4.支持基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级，支持白名单； 5.支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，支持控制所有或单 IP 会话总数及单 IP 新建连接数； 6.支持基于 HTTP、FTP、TELNET、SMTP、POP3、IMAP 等协议的内容过滤策略； 7.支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理； 8.支持在 WEB 界面进行 PING、TRACEROUTE、TCP、HTTP、DNS 诊断方式；支持在 WEB 界面进行网络抓包，支持设置接口、IP、协议、端口、包数等过滤条件，抓包文件支持导出； 9.支持日志本地存储，支持对不同类型日志设置存储空间	台	2	3 年

			或存储时间；支持日志外发至多个 SYSLOG 服务器；			
4	街镇边界与核心	入侵防御系统	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、6 个万兆光口，配置 4 个千兆多模光模块、6 个万兆多模光模块； 2.满检速率≥49Gbps，最大并发连接数≥1970 万；兼容国家信息安全漏洞库； 软件要求： 1.支持按照受害者、攻击者、威胁事件、攻击类型、攻击主机、受害主机、应用类型等维度进行综合分析；支持威胁事件的失陷/成功/尝试/失败等攻击结果、攻击事件级别、攻击类型分布、攻击阶段、事件详情等信息；支持按照时间范围、攻击者 IP、事件类型、处置状态、来源、攻击者所属国家等条件综合分析攻击者信息。 2.支持入侵攻击检测，支持 10000 种漏洞规则，同时支持在界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则； 3.支持服务器非法外联检测，支持 DGA 恶意域名检测，支持 HTTP 隧道检测，支持违规应用检测； 4.支持对多种加密流量的分析检测； 5.支持独立的僵尸主机检测库，支持 10000 种以上的僵尸主机规则库； 6.支持带外管理,保障管理网络和业务网络相互隔离； 7.支持 SNMP V1/V2/V3/Trap 等标准网络管理协议； 8.支持规则库在线升级、离线升级； 9.支持通过 Syslog 或 Kafka 方式将日志数据发送给第三方平台；支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间； 10.支持手动导出和自动导出，支持导出 PDF、Word、HTML、Excel 等多种文件类型报表；	台	2	3 年
5	街镇边界与核心	统一安全接入网关系统（管理平台）	硬件要求： ★CPU≥32 核，内存≥256G，硬盘：HDD≥36T，SSD≥480G； 2.配置双电源，千兆电口≥6 个、千兆光口≥4 个，扩展槽≥3 个，支持终端接入数≥100000 个； 软件要求： 1.含不少于可管理 20 台物联网安全接入网关设备的授权许可； 2.支持全资产类型一机一档功能，资产类型包括 IPC、PC、NVR、服务器、网络设备、门禁、物联感知设备等，同时支持一机一档按资产类型导入导出功能； 3.支持资产属性完整度检查功能，可查看到单个资产的属性完整度和整个类型属性完整度的统计信息； 4.支持一机一档资产类型和属性自定义扩展功能，可对新添加的资产自定义新的类型，同时可对该类型资产自定义新的属性；	套	1	3 年

			5.支持一机一档信息双平台上报功能，可进行一机一档远程同步配置，上报成功后，可在其他平台查看一机一档信息； 6.支持资产注册及审批功能，资产注册用户可登录平台填写资产注册信息并提交申请，管理员用户可在申请记录中进行审批，同时支持资产注册流程可基于资产一机一档属性录入完整度下发阻断策略功能； 7.支持基于多维度的资产在线率统计功能，可根据资产类型和属性进行分组在线率统计； 8.支持通过组织架构、子网结构等维度进行可视化展示；支持通过可视化界面查看 IP 地址分配情况，查看已分配 IP 地址对应资产状态及资产属性；支持在 IP 资源可视化界面手动添加、修改资产属性；支持 IP 地址自动回收功能，可自定义设计回收周期； 9.支持基于安全日志自动生成工单，派发工单可分为自动和手动，支持根据派工模板自动派发工单功能和手动派发工单功能； 10.支持工单运维用户分权管理功能，不同工单运维用户仅能查看其对应的工单信息，同时支持工单运维用户申请延期功能； 11.支持自定义知识库功能，管理员可根据事件自定义处理意见并派发工单；支持工单统计功能，可查看本月待处理工单、本月工单热度分布、工单类别统计和超时工单统计；支持根据资产查看历史工单信息； 12.支持基于 web 特征自学习识别功能，支持基于端口特征自学习识别功能，支持基于型号特征自学习识别功能，支持基于流量特征自学习识别功能； 13.支持近七日日志分析，支持近七日告警日志统计，支持近七日告警日志 TOP5； 14.支持各类型日志分析统计，包括非可信设备、非法扫描、敏感端口、非法外联等，同时支持日志聚合功能； 15.支持对新入网终端进行资产识别，将终端添加到资产库；支持对未知业务协议特征自学习功能，下发特征后不再产生告警日志；支持对新入网业务延时阻断功能； 16.支持自定义生成报表，可查看自定义时间段的资产、预警信息总览、预警信息统计、资产信息统计等，同时支持周期自动生成报表，时间周期可以选择天； 17.支持联动本次态势分析与安全运营系统，同步终端资产信息，支持接收态势分析与安全运营系统下发的资产管理策略；			
6	街镇边界与核心	统一安全接入网关系统（核心侧）	硬件要求： 1.实配双电源，千兆电口≥8 个、千兆光口≥2 个，设备吞吐量≥10G，支持接入终端数 500 个以上； 软件要求： 1.无缝对接统一安全接入网关管理平台； 2.设备本身不能出现对视频业务产生如视频抖动、卡顿等现象，基于 SIP 的视/音频传输时延＜20 微秒； 3.支持 MAC 认证功能，MAC 地址在白名单中的终端能够通过设备进行正常访问，MAC 地址不在设备白名单中的终端通讯会被阻断；支持 IP 认证功能，IP 地址在白名单中的终端能够通过设备进行正常访问，IP 地址不在设	套	1	3年

			备白名单中的终端通讯会被阻断； 4.支持符合 GB/T28181 标准协议接入网络的终端进行通信，采用非 GB/T28181 标准协议接入网络进行通信的终端会被系统阻断并产生告警日志； 5.支持 GA/T1400 协议检测功能，可对不符合 GA/T1400 协议的终端进行阻断并告警； 6.支持对扫描行为的识别与阻断功能，可对存在扫描行为的终端进行阻断并告警； 7.支持基于 Portal 认证的实名制违规外联检测机制，基于 portal 认证入网的设备，存在违规外联行为的终端，通讯会被阻断；支持无感知方式的违规外联检测机制，存在违规外联行为的终端，通讯会被阻断； 8.支持基于历史数据重放检测功能，可对存在历史数据重放攻击的终端进行阻断； 9.支持一机一档信息双平台上报功能，可进行一机一档远程同步配置，上报成功后，可在其他平台查看一机一档信息； 10.支持资产注册及审批功能，资产注册用户可登录平台填写资产注册信息并提交申请，管理员用户可在申请记录中进行审批，同时支持资产注册流程可基于资产一机一档属性录入完整度下发阻断策略功能； 11.支持基于安全日志自动生成工单，派发工单可分为自动和手动，支持根据派工模板自动派发工单功能和手动派发工单功能；			
7	街镇边界与核心	统一安全接入网关系统（街镇侧 1）	硬件要求： 1.冗余电源；千兆电口≥6 个、千兆光口≥4 个、万兆光口≥4 个，扩展槽≥4 个；设备吞吐量≥50G，支持接入终端数 10000 个以上； 软件要求： 1.无缝对接统一安全接入网关管理平台； 2.设备本身不能出现对视频业务产生如视频抖动、卡顿等现象，基于 SIP 的视/音频传输时延＜20 微秒； 3.支持 MAC 认证功能，MAC 地址在白名单中的终端能够通过设备进行正常访问，MAC 地址不在设备白名单中的终端通讯会被阻断；支持 IP 认证功能，IP 地址在白名单中的终端能够通过设备进行正常访问，IP 地址不在设备白名单中的终端通讯会被阻断； 4.支持符合 GB/T28181 标准协议接入网络的终端进行通信，采用非 GB/T28181 标准协议接入网络进行通信的终端会被系统阻断并产生告警日志； 5.支持 GA/T1400 协议检测功能，可对不符合 GA/T1400 协议的终端进行阻断并告警； 6.支持对扫描行为的识别与阻断功能，可对存在扫描行为的终端进行阻断并告警； 7.支持基于 Portal 认证的实名制违规外联检测机制，基于 portal 认证入网的设备，存在违规外联行为的终端，通讯会被阻断；支持无感知方式的违规外联检测机制，存在违规外联行为的终端，通讯会被阻断； 8.支持基于历史数据重放检测功能，可对存在历史数据重放攻击的终端进行阻断； 9.支持一机一档信息双平台上报功能，可进行一机一档远	套	9	3 年

			程同步配置，上报成功后，可在其他平台查看一机一档信息； 10.支持资产注册及审批功能，资产注册用户可登录平台填写资产注册信息并提交申请，管理员用户可在申请记录中进行审批，同时支持资产注册流程可基于资产一机一档属性录入完整度下发阻断策略功能； 11.支持基于安全日志自动生成工单，派发工单可分为自动和手动，支持根据派工模板自动派发工单功能和手动派发工单功能；			
8	街镇边界与核心	统一安全接入网关系统（街镇侧 2）	硬件要求： 1.冗余电源，千兆电口≥6 个、千兆光口≥4 个、万兆光口≥2 个，扩展槽≥3 个，设备吞吐量≥25G，支持接入终端数 5000 个以上； 软件要求： 1.无缝对接统一安全接入网关管理平台； 2.设备本身不能出现对视频业务产生如视频抖动、卡顿等现象，基于 SIP 的视/音频传输时延＜20 微秒； 3.支持 MAC 认证功能，MAC 地址在白名单中的终端能够通过设备进行正常访问，MAC 地址不在设备白名单中的终端通讯会被阻断；支持 IP 认证功能，IP 地址在白名单中的终端能够通过设备进行正常访问，IP 地址不在设备白名单中的终端通讯会被阻断； 4.支持符合 GB/T28181 标准协议接入网络的终端进行通信，采用非 GB/T28181 标准协议接入网络进行通信的终端会被系统阻断并产生告警日志； 5.支持 GA/T1400 协议检测功能，可对不符合 GA/T1400 协议的终端进行阻断并告警； 6.支持对扫描行为的识别与阻断功能，可对存在扫描行为的终端进行阻断并告警； 7.支持基于 Portal 认证的实名制违规外联检测机制，基于 portal 认证入网的设备，存在违规外联行为的终端，通讯会被阻断；支持无感知方式的违规外联检测机制，存在违规外联行为的终端，通讯会被阻断； 8.支持基于历史数据重放检测功能，可对存在历史数据重放攻击的终端进行阻断； 9.支持一机一档信息双平台上报功能，可进行一机一档远程同步配置，上报成功后，可在其他平台查看一机一档信息； 10.支持资产注册及审批功能，资产注册用户可登录平台填写资产注册信息并提交申请，管理员用户可在申请记录中进行审批，同时支持资产注册流程可基于资产一机一档属性录入完整度下发阻断策略功能； 11.支持基于安全日志自动生成工单，派发工单可分为自动和手动，支持根据派工模板自动派发工单功能和手动派发工单功能；	套	9	3 年
9	互联网出口边界	下一代防火墙	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、4 个万兆光口，配置 4 个千兆多模光模块、4 个万兆多模光模块； 2.网络层吞吐量≥38Gbps，应用层吞吐量≥19Gbps，每秒新建连接速率≥260 万/秒，最大并发连接数≥6000 万；	台	2	3 年

			软件要求： 1.支持根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口等条件配置链路负载算法； 2.支持通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置； 3.支持域名控制，支持对多级域名进行控制，域名对象支持通配符； 4.支持基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级，支持白名单； 5.支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，支持控制所有或单 IP 会话总数及单 IP 新建连接数； 6.支持基于 HTTP、FTP、TELNET、SMTP、POP3、IMAP 等协议的内容过滤策略； 7.支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理； 8.支持在 WEB 界面进行 PING、TRACEROUTE、TCP、HTTP、DNS 诊断方式；支持在 WEB 界面进行网络抓包，支持设置接口、IP、协议、端口、包数等过滤条件，抓包文件支持导出； 9.支持日志本地存储，支持对不同类型日志设置存储空间或存储时间；支持日志外发至多个 SYSLOG 服务器；			
10	互联网出口边界	入侵防御系统	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、6 个万兆光口，配置 4 个千兆多模光模块、6 个万兆多模光模块； 2.满检速率≥49Gbps，最大并发连接数≥1970 万；兼容国家信息安全漏洞库 软件要求： 1.支持按照受害者、攻击者、威胁事件、攻击类型、攻击主机、受害主机、应用类型等维度进行综合分析；支持威胁事件的失陷/成功/尝试/失败等攻击结果、攻击事件级别、攻击类型分布、攻击阶段、事件详情等信息；支持按照时间范围、攻击者 IP、事件类型、处置状态、来源、攻击者所属国家等条件综合分析攻击者信息。 2.支持入侵攻击检测，支持 10000 种漏洞规则，同时支持在界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则； 3.支持服务器非法外联检测，支持 DGA 恶意域名检测，支持 HTTP 隧道检测，支持违规应用检测； 4.支持对多种加密流量的分析检测； 5.支持独立的僵尸主机检测库，支持 10000 种以上的僵尸主机规则库； 6.支持带外管理,保障管理网络和业务网络相互隔离； 7.支持 SNMP V1/V2/V3/Trap 等标准网络管理协议； 8.支持规则库在线升级、离线升级；	台	2	3年

			9.支持通过 Syslog 或 Kafka 方式将日志数据发送给第三方平台；支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间； 10.支持手动导出和自动导出，支持导出 PDF、Word、HTML、Excel 等多种文件类型报表；			
11	互联网出口边界	抗 DDOS 系统	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、4 个万兆光口，内存≥32GB，硬盘≥4TB，配置 4 个千兆多模光模块、4 个万兆多模光模块； 2.清洗性能≥10Gbps，网络层吞吐量≥19Gbps，最大并发数≥1000 万，每秒新建连接数≥25 万； 软件要求： 1.至少支持在线串接、旁路检测和旁路清洗三种模式； 2.支持透明部署、旁路回注、旁路下注、主备模式、负载模式、集群及双活等部署模式，支持 IPv4/IPv6 双栈部署模式； 3.支持镜像、分光、NetFlow 等方式进行数据采集； 4.支持 Flow 流数据流转发，转发策略支持配置目的 IP 和目的端口； 5.支持 IP 地址静态黑白名单，支持 IP 地址动态黑白名单，支持 IP 地址黑白名单的导入、导出； 6.支持域名定义防护对象组、防护对象、目的黑白名单； 7.支持抓包名称、抓包时长、接口、抓包数量、协议类型、IP 报文长度、报文截断长度、源、目的地址、源或目的地址、源端口、目的端口、源或目的端口等；支持抓包溯源与指纹提取进行攻击源 IP 溯源； 8.支持基于源 IP、目的 IP、源和目的 IP、协议等统计方式对 IPv4 或 IPv6 地址进行连接排名的统计分析；	台	2	3 年
12	互联网出口边界	抗 DDOS 系统（千兆板卡扩容）	硬件要求： 千兆板卡：4 个 RJ45 接口 4 个 SFP 插槽,电口支持 2 组 bypass。	个	2	3 年
13	应用系统区	下一代防火墙	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、4 个万兆光口，配置 4 个千兆多模光模块、4 个万兆多模光模块； 2.网络层吞吐量≥38Gbps，应用层吞吐量≥19Gbps，每秒新建连接速率≥260 万/秒，最大并发连接数≥6000 万； 软件要求： 1.支持根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口等条件配置链路负载算法； 2.支持通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置； 3.支持域名控制，支持对多级域名进行控制，域名对象支持通配符； 4.支持基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持	台	2	3 年

			带宽策略优先级，支持白名单； 5.支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，支持控制所有或单 IP 会话总数及单 IP 新建连接数； 6.支持基于 HTTP、FTP、TELNET、SMTP、POP3、IMAP 等协议的内容过滤策略； 7.支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理； 8.支持在 WEB 界面进行 PING、TRACEROUTE、TCP、HTTP、DNS 诊断方式；支持在 WEB 界面进行网络抓包，支持设置接口、IP、协议、端口、包数等过滤条件，抓包文件支持导出； 9.支持日志本地存储，支持对不同类型日志设置存储空间或存储时间；支持日志外发至多个 SYSLOG 服务器；			
14	应用系统区	入侵防御系统	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、6 个万兆光口，配置 4 个千兆多模光模块、6 个万兆多模光模块； 2.满检速率≥49Gbps，最大并发连接数≥1970 万；兼容国家信息安全漏洞库 软件要求： 1.支持按照受害者、攻击者、威胁事件、攻击类型、攻击主机、受害主机、应用类型等维度进行综合分析；支持威胁事件的失陷/成功/尝试/失败等攻击结果、攻击事件级别、攻击类型分布、攻击阶段、事件详情等信息；支持按照时间范围、攻击者 IP、事件类型、处置状态、来源、攻击者所属国家等条件综合分析攻击者信息。 2.支持入侵攻击检测，支持 10000 种漏洞规则，同时支持在界面通过漏洞 ID、漏洞名称、危险等级、漏洞 CVE 标识、漏洞描述等条件查询漏洞特征信息，支持用户自定义 IPS 规则； 3.支持服务器非法外联检测，支持 DGA 恶意域名检测，支持 HTTP 隧道检测，支持违规应用检测； 4.支持对多种加密流量的分析检测； 5.支持独立的僵尸主机检测库，支持 10000 种以上的僵尸主机规则库； 6.支持带外管理,保障管理网络和业务网络相互隔离； 7.支持 SNMP V1/V2/V3/Trap 等标准网络管理协议； 8.支持规则库在线升级、离线升级； 9.支持通过 Syslog 或 Kafka 方式将日志数据发送给第三方平台；支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间； 10.支持手动导出和自动导出，支持导出 PDF、Word、HTML、Excel 等多种文件类型报表；	台	2	3 年
15	应用系统区	Web 应用防护系统	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、2 个万兆光口，配置 4 个千兆多模光模块、2 个万兆多模光模块； 2.HTTP 吞吐量≥9Gbps，HTTP 请求速率≥6 万/秒，HTTP 并发连接数≥220 万；兼容国家信息安全漏洞库	台	2	3 年

			软件要求： 1.支持透明串联、负载均衡、反向代理、旁路监测等； 2.支持基于源 IP 地址、目的 IP 地址、协议类型及接口区域等条件的访问控制，支持 IP 黑白名单配置，支持 URL 路径限制； 3.支持识别和阻断多种攻击类型进行防护； 4.支持管控非法、违规网站的访问行为，具备海量的 URL 分类库； 5.支持对上传及下载最大文件大小、文件扩展名、MIME 类型等进行控制； 6.支持对指定 URL 地址进行协议合规性检查； 7.支持通过学习正常 URL 参数的长度、参数类型、请求方法等数据特点创建白名单模型防护策略； 8.支持对攻击事件类型，攻击源，URL 攻击次数统计与 web 展示；支持多条件的安全日志组合查询，查询条件包括但不限于日志类型、日志级别、生成时间； 9.支持多种安全日志存储方式，至少包括本机、日志服务器等不同方式等； 10.支持主备、主主负载均衡等模式、支持全局配置同步和策略同步等、支持硬件 bypass、软件 bypass、支持接口状态联动；			
16	安全管理区	下一代防火墙	硬件要求： 1.符合标准机柜摆放、冗余电源，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、4 个万兆光口，配置 4 个千兆多模光模块、4 个万兆多模光模块； 2.网络层吞吐量≥38Gbps，应用层吞吐量≥19Gbps，每秒新建连接速率≥260 万/秒，最大并发连接数≥6000 万； 软件要求： 1.支持根据源/目的 MAC、源/目的 IP、源/目的端口、五元组、端口等条件配置链路负载算法； 2.支持通过一条策略实现五元组、源 MAC、源地区、目的地区、域名、应用、服务、时间、长连接、并发会话、WEB 认证、IPS、AV、URL 过滤、WAF、邮件安全、数据过滤、文件过滤、审计等功能配置； 3.支持域名控制，支持对多级域名进行控制，域名对象支持通配符； 4.支持基于上下行区域、地址、地理对象、用户/用户组、服务/服务组、应用/应用组和时间等配置带宽策略，支持带宽策略优先级，支持白名单； 5.支持对指定的源/目的地址对象、源/目的地理对象、应用制定连接限制策略，支持控制所有或单 IP 会话总数及单 IP 新建连接数； 6.支持基于 HTTP、FTP、TELNET、SMTP、POP3、IMAP 等协议的内容过滤策略； 7.支持策略生命周期管理功能，支持对安全策略修改的时间、原因、变更类型进行统一管理，便于策略的运维与管理； 8.支持在 WEB 界面进行 PING、TRACEROUTE、TCP、HTTP、DNS 诊断方式；支持在 WEB 界面进行网络抓包，支持设置接口、IP、协议、端口、包数等过滤条件，抓包文件支持导出；	台	2	3年

			9.支持日志本地存储，支持对不同类型日志设置存储空间或存储时间；支持日志外发至多个 SYSLOG 服务器；			
17	安全管理区	数据库审计	硬件要求： 1.符合标准机柜摆放、冗余电源，内存≥32GB，硬盘≥4TB，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、2 个万兆口，配置 4 个千兆多模光模块、2 个万兆多模光模块； 2.整机吞吐≥5Gbps，每秒记录事件≥5 万条； 软件要求： 1.支持旁路部署、代理部署、分布式部署； 2.支持自动发现数据库类型、IP 地址、端口号等信息，支持一键审计； 3.支持国产化/非国产化的关系型数据库、非关系型数据库等； 4.支持审计访问数据库的时间、源目 IP、源目端口、事件 ID、源目 MAC、应用协议、实名用户、规则名称、告警描述、数据库名、客户端程序、数据库用户等 5.支持数据库请求和返回的双向审计，支持操作类、表、视图、索引、触发器、游标、事务等各种对象的 SQL 操作审计； 6.支持以访问数据库时间、源目 IP、源目端口、数据库名、客户端程序、数据库用户名、SQL 语句敏感类型等字段作为查询和统计条件； 7.支持对审计日志中敏感数据（身份证号、手机号、银行卡号等）进行掩码处理； 8.支持自定义格式报表，支持日、周、月等周期自动生成报表、持 DOCX、HTML、PDF、XLSX 等格式导出报表； 9.支持历史版本回退，支持抓包工具，支持一键巡检，支持配置导入导出，支持多种方式外发日志，支持磁盘清理，支持磁盘利用率、保存时限配置等磁盘清理条件；	台	1	3年
18	安全管理区	堡垒机	硬件要求： 1.符合标准机柜摆放、冗余电源，内存≥32GB，硬盘≥4TB，配置不少于 1 个管理口、1 个 HA 口、4 个千兆电口、4 个千兆光口、2 个万兆光口，配置 4 个千兆多模光模块、2 个万兆多模光模块； 2.图形并发≥200，字符并发≥400，不少于 400 个主机/设备许可； 软件要求： 1.支持物理旁路部署，支持双机部署，支持在 IPV4/IPV6 网络环境下部署，支持管理 IPV4/IPV6 资产； 2.支持用户增删改查、锁定、解锁、清空等操作，支持以部门方式对用户进行分组管理，支持用户批量导入和导出，支持用户有效期定义，支持批量修改用户所属部门、用户角色、密码、邮箱、手机号、有效期、密码认证方式、多因素认证等信息； 3.支持本地认证和三方认证服务器接入认证，支持通过 AD 域服务器、LDAP 服务器等进行用户同步，支持手动和自动同步； 4.支持资产的增删改查、锁定、解锁等操作，支持以部门的方式对资产进行分组管理，支持多种资产协议端口号	台	1	3年

			变更，支持资产批量导入和导出。 5.支持按照用户、用户组、账号、账号组、资产组进行一对一、一对多、多对一、多对多授权； 6.支持设置运维授权的有效期； 7.支持以 EXCEL、PDF 等方式导出授权关系； 8.支持 web 页面直接发起运维，无需安装任何控件，并同时支持调用 SecureCRT、Xshell、Putty 等客户端工具实现单点登陆，不改变运维人员操作习惯； 9.支持对在线会话的实时监控和阻断； 10.支持图形化查看用户的运维记录，支持以鱼骨图按照时间倒序自上而下而下展示； 11.支持多种格式导出；支持手动或自动将审计数据异地备份至指定 FTP 服务器；手动或自动清理审计数据，支持自定义审计数据保留周期； 12.支持手动/自动配置数据备份，支持配置数据还原，支持还原至任一备份点；			
19	安全管理区	日志审计	硬件要求： 1.符合标准机柜摆放、冗余电源，内存≥32GB，硬盘≥4TB，配置不少于 6 个千兆电口、4 个千兆光口、2 个万兆光口，配置 4 个千兆多模光模块、2 个万兆多模光模块； 2.日志采集处理均值≥3000EPS；≥50 个日志源许可； 软件要求： 1.支持安全设备、网络设备、中间件、服务器、数据库、操作系统、业务系统等日志数据采集； 2.支持日志转发给第三方系统平台，支持设置多个日志转发 IP 地址，支持转发格式化日志或仅转发原始日志； 3.支持日志原始数据完整存储，支持数据本地集中存储；支持自定义存储位置，支持多盘并行存储，支持自动切换存储位置；支持日志本地备份和 FTP 备份，支持自动备份和手动备份； 4.支持多种方式日志查询，支持历史备份文件导入查询；支持多种查询条件；支持查询结果格式化日志、原始日志导出； 5.支持根据告警规则、告警级别两个维度进行实时告警监视；支持根据告警级别、告警规则类型、规则名称、时间范围、事件名称、设备 IP、源 IP、目的 IP 等方式检索安全事件告警，支持 Excel 等格式导出；支持告警抑制规则设定； 6.支持针对不同类型、不同种类以及不同安全级别的安全事件制定不同的告警方式； 7.支持自定义统计日志数据形成报表，支持统计分析报表以 PDF、word、execl、html 等方式导出，支持实时报表、计划报表； 8.支持以业务角度将日志源进行分组，支持在日志查询时以业务组进行查询，支持在首页拓扑展示时以业务组进行展示； 9.支持基于拓扑图的日志源相关数据信息快速查看；支持通过拓扑下钻查看对应日志源的日志、报表、告警数据。 10.支持将日志源管理权限分配给不同的操作管理员；支持设置非法用户访问控制策略；支持防恶意暴力破解账号与口令功能；	台	1	3年

20	安全管理区	漏洞扫描	硬件要求： 1.冗余电源，内存≥64GB，硬盘≥4TB，配置千兆电口≥6 个、万兆光口≥4 个，含满配光模块； 2.支持无限 IP 扫描，支持无限 Web 域名扫描，支持不少于 100 个资产的并发的基线核查；最大并发任务≥15 个，设备内置漏洞库数量大于 300000 种； 软件要求： 1.支持生成导出专业资产盘点报告（支持 HTML、EXCEL 等格式），报告内容至少包含以下维度：资产汇总（设备分类）、资产分析（区域资产分析、厂商分析、应用服务分析）、资产详情（地址、厂商信息、设备型号、序列号、开放端口及服务、资产上下线详情）； 2.支持基于 A 段、B 段创建并下发资产盘点任务，检测任务可发现目标范围内在线的资产，可检测到在线资产的 IP 地址、 MAC 地址、操作系统、资产类型、设备厂商、设备型号、软件版本，并在报告中展示设备开放的高危端口； 3.具备对高危漏洞的自动化验证功能，平台自动对漏洞进行验证、判断，并可在安全检测报表中体现； 4.支持检测出目标设备连接智能手机热点、通过智能手机 USB 共享网络等违规双网卡共享外联行为； 5.支持安全可视化监测大屏，可 7×24h 监控资产状态及安全风险态势。可展示当前检测任务进度、最新漏洞情况、弱口令统计、高危端口统计、资产类型统计、资产风险分析以及模拟人工渗透等内容； 6.支持自定义资产指纹特征，特征包含资产访问链接、Web 页面特征、操作系统特征、端口特征、资产类型、设备名称、设备厂商等，同时支持资产指纹导出； 7.支持违规外联检测微信公众号告警推送，可对检测到的违规外联信息及时推送，查询及绑定检测局点；微信推送信息包括：IP 地址、MAC 地址、出口 IP、数据来源、初次告警时间、末次告警时间、告警次数等信息； 8.支持对最新发布的高危漏洞及时进行更新，推送至平台，对最新高危漏洞预警进行立即检测； 9.支持标准安全检测、深度安全检测、弱口令检测、高危专项检测、web 安全检测等，检测目标支持以资产盘点目标区域导入或直接文件导入； 10.支持系统安全配置核查功能，能够对主流操作系统、数据库、中间件、网络设备等安全配置项目进行检查； 11.支持联动本次态势分析与安全运营系统，同步现网漏洞信息，支持接收态势分析与安全运营系统下发的漏扫任务，执行相应的扫描策略；	台	1	3年
21	安全管理区	态势分析与安全运营系统	硬件要求： ★冗余电源，cpu 不少于 2 颗 16 核 32 线程，内存≥512G，硬盘：HDD≥48T，SSD≥480G，配置不少于 6 个千兆电口，2 个万兆光口,配置 2 个万兆多模光模块； 为提高系统态势分析的准确性，运营系统须配备独立的流量采集探针；探针关键元器件自主可控，支持国产化 CPU 和国产化操作系统；流量探针支持千兆电口≥2 个，万兆光口≥2 个，扩展槽≥2 个，内存≥64G，硬盘≥4T，冗余电源；支持设置标准模式、增强模式、深度模式、	套	1	3年

			专家模式等流量分析策略，可设置不同策略类型，包括攻击策略、审计策略、采样等级、高级设置 系统实配资产管理节点授权≥600 个； 软件要求： 1.具备各类 DDOS 攻击、僵尸网络、恶意程序攻击、CVE 公开漏洞攻击和 APT 攻击的识别和溯源等基本能力，具备基于攻击过程链、黑客画像和聚合分析等攻击溯源能力， 2.支持综合态势、威胁态势、资产态势、漏洞态势、文件威胁态势、机构威胁态势等大屏展示； 3.支持态势大屏中相关信息下钻跳转到对应的详细页面； 4.支持对相应的攻击特征进行高亮展示；包含所命中规则的详情信息和相对应的解决方案 5.支持漏洞视角进行漏洞的查询展示及处置，至少包括时间、漏洞名称、漏洞编号、漏洞级别、漏洞类型、影响资产数目 6.支持资产视角进行资产的价值分布情况，点击一类资产即可弹框显示该类价值资产列表，至少包括资产名称、资产地址、资产价值、资产风险、资产类型等 7.支持预警规则自定义配置，包括但不限于预警级别、预警对象、详情、是否推送级联平台和客户端； 8.支持基于场景的安全策略响应编排 9.支持从外连地址和受害者的维度展示外连威胁，查看单条外连威胁详情时将外连攻击行为信息进行展示；支持基于 DNS 请求的恶意域名检测，界面可展示外连地址、受害者、DNS 服务器、DNS 域名请求的映射地址，以及 DNS 请求行为的逻辑图呈现；支持恶意域名的 DNS 回连行为分析，界面可展示外连地址、受害者、DNS 域名请求的映射地址，以及回连行为的逻辑图呈现，并可点击跳转展示 DNS 恶意请求行为功能； 10.支持基于 ATT&CK 框架的攻击链分析，内置 14 个入侵阶段的攻击链知识库，入侵阶段包括但不限于：侦察目标、资源开发、初始访问、命令执行、持续控制、权限提升、防御规避、凭据访问、环境观察、横向移动、收集信息、命令控制、窃取数据、侵害破坏；对单次安全事件中涉及的入侵阶段以及使用的攻击技术有明显标注，对使用的攻击技术进行具体战术分析和技术说明展示； 11.支持查看 5G 威胁的日志统计数据，包括威胁级别分布，威胁名称 Top5 和手机号 Top5 统计图以及 5G 威胁事件的列表；支持查看 5G 威胁日志的攻击列表展示，包括手机号、所属机构、所属分组、威胁类型、威胁名称、攻击次数、详情； 12.支持从攻击者和受害者视角分别展示用户威胁列表，至少包括：用户名称、攻击类型、攻击名称、发起或遭受攻击次数等，并支持下钻展示单个用户发起或遭受攻击的列表及详情； 13.支持从用户维度统计威胁信息，至少包括：威胁级别分布、攻击者资产名称 TOP5、受害者资产名称 TOP5、威胁类型 TOP5、威胁名称 TOP5 和威胁趋势等； 14.支持自定义配置的分析条件，配置维度包括：源 IP、			

			源 IP 端口、目的 IP、目的 IP 端口、威胁 id、威胁名称、URL、HTTP 方法、HTTP 域名、HTTP 状态码、DNS 解析域名、TLS 指纹、TLS 版本、SSH 服务端协议版本、SSH 客户端协议版本、SMTP 发件人、文件类型、文件哈希值、恶意文件名称、恶意文件家族等； 15.支持时间轴溯源分析，以时间轴的形式展示攻击者在入侵全过程中各个入侵时间节点中的攻击目标、攻击次数、攻击手段以及攻击阶段，同时提供各攻击手段安全处置建议；展示该攻击事件历史的处置记录； 16.支持多层溯源功能，开启多层溯源后，默认展示两层溯源信息，攻击手段在展示图中消失(改为显示受害者ip)，右侧展示攻击手段 TOP6 及描述信息；支持选择 1-10 层进行溯源，溯源层数不足时默认展示可溯源的最高层数，不同层源使用不同颜色区别展示，并可点击攻击者跳转查看攻击事件详情； 17.支持访问记录分析，可展示本次攻击事件的访问关系，至少包括：访问者、攻击者端口、被访问者、受害者端口、所属机构、日志类型、访问信息和发现时间等，并可查看单次访问的详细情况； 18.支持下载单次攻击事件溯源报告，以及批量删除和批量导出攻击事件列表，攻击事件列表至少包括攻击者 IP、资产名称、资产类型、地理位置，机构名称、受害者 IP、资产名称、资产类型、地理位置，攻击手段，攻击次数，事件级别，影响状态，溯源时间等字段信息； 19.支持利用威胁情报进行关联分析，获取攻击者黑客档案信息，支持用全球和全国地图切换展示黑客地理位分布，用颜色区分每个区域黑客数量；支持展示黑客 TOP 和列表，点击单条黑客能下钻查看详情，详情至少包括黑客名称、地理位置、威胁等级、累计攻击次数、累计攻击目标、常用攻击手段、最近一次攻击目标和攻击手段，以及关联的威胁情报详情和攻击举证图； 20.支持重保分析，对添加过滤重点关注遭受攻击 IP 地址和 IP 地址段；支持威胁类型层面的攻击数量统计和类型过滤，支持添加重点关注攻击类型和过滤，便于统计分析当前遭受攻击的类型情况；支持攻击状态、攻击方向、机构分组、威胁类型、数据来源、检测引擎等多维度的精确检索，可收藏保存查询条件和列表条件过滤，便于快速检索； 21.5G 威胁单条威胁日志展示的主机信息包括攻击者 IP、攻击者端口、受害者 IP、受害者端口、协议、资产的机构分组或非资产的国家名，检测信息包括发现时间、检测引擎、威胁名称、威胁级别、威胁类型、数据来源、特征 ID、解释说明和解决方案、关键字、APN 接入点、特征描述； 22.支持独立的威胁情报检索模块，可根据 IP、域名、文件哈希等进行威胁情报检索功能；支持对检索到的威胁情报进行展示，展示内容包括：级别、类型、时间、评分、关联情报，以及影响的资产范围； 23.支持攻击详情分析，基于攻击者、受害者、受害者端口、数据来源、所属机构、攻击手段、威胁类型、威胁级别、威胁名称、关键字、发现时间等十一个维度进行			

			网络攻击日志检索，可查看本次攻击事件涉及的网络攻击的详细情况，以及下载当前 pcap 包和完整 pcap 包。 24.支持资产探测任务管理，支持任务添加、修改、删除、开始扫描、重新扫描等操作； 25.支持资产管理，支持资产新增、修改、删除，支持自定义资产信息； 26.支持采集管理现网资产（如网络设备、安全设备、服务器等）信息，自动生成网络拓扑，支持手动编辑拓扑；			
22	安全管理区	态势分析与安全运营系统（日志源 License）	软件要求：日志源 License。1 个 License 支持 5 个日志源。	个	9	3 年
23	安全管理区	备份一体机	硬件要求： 1.★符合标准机柜摆放、冗余电源，≥2 颗 CPU（12 核、主频 2.1GHz），≥128GB DDR4 内存，≥2 块 240GB SSD 系统盘，≥8 块 8TB SATA-3 硬盘，≥4 个千兆电口，≥2 个万兆光口，配置 2 个万兆多模光模块； 3.备份速度不低于 18MB/S； 软件要求： 1.内含数据安全管理系统；可保护无数量限制的主机,可实现小时级的数据保护，永久增量备份，基于快照的副本管理，任意备份时间点的数据均可形成多个数据副本，帮助用户实现副本数据的开发测试和查询分析，充分发挥灾备数据的价值;包括配置 IPSAN 盘阵和 NAS 功能授权模块； 2.配置 50T 容量授权。配置合成备份功能模块，无限数量的 linux 版本文件代理模块，无限数量的 linux 版本操作系统代理模块，无限数量的 linux 版本数据库代理模块，无限数量 CAS、FusionSphere 虚拟化备份代理模块，存储功能模块，数据压缩功能模块； 3.持多种国产处理器平台上数据备份；支持多种操作系统下文件或数据库在线备份； 4.支持数据库的增量备份、差异备份、完全备份、永久增量备份等多种备份方式； 5.支持 CDM 快照技术，CDM 快照技术在一体机内实现，不接受外挂存储设备的方式实现快照功能。支持以快照的方式在线查看历史备份数据； 6.支持将备份快照转换为黄金副本，且该副本独立于备份数据，对副本的修改不影响原有备份数据，支持通过 NFS、SMB 等方式共享备份数据副本； 7.支持卷或分区/目录/文件夹/单文件等级别的细粒度备份恢复； 8.支持对主流虚拟化平台的备份恢复； 9.支持虚拟机的挂载恢复功能，在原有虚拟机故障后，无需数据恢复过程，可将任意备份快照点挂载启动。支持单虚拟机粒度挂载，并支持虚拟机挂载后是否自动开机和联网； 10.支持文件的即时挂载恢复功能； 11.支持自定义脚本方式备份恢复应用，完全备份脚本、增量备份脚本、差异备份脚本按需添加脚本文件或脚本	台	1	3 年

			内容即可。备份过程提供文件列表，日志详细过程。			
24	安全管理区	备份一体机（存储扩展）	硬件要求： 包含不小于 8 块 8T SATA-3 硬盘。并配置相应容量 CDM 备份授权。配置 CDM 合成备份功能模块 配置无限数量的 linux 版本文件代理模块 配置无限数量的 linux 版本操作系统代理模块 配置无限数量的 linux 版本数据库代理模块 配置无限数量 CAS、FusionSphere 虚拟化备份代理模块 配置存储功能模块，包括 NAS 配置重复数据删除功能模块，数据压缩功能模块 配置远程复制功能模块	台	1	3年
25	安全管理区	网络审计系统	硬件要求： 1.符合标准机柜摆放、冗余电源，内存≥32GB，硬盘≥4TB，配置不少于 6 个千兆电口、4 个千兆光口、2 个万兆光口，配置 4 个千兆多模光模块、2 个万兆多模光模块； 2.整机吞吐≥5480Mbps，记录事件能力≥50000 条/秒； 软件要求： 1.支持协议内容审计，至少支持 50 种协议；支持文件还原，支持不低于 18 种协议文件还原； 支持网盘外发文件审计，支持对文件进行还原； 软件要求： 2.支持对 HTTP 协议进行内容审计，支持审计访问域名、HTTP 引用页、URL、HTTP 请求类型、HTTP 响应类型、请求文件、请求参数、访问行为、响应码、访问浏览器、服务器、Cookie、源目的 IP 地址、信誉分值等内容； 3.支持 4000 种以上的应用协议行为自动识别与审计记录； 4.支持多种查询方式，支持展示查询条件、事件数、应用协议及任务运行时间；支持导出审计日志； 5.支持审计事件在指定时间段内发送的次数超过设定的阈值时产生对应级别的告警日志； 6.支持发现不同对象相互关联事件之间的隐含关系与规律并产生告警； 7.支持黑 URL、黑 IP、黑域名、黑账号检测等审计策略，支持报文留存； 8.支持按协议或告警类型统计报表，支持 WORD、PDF、OFD、EXCEL、HTML 等格式导出报表； 9.支持通过多种方式进行告警。支持通过多种方式对审计日志、系统日志进行告警通知。 10.支持根据时间或磁盘空间利用状况实现对审计数据的自动备份、自动清理；	台	1	3年
26	安全管理区	数据防泄漏系统（终端 DLP 代理许可）	软件要求：终端 DLP 代理许可（2000 点）	套	1	3年

27	安全管理区	信息数字证书认证系统（智能密码钥匙）	硬件要求： SM4 加/解密速度 19.76Mbps/19.82Mbps；SM2 密钥对生成速率为 36.03 对/秒，加/解密速率为 55.25Kbps/102.25Kbps，签名速率为 93.36 次/秒，验签速率为 50.92 次/秒；SM3 运算速率为 17.67Mbps	套	1000	3年

5.4 安全服务

安全服务				
序号	服务名称	服务内容	单位	数量
1	漏洞扫描服务	漏洞扫描服务	项	4
2	渗透性测试服务	渗透性测试服务	项	2
3	源代码审计服务	源代码审计服务	项	2
4	安全配置基线核查服务	安全配置基线核查服务	项	2
5	在线安全检测	在线安全检测	项	4
6	安全告警服务	安全告警服务	项	4
7	安全加固整改指导	安全加固整改指导	项	1
8	安全策略维护服务	安全策略维护服务	项	4
9	重保 HW	重保 HW	项	5

5.5 其他服务

序号	服务名称	服务内容	单位	数量
1	机房迁建配套	服务器搬迁----原机房 231 台主机设备（详见 4.2.4 现有设备）拆机、运输、设备安装，含系统调试、平台调测等；	项	231
2	集成	系统集成	项	1

6、项目实施要求

投标人应充分考虑满足投标项目的建设要求，提供完整、科学、合理的项目实施与管理方案，在项目进度管理、质量管理、风险管理、人员组织、集成实施等方面做出详细的说明，提出需采取的确保整个项目正常有序实施的措施和办法。具体要求包括但不限于以下内容：

6.1 实施工期要求

本项目要求 180 天内完成建设，其中：

合同签订后 1 个月内完成设备到货及实施准备工作；

4 个月内完成包括设备安装调试、机房迁建、设备集成等；

试运行 1 个月。

6.2 验收

设备到货验收

投标人完成备货后，根据投标设备清单送货至采购人指定地点（松江区）。

货物到达现场后，由投标人提交到货清单，采购人在投标人和第三方监理单位在场情况下共同对货物开箱验收。

投标人应保证货物到达采购人所在地完好无损，如有缺漏、损坏，由中标人负责调换、补齐或赔

偿。
投标人应提供必备的技术资料：1、相关的技术资料（测试报告、产品合格证书、保修卡等）；2、提供主要部件的技术性能参数（列出清单）；3、提供设备保养、维修操作规程；4、提供系统特殊件及配套件的清单、技术参数。
对到货产品与投标产品不一致的，采购人有权拒绝接收。
试运行验收
系统完成集成与测试并上线后进行部署试运行。在系统试运行阶段，投标人应负责完成以下工作内容：
编制《试运行方案》、《试运行阶段培训计划》、《试运行报告》等文档。
试运行期间投标人需不断完善系统功能，提高系统性能。
组织协调用户方、供货方进行系统试运行工作。
试运行期内应完成人员培训工作，并对期间出现的问题进行整改，同时应建立完善的系统运维体系。
完成其它需要在系统试运行阶段的工作。
项目终验
本项目以通过第三方权威机构安全测评和等保测评为终验要求，测评费用由采购人负责，如果测评不通过，投标人应配合后续整改直至通过测评。终验合格后，设备所有权交付采购人投入正式运行，开始计算质保期。
6.3 实施过程要求
1）应采用国家、地方、行业的规范化标准，对项目实施的全过程进行监控和管理。
2）建设期间，项目负责人电话要保持 7*24 小时通畅，如遇到特殊情况需提前通知采购人相关人员。
3）投标人应积极参加采购人组织的项目例会、项目协调会等项目相关会议，并按采购人的要求及时提交各类项目过程报告。项目的重大事件或者管理变更需要得到采购人同意。
4）依据政府有关建设项目的规定，投标人需自行解决进场施工手续，协调相关单位及时解决本项目所需的一切事项；
5）投标人需结合项目工期要求，合理编制施工进度计划表，明确软硬件产品交付节点及交付计划、系统联调联试计划、试运行计划，应在规定时间内，完成项目所有内容的建设，一次性验收合格率 100%；
6）投标人应全面深化实施方案，明确安装调试、集成对接、技术保障、安全管理等内容，实施方案须经采购人、监理方确认后方可实施。
6.4 机房迁建要求
最小化业务中断：
1）投标人需提供详细的业务影响分析和风险评估报告。
2）必须提交分阶段/分批迁移方案，明确每阶段涉及的系统和预计停机窗口（优先非高峰/周末）。
3）关键系统必须提供“零停机”或“接近零停机”迁移方案 (如：使用在线迁移、冗余切换等技术)，明确实现方式。
4）提供清晰的回退/应急计划，确保迁移失败时可快速恢复业务至原状态。
确保数据安全与完整性：
1）明确数据迁移全流程的安全策略（传输加密、访问控制）。
2）提供详细的数据备份与验证方案（迁移前完整备份、迁移后完整性校验方法与工具）。
3）承诺实现数据零丢失、零错误，并明确验收标准和责任。
保障设备安全无损：
1）提供专业的设备拆卸、包装（防静电、防震）、运输、上架安装方案及操作规范。
2）证明具备经验丰富的专业搬运团队和符合要求的运输工具。
3）明确设备损坏的责任界定、赔偿方案。
周密规划与迁建管理：
迁建地址从嘉松南路与南期昌路路口附近一办公楼二楼（无电梯）搬迁至松江区欣玉路与玉树路路口附近一办公楼四楼（有电梯），两址距离 5 公里左右。
1）提供详细的整体迁移实施计划，包含时间表、任务分解、资源计划、第三方协同计划。
2）提交完整的现有机房设备与系统清单（含配置、连接关系）及迁移后拓扑图。

3）明确项目团队结构、关键人员资质与经验。
4）制定详尽的测试方案（迁移前、迁移后、业务验证、性能测试）。
5）明确各方职责 (责任分配矩阵)。
5. 投标人应在报价中充分考虑现场实际条件可能产生的全部费用，采购人将不予接受因投标人对本项目的风险预判不足而提出的任何价格调整及结算要求。
6.5 设备集成要求
1）投标人需根据项目要求（4.2.5 “雪亮工程”区综治分平台网络安全加固结构设计、4.2.6“雪亮工程”区综治物联感知数据接入平台升级建设架构设计）、设备安装规范，对所提供的设备进行综合布线、安装、调试，满足项目验收要求。
2）投标人需在采购人的指导下，负责编制集成方案及相关图表（包括综合布线图、网络拓扑、地址规划等），通过采购人审核后，方可实施。
3）实现对各类安全设备、网络设备及终端的安全信息能力纳管，实现跨域设备动态感知、集中监控、基于统一策略的自动化联动响应与处置，实现统一监管。
4）实现对前端智能门禁、视频抓拍图片等数据接入，兼容现有原有人脸分析算法平台、数据存储平台和运维管理平台，实现统一管理应用。
6.6 质量保障
项目的质量管理是确保项目按时保质的完成预期目标的重要手段，建设方应提供贯穿项目全过程的质量管理办法，确保项目工程的实施质量。
1）提供分阶段的详细质量管理办法。
2）提供系统联调测试及验证步骤方案用以管理系统集成质量。
3）提供项目各个阶段的各类文档管理和版本控制流程说明。
4）提供项目竣工验收后的系统安全运行管理办法。
6.7 项目人员要求
1）投标人需组织具备丰富经验的项目经理和技术人员承担本项目工作。投标人需成立合理的组织机构，建立健全保障项目顺利实施的各项管理制度和质量保证体系，安排各项管理团队参加本项目的建设。
2）投标人应详细列出项目实施团队人员姓名、相关认证资质、项目经验证明、在本单位至少连续工作 6 个月的社保缴纳证明。
3）投标人项目小组人员一旦得到确认，无特殊理由不得随意变动，其中项目经理具有相当项目经验，项目经理未得到采购人同意的情况下不得随意更换。
4）采购人有权根据实施情况要求更换项目经理和实施人员。投标人必须在 10 个工作日内解决，并对此而延误的项目工期负责。

售后服务
质保期
保修期从终验完成之后开始计算，保修时间由投标方投标时明确。本项目产品及系统集成质量保修期不得低于 3 年，软件保修期不得低于 3 年。设备开通后,如发生软件升级及设备升级、扩展等有关情况，投标人应向采购人提供必要的技术资料，并免费提供软件升级。（项目质量保修期不满足招标文件要求的作无效投标处理）
售后服务要求
1）投标人需提供完整的售后服务方案
投标人需提供完整的售后服务方案（①售后服务机构及人员；②响应时间；③零配件供应周期等；④定期安排技术人员针对产品的使用环境、使用频率及更新等进行回访、巡检、维护、保养等方案）；提供不少于 3 人 5*8 小时的驻场运维服务（驻场运维服务地点：松江区）。
2）质保期内，投标人应无偿提供原厂维护维修、免费升级软件等服务，以确保系统运行正常。
投标人应在接到设备故障的通知后，工作时间立即响应，无法远程处理的 1 小时内到现场，2 小时内排除故障。非工作时间 15 分钟内响应，无法远程处理的 2 小时内到现场，4 小时内排除故障。并根据实际需求修复或更换相应的硬件，由此发生的全部费用由投标人负责。
投标人需作出无推诿承诺。即投标人应提供特殊措施，无论由于哪一方产生的 问题而使系统发生不正常情况时，在得到用户方通知后，需立即派工程师到现场，全力协助用户方和其他供应商，使系统尽快恢复正常。

3）在质保期到期前，由投标人工程师和采购人代表进行一次全面检查，任何缺陷需由投标人负责修理，在修理之后，投标人应将缺陷原因、修理内容、完成修理及恢复正常的时间和日期等报告给用户方，报告一式两份。
4）保修期后，投标人应对其提供的设备提供终身技术支持（终身技术支持是指系统过保后，投标公司有能力免费提供终身的技术咨询服务，并以最优惠的价格提供续保服务）。
应急保障
为确保综治业务的正常开展，投标人需提供完备的应急保障方案，至少包括：重大活动安全保障、突发故障快速定位及配合处理、专业技术人员协调支持及应急所需必要专业设备保障等。
技术培训
投标人应为采购人提供多方面、多层次的培训。培训应包括：针对管理人员、操作人员、技术管理和维护人员的培训。
投标人应提供各类的培训资料给采购人，培训资料以电子文档和纸质文 档两种通用格式为主，结合多媒体介绍和演示进行。
培训内容：使管理人员能够了解项目的总体情况、了解如何运转，以及管理过程中如何获取各项信息、数据预警、各类报告等；使操作人员以操作实例和应用场景为主，能够快速上手操作系统；技术管理和维护人员的培训主要从技术层面予以讲解，能够为采购方培养出相对专业的系统运行和维护管理员，保证参与该项目的技术人员充分了解设备的使用，以保证该项目后续的升级与优化。
技术文件
中标人提供的书面技术资料应能满足确保系统正常运行所需的管理、运营及维护有关的全套文件。
中标人提供的技术文件至少应包括：
系统说明文件；
技术手册(安装、测试、操作、维护、故障排除等)；
用户使用手册；
软件资料。
其他要求
投标人应遵守合同文件约定内容的保密要求。如果采购人提供的内容属于保密的，应签订保密协议，且双方均有保密义务。投标人不得利用工作之便外泄资料或做其他用途，否则投标人需承担由此引起的法律责任和赔偿采购人的经济损失。

8、兼容性对接及测评承诺

序号	产品名称	兼容性要求	响应说明
1	物联感知数据接入平台软硬一体机	支持现有前端智能门禁、视频抓拍图片等数据接入，兼容现有原有人脸分析算法平台、数据存储平台和运维管理平台，实现统一管理应用，确保无缝对接。	提供承诺书并加盖公章（格式详见“二、技术响应文件有关表格格式 4、物联感知数据接入平台软硬一体机对接承诺声明函”）
2	态势分析与安全运营系统	支持对各类安全设备、网络设备及终端的安全信息能力纳管，实现跨域设备动态感知、集中监控、基于统一策略的自动化联动响应与处置，实现统一监管。	提供承诺书并加盖公章（格式详见“二、技术响应文件有关表格格式 5、态势分析与安全运营系统兼容性承诺声明函”）
3	测评承诺	承诺配合用户方进行安全测评及等级保护测评工作，并根据测评结果进行整改复测，确保项目通过等级保护三级。	提供承诺书并加盖公章（格式详见“二、技术响应文件有关表格格式 6、测评承诺声明函”）

9、#号项指标汇总

序号	系统名称	产品名称	#重要参数指标	响应说明
1	安全产品购置	下一代防火墙	#支持链路连通性检查功能，支持通过 DNS 解析、ARP 探测、PING 和 BFD 等方式对链路连通性进行探测；	提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告
2			#支持策略匹配分析、策略冗余分析、风险端口分析，提供安全策略优化建议；	提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告
3			#支持对 HTTP/SMTP/POP3/FTP/等协议进行病毒防御；	提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告
4			#当主机故障时，双机切换时不丢包，并可实现双机部署下升级不断网；	提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告
5	综治分平台安全加固	态势分析与安全运营系统	#支持攻击事件时间溯源轴展示匹配上的威胁建模模型信息，攻击手段显示模型名称，事件类型显示威胁建模设置的事件标签，覆盖的攻击阶段显示 威胁建模设置的攻击链，安全处置建议显示 威胁建模设置的处置建议	提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告
6			#支持自定义弱密码字典的增删改查，可用于检测自定义的弱密码，弱密码字典支持对事件和密码进行筛选和检索	提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告
7			#支持自定义攻击事件分析模型，至少包括：事件规则匹配模型、事件统计分析模型、事件关联分析模型；内置 38 种及以上安全事件分析模型，如冰蝎 webshell 通信、利用 Sqlmap 上传 webshell、Acunetix 安全工具扫描、APPSCAN 工具扫描等	提供产品功能界面截图证明并加盖公章或第三方权威机构检测报告

10、“★”汇总表

序号	设备名称	类型	参数规格	证明材料
1	物联感知数据接入平台软硬一体机	PC 服务器	★配置不低于 64G 内存，2 颗高性能国产 CPU，不低于 2.5GHZ（非超频），不少于 2 块 480G 固态硬盘，2 块 4T 硬盘，不少于 12 个硬盘槽位；	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
2	物联感知数	PC 服	★配置不低于 2 块 4T 硬盘，3	1.CPU 提供通过政府有关部门指

	据库	务器	块 480G 硬盘，不低于 128G 内存，不少于 4 个 GE 电口，不低于 2 颗国产化 ARM 架构，32 核，≥2.5GHz	定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
3	视频国标网关（扩容）	PC 服务器	★不少于 2 颗 cpu，主频≥2.5GHz（非超频），不低于 32G 内存，2 块 4TB3.5 寸硬盘，1 块 480GSSD，4 个千兆网口；	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
4	一机一档数据治理平台（扩容）	PC 服务器	★不低于 2 颗 CPU，≥2.5GHZ（非超频），不少于 2 块 4T 硬盘；	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
5	运维平台（升级）	PC 服务器	★不低于 2 颗 CPU，≥2.5GHZ（非超频），不少于 2 块 4T 硬盘；	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
6	终端威胁防御系统（EDR）	机架式服务器	★不少于 1 颗 32 核 CPU，2.0G/64G/240G/2T 企业级*2/标配三合一	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
7	数据防泄漏系统	机架式服务器	★不少于 1 颗 32 核 CPU，2.0G/64G/240G/2T 企业级*2/标配三合一	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
8	信息数字证书认证系统	机架式服务器	★不少于 1 颗 32 核 CPU，2.0G/64G/240G/2T 企业级*2/标配三合一	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图；

				2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
9	终端威胁防御系统（EDR）	操作系统	★操作系统需通过中国信息安全测评中心的安全可靠评测	1.操作系统提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图。
10	数据防泄漏系统	操作系统	★操作系统需通过中国信息安全测评中心的安全可靠评测	1.操作系统提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图。
11	信息数字证书认证系统	数据库	★数据库需通过中国信息安全测评中心的安全可靠评测	1.数据库提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图。
12	信息数字证书认证系统	操作系统	★操作系统需通过中国信息安全测评中心的安全可靠评测	1.操作系统提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图。
13	统一安全接入网关系统（管理平台）	安全隔离与信息交换产品	★CPU≥32 核，内存≥256G，硬盘：HDD≥36T，SSD≥480G；2.配置双电源，千兆电口≥6 个、千兆光口≥4 个，扩展槽≥3 个，支持终端接入数≥100000 个；	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
14	态势分析与安全运营系统	安全管理平台产品	★冗余电源，cpu 不少于 2 颗 16 核 32 线程，内存≥512G，硬盘：HDD≥48T，SSD≥480G，配置不少于 6 个千兆电口，2 个万兆光口,配置 2 个万兆多模光模块；	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。
15	备份一体机	数据安全	★符合标准机柜摆放、冗余电源，≥2 颗 CPU（12 核、主频 2.1GHz），≥128GB DDR4 内存，≥2 块 240GB SSD 系统盘，≥8 块 8TB SATA-3 硬盘，≥4 个千兆电口，≥2 个万兆光口，配置 2 个万兆多模光模块；	1.CPU 提供通过政府有关部门指定的中国信息安全测评中心和国家保密科技测评中心网站查看安全可靠测评结果的截图； 2.提供所投产品彩页或产品技术白皮书（或产品说明书）或产品官网网站链接及网站产品说明的截图等详细技术资料。

注：物联感知数据接入平台软硬一体机、态势分析与安全运营系统为本项目核心产品。