## 采购包1采购需求

### 1、项目名称

海南智慧法院综合办公办案平台（一期）项目（采购包1）。

### 1.1总体技术要求

#### 1.1.1建设目标

总体目标是结合海南省自贸港建设的司法服务要求，坚持以业务需求为导向，以数据为牵引，加强信息化顶层设计，整合现有资源，强化深度应用，充分运用人工智能、大数据、区块链等先进技术，按照最高人民法院“三云五网”总体框架，构建海南法院信息化整体布局，紧紧围绕“一个核心”，深化完善智慧服务、智慧审判、智慧执行、智慧管理四类智能服务平台、输出多层次、多种类业务应用，形成面向服务人民群众、服务司法审判执行、服务司法管理、服务廉洁司法和运维保障的一体化支撑能力，努力实现全面覆盖、移动互联、跨界融合、深度应用、透明便民、安全可控的信息化建设目标，大力推进海南省法院信息化建设转型升级，同时为后续海南智慧法院平台打造具有自贸特色、符合智慧法院七大趋势的“一核、两翼、四智”的海南特色智慧法院版提供能力基础，为全省法院现代化提供坚实的信息科技保障，助力海南自由贸易港”建设，创建中国特色社会主义实践范例。

项目的建设可提高全省法院办公人员的办事效率，提升民众对司法的认可度。

#### 1.1.2标准与规范

主要标准与规范不限于以下标准：

1. 《信息技术　软件重用　重用库互操作性的数据模型　基本互操作性数据模型》（GB/T26223-2010）；
2. 《信息技术　软件生存周期过程　重用过程》（GB/T26224-2010）；
3. 《计算机软件产品开发文件编辑指南》(GB8567－88)；
4. 《计算机软件开发规范》(GB8566－88)；
5. 《计算机软件需求说明编制指南》（GB/T9385-1988）；
6. 《网络安全等级保护实施指南》（GB/T25058-2019）；
7. 《网络安全等级保护基本要求》（GB/T22239-2019）；
8. 《网络安全等级保护测评要求》（GB/T28448-2019）；
9. 《网络安全等级保护测评过程指南》（GB/T28449-2018）；
10. 《信息系统安全管理要求》（GB/T20269-2006）；
11. 《信息安全事件管理第1部分：事件管理原理》（GB/T20985.1-2017）；
12. 《网络安全事件分类分级指南》（GB/Z20986-2007）；
13. 《信息系统密码应用基本要求》（GB/T39786-2021）；
14. 《信息系统密码应用评测要求》；
15. 《信息系统密码应用测评过程指南》；
16. 《商用密码应用安全性评估量化评估规则》；
17. 《信息系统密码应用高风险判定指引》；
18. 《信息技术服务运行维护第1部分：通用要求》（GB/T 28827.1-2024）；
19. 《信息技术服务运行维护第2部分：交付规范》（GB/T 28827.2-2024）；
20. 《信息技术服务运行维护第3部分：应急响应规范》（GB/T 28827.3-2024）；
21. 《信息技术服务运行维护第6部分：应用系统服务要求》（GB/T28827.6-2019）；
22. 智能庭审应用技术要求FYB\_T\_52038-2020；
23. 科技法庭信息化建设规范FYB\_T\_54001-2021；
24. 《视频安防监控系统工程设计规范》（GB50395-2007）；
25. 《视频安防监控系统技术要求》（GA/T367-2001）；
26. FYB\_T\_54009-2020-法院统一DNS系统建设技术规范。

#### 1.1.3建设需求

##### 1.1.3.1业务需求

###### 1.1.3.1.1海南法院智慧审判业务需求

1.1.3.1.1.1证券纠纷代表人诉讼服务系统需求

证券类纠纷案件数量众多、社会影响面广。投资者损失核算相关事实查明和法律适用，是证券类案件，尤其是证券虚假陈述责任纠纷的审理难点和重点。从过去三年全国证券虚假陈述责任纠纷看，损失计算相关的高发争议焦点包括“案件的实施日、揭露日、基准日如何确定以及基准价的计算方法”、“涉案虚假陈述行为与原告主张的投资损失之间是否存在因果关系”、“原告的损失如何计算，如何计算系统风险和其他应扣除风险占比”等。系统具体功能如下：

证券纠纷代表人诉讼服务系统（当事人端）：用户登录、代表人诉讼在线平台首页、公示公告信息、权利登记、代表人推选、调解草案异议、提起上诉、放弃上诉、退出诉讼、消息提醒。

证券纠纷代表人诉讼服务系统（法官端）：用户登录、启用代表人诉讼、公告公示、登记信息审核、代表人推选。

第三方接口：对接法院统一身份认证系统接口、对接诉讼服务平台接口、对接审判系统接口、对接短信平台接口。

1.1.3.1.1.2 CA及密评需求

结合海南高院CA及密评要求，需要具备PC端用户身份鉴别、重要数据安全传输的机密性及完整性、访问控制信息与敏感标记完整性、应用数据抗抵赖、应用系统日志记录完整性等功能。

###### 1.1.3.1.2海南法院智慧诉服业务需求

1.1.3.1.2.1 CA及密评需求

结合海南高院CA及密评要求，需要具备PC端用户身份鉴别、重要数据安全传输的机密性及完整性、访问控制信息与敏感标记完整性、应用数据抗抵赖、应用系统日志记录完整性等功能。

###### 1.1.3.1.3海南法院智慧执行业务需求

1.1.3.1.3.1 CA及密评需求

结合海南高院CA及密评要求，需要具备PC端用户身份鉴别、重要数据安全传输的机密性及完整性、访问控制信息与敏感标记完整性、应用数据抗抵赖、应用系统日志记录完整性等功能。

###### 1.1.3.1.4海南智慧管理业务需求分析

1.1.3.1.4.1智慧教学管理系统

建设打造适用于海南本地的集法院干警教育培训学习应用和教务教学管理等日常事务和功能为一体、前后台相融合的综合性法官教育培训与智慧教学管理平台，技术层面实现一站式在线单点登录并支持内外网数据交互，并打造与平台相应功能适配的小程序系统，为海南省法院系统干警提供一站式、全方位的教育培训、学习提升、事务管理应用平台与服务。通过开发精品课程体系、开展专题培训项目、搭建综合服务平台、整合优质信息资源等多项举措，积极构建海南省法院教育培训工作发展新格局。

一、海南法官教育培训管理后台

海南法官教育培训管理后台，充分利用现代科技手段赋能服务培训管理工作，综合管理后台集教务教学管理、学员管理、资源管理、信息管理与行政事务管理于一身，实现法官学院各项教务教学管理工作信息资源数字化、协同工作流程化、决策支持智能化，面授培训、网络培训与日常事务管理融合应用，实现面授培训与网络培训统一管理，实现学员管理、在线报名管理、培训班次管理、师资管理、课程管理、课程评价管理、线上学习与线下学习综合评定、数据统计分析、管理员分级赋权管理。

基于教育培训管理后台后台：

1.建设以线上课程内容、线下课件管理、课程信息编辑处理、师资管理为主要功能的后台资源管理中心模块：

2.建设以学员信息管理、法院基础信息管理、管理员分权赋权管理为主要功能的后台用户系统管理模块：

3.建设以培训事务性管理、培训班次管理、培训招生、培训考试、证书管理、课程评估管理、资料归档管理、统计分析管理为主要功能的教务综合管理平台模块。

4.素材库模块管理：支持将培训基础素材包含视频、文档、图片、音频、scorm\html压缩包进行统一的建设管理，并支持通过资源素材类型进行快速的筛选查看，同时对素材内容可锁定，以防止误操造成的资源损失。

5、课程管理模块：管理员可通过该模块新增\创建线上课程，支持在课程章节课时中，通过本地上传、素材库添加、在线编辑、链接添加形式，创建课程的具体内容，课程内容在创建完成后可设置课时素材的下载权限，同时对于课程的播放可设置快进、防止挂机、水印等播放配置，并设置课程的有效时间，完成创建后发布课程，学员即可参与课程学习。

二、智慧教学管理子系统

建设智慧教学管理子系统，及时发布各类各批培训班次及课程信息、学术活动、发布培训的动态信息、课程推荐、热点资讯等，提供相应政策资讯及法院系统内部教育培训工作相关规范文件的查询；支持学员通过首页登录平台、报名参训、在线培训学习、在线考试及学员个人资料修改调整、信息查询，培训资料的查询，了解培训班次和课程，下载课程附件和相关教辅材料等，以及与后台管理功能相匹配的内容发布管理、公告管理、调查问卷管理等功能。通过搭建学员个人中心，学员可通过个人中心对个人资料信息编辑补充修改，查询了解个人参与的培训班、已选课程、学习记录等情况以及参与的调查问卷、课程与师资相应评价，最大程度满足学员自主学习和其他个性化需求及功能体验。

三、海南法官教育培训移动学习应用平台（小程序）

依托微信小程序打造新型移动学习平台，为海南法院系统干警在日常最熟悉、当前最普及的智能手机上提供各类便捷、高效的学习服务，方便海南法院干警利用非工作时间、碎片化时间随时随地参与学习,最大程度的满足学员随身学习需求。

移动端小程序学习应用平台主要功能包括外网登录、在线报名、在线学习、线下现场签到、参与考试、教学评估、课程评价等功能模块，优先实现通过小程序平台培训报名、线下现场签到、考勤打卡、课程评价、师资评价等基础功能。

四、海南法官教育培训平台环境资源与信息共享

结合具体情况，积极推动网络教育培训平台外网化建设，可通过公有云搭建网络教育培训平台架构及所有功能，通过技术手段实现外网与法院专网双网运行，积极推进外网与工作网和法院专网同步相关学习、统计数据、小程序平台技术支撑等。

后续需与法院专网相关应用系统进行业务协同，通过法院专网赋权和接口开发调用，打通接入法院用户管理统一用户平台，实现用户统一平台一站式登录，支持用户一次认证登录即可全网内通行使用。

###### 1.1.3.1.5信息基础设施支撑系统业务需求

1.1.3.1.5.1科技法庭升级改造-智慧法庭业务需求

一、为法官提供辅助阅卷的需求

在案件审理的过程中，法官需要对卷宗进行重复、反复的研判，在传统的阅卷过程中，法官需要不断翻阅卷宗，既降低了办案效率，同时又容易导致案件信息的不同步。因此，法官辅助阅卷需要可以对卷宗文件进行即时同步，同时，系统还应可以将庭审提纲进行导入，方便法官快速熟悉案件详情，以保证庭审的高效性。

二、庭审提纲智能推送的需求

不同的审判程序和案件类型，法官应制定不同的庭审提纲。法官在庭前阅卷时，针对该案件的审理过程，整理出针对该案件庭审提纲，以往的做法是手工编写，或根据法官的经验在庭审中自由发挥，可能导致庭审环节的不完整。所以需要建立一套机制，在庭前法官总结的庭审提纲能够顺利应用到庭审的环节中，使法官能够按照规范的庭审提纲进行庭审环节的掌控，避免出现庭审环节的遗漏。针对部分一审的简易程序案件，系统需能够智能提炼出庭审提纲以在庭前阅卷和庭审过程中自动推送给法官。

三、争议焦点辅助归纳的需求

不同的案件类型和案件性质，都有不同的争议焦点出现。对于争议焦点的归纳，法官需在庭前阅卷阶段，根据诉讼双方提供的证据材料，整理出该案件的争议焦点，以便在庭审中重点关注和审理，以保证庭审的高效性。需要实现在庭前法官手工编写争议焦点，在庭审过程中自动推送到法官的应用端中。系统需能同步归纳出案件的争议焦点以在庭审过程中自动推送给法官，以使法官掌控庭审环节。

四、庭审笔录辅助制作的需求

在立案材料生成电子卷宗后，案件要素在语义分析中已经确定。庭审时，书记员庭审应用系统即可根据案件类型匹配相应的笔录模板，同时生成笔录纲要，在庭审常规流程的各个阶段插入固定内容笔录。例如，笔录首先通过要素回填和案件排期的内容，在笔录中列出案由、审判场所、审判人员等内容，对宣读法庭纪律、说明开庭程序、告知当事人权利与义务等内容在相应的阶段辅助插入笔录中，对核实当事人及代理人身份则进行信息回填，然后书记员只需记录核实过程中的双方发言。同样，在庭审的各个阶段中，凡是已有的信息内容都尽可能的以辅助操作的方式填写到相应的位置。

书记员庭审笔录辅助功能之外，原有的书记员开庭各类操控、开庭录像、休庭关闭、证据展示设备操控等各类原有功能都需要继续保留在同一系统界面内，不需要单独开设专门的软件窗口，是书记员的工作保持延续性。

五、庭审过程质证的需求

在庭审调查、质证阶段，能够自动推送当事人所提及的证据图片，便于法官把握证据内容。

通过语音识别对当事人口述内容中所提及的证据名称的识别结果，自动在电子卷宗中查找对应的电子证据材料并显示给法官。

对电子证据的推送展示不应只是法官可以看到，而是能够同步显示在双方当事人的应用系统上，体现司法公正；同时，电子证据还应同步显示在旁听人员大屏幕显示设备上。

法官可以调出电子卷宗中双方的其他电子证据内容，与当事人提及推送的电子证据进行同屏比对，确定双方证据材料的使用方式。

六、向法官推送相关法律条文及相关案例的需求

根据立案材料电子卷宗提取要素、庭审笔录中新增要素以及争议焦点的梳理，向法官提供相关法律法规（包括国家法律、最高院释法、地方法规）的参考支持和与本案相似度从高到低的类似案例支持，辅助法官做出达到“类案同判”结果的裁决，维护司法统一性的要求。

在智慧法庭的法官客户端中，集成无缝获取相关法律库以及相关案例库的途径，并自动智能化筛选，同时自动梳理争议焦点也能便于法官对案件判决的考量。

七、对办案助手的需求

在法院案件审理的过程中，根据案件类型的不同，需要法官对与案件相关的费用进行计算，例如在民事案件中需要对原告的赔偿损失进行计算，刑事案件中附加民事诉讼费用的计算等。因此，需要系统提供对费用的辅助计算功能，法官应可以根据不同案件类型选择不同的计算方式，同时具备法律法规做参考依据。

八、文书智能辅助制作的需求

法院对于法律文书制作有严格的要求，包括格式、内容均要符合最高人民法院出具的相关规范执行。需具备满足最高人民法院对于法律文书的相关模版，且需提供准确的卷宗辅助信息，提供给法官予以在编写法律文书时进行复制，以减轻法官的编写压力。对于能够自动生成的部分，需严格按照格式要求自动生成包括文书首部、当事人基本信息部分、案件由来及审理经过、诉称、辩称以及文书尾部，文书的审理查明、本院认为、裁判结果等内容需由承办人根据卷宗等相关内容进行手工编写。

九、对裁判结果预估的需求

法官在对案件进行仔细研究分析后，在庭审的最后阶段需要对案件进行审理终结。而为了保证审判结果的准确性，需要系统为法官的判决结果提供参考。系统需可以关联到本地、本省、全国的类似案件的判决结果，对当前案件进行风险预警与案情分析，可以有效提高案件原被告双方的满意度，同时体现司法的公正。

十、电子签名和捺印的需求

随着智慧法庭的深入应用建设，对于传统的对笔录打印后进行签名，再扫描到法院应用系统中的应用流程，已不能满足高效和业务的使用。尤其在远程开庭、远程提讯或远程作证的应用中，当事人或证人的签字归档是个比较棘手的问题，为解决存档的笔录文件、证人证言以及其他法律文书卷宗归档的一致，需统一使用电子签名和捺印系统，以解决当庭、远程签字的需求。

十一、对证人保护的需求

为确保案件审判的公正，在案件审理过程中，往往需要目击证人或者了解案情的相关人员出庭作证，而针对重大案件如缉毒案件等，证人的出庭很有可能导致危险情况的出现，法院由于经费等原因，难以立即组建若干机构专门进行证人保护的工作，因此对证人的保护也变得迫在眉睫。

为保证证人作证时对案件进展的实时把握，系统需要支持对庭审音视频、笔录文件的实时接收与显示；需要提供对证人的保护措施，如对其图像进行马赛克处理、对声音进行变声处理等，同时，当证人作证完毕之后，可以对其证词证言进行及时打印，证人确认证人证言后，即可离开法庭，无需等待庭审结束，多方面保障证人的安全。

十二、旁听辅助功能需求

在前期科技法庭建设中，对于配置的大屏幕显示设备，原来一般设计为显示法庭的现场画面，根据法庭信息化的新发展和智慧法庭的新需求，在庭审过程的不同庭审阶段向旁听人员提供相应阶段性解释，如当前案件的审理信息，在庭前准备阶段，显示法庭纪律、本庭审判人员信息，开庭身份验证时显示当事人的诉讼地位及姓名、性别等身份信息，显示告知当事人的庭审中权利和义务，法庭调查阶段说明本阶段当事人该做的事情，在法庭调查、法庭辩论、宣判结果三个阶段中智能推送由智能语音识别出庭审发言中提及的法律法规详细内容。这类应用可使旁听人员对案件审理的过程有完善的了解，也可达到以案释法的作用。

1.1.3.1.5.2 DNS建设需求

提供给全省31家法院使用，未来5-10年逐年增加。本次采购的DNS用于海南省法院专网类业务的解析，一方面可实现与最高人民法院DNS系统的数据无缝对接、交互与管理，符合《FYB\_T\_54006-2018-法院专网域名编码规范》和《FYB\_T\_54009-2020-法院统一DNS系统建设及接入规范》等建设智能、安全、合规、稳定的法院专网域名服务系统要求；另一方面可全面规避当前采用通用服务器硬件+WindowsDNS软件方式部署的非专业DNS系统带来的性能低下、智能解析功能不足、安全性差漏洞多、稳定性差无高可靠冗余机制、缺乏统一集中管理且无法实现基于角色的管理功能及权限分配等问题。

###### 1.1.3.1.6接口对接需求分析

1、海南法院智慧审判：对接法院统一身份认证系统接口、对接诉讼服务平台接口、对接审判系统接口、对接短信平台接口。

2、互联网庭审管理系统：需要与省政务短信平台对接，采用政务短信平台向当事人提供短信消息通知或身份认证码确认服务。

##### 1.1.3.2业务协同需求

如有，则根据实际业务情况协同。

##### 1.1.3.3信息交换与共享需求

本次项目建设将进一步丰富完善我省法院智慧审判、智慧诉服、智慧管理等业务系统应用数据，将根据政务信息归集共享要求与进行数据归集和共享开放，其他部委根据各自需求，自行向大数据局申请。

海南高院作为数据共享方通过共享交换平台，向法院专网、互联网、外部专网的数据接收方提供数据共享。数据接收方可以是各级法院专网应用系统、互联网应用系统、外部单位应用系统。

根据最高人民法院相关的信息接口要求，智慧庭审的后台管理系统必须能够取得案件信息管理系统相关庭审案件信息数据，实现案件信息管理系统与智慧法庭的数据同步，同时具备由案件信息管理系统中调取智慧庭审系统庭审音视频信息直播和点播的能力。

##### 1.1.3.4信息基础设施需求

###### 1.1.3.4.1机房及配套设施需求

目前机房设备总功率为85180W，本项目需要对在主楼负一楼已经老旧、及损坏的2012年采购的2台80KVAUPS主机，和58节12V/200AH电池进行更换，且根据本次新建内容进行扩容，在满足目前需求的同时，为以后的业务发展预留出可扩容的资源。

###### 1.1.3.4.2存储备份需求

视频监控与门禁系统：本次需根据新建视频监控设备与门禁系统，采购相关存储设备，按存储时间不小于3个月进行配置。

###### 1.1.3.4.3网络建设需求

根据海南省高级人民法院的系统建设情况，整体网络划分为专享云业务区、专享云安全边界区、法院专网接入区、安防视频接入区、核心交换区、办公终端区、专网业务区、安全管理区、安全隔交换平台区、公钥密码基础设施区、信任服务区、外部区（包含互联网网系、外部专网网系、电子政务外网/移动互联网）等重要建设安全区域。

因为在法院专网、政务外网、互联网等现有网络中部分网络设备已经老旧，已超过使用年限，且无法满足国产化建设需求，所以本项目需要根据原网络架构更换老旧的网络设备。

###### 1.1.3.4.4云服务需求

本项目所需服务器、存储、系统软件等资源均可向政务云申请。

###### 1.1.3.4.5基础硬件设备需求

1、涉及的服务器主要采用申请政务云的方式获取。

2、安防监控系统的门禁、摄像头、报警器等部署于高院大楼内部。

3、法院专网的安全设备部署于政务云法院专区机柜内。

4、域名解析服务器建设需求：海南法院当前仍有大量办公、业务系统使用IP地址形式进行部署，IP与业务系统紧耦合，IP地址冗长且不易记忆，日常访问效率低。另外当系统由于升级、变更等原因需要变更IP地址时，需要进行再次通知，影响各部门的访问效率和信息资源共享。

##### 1.1.3.5性能和其他需求

###### 1.1.3.5.1基本需求

1）先进性：选用先进、成熟、主流的技术搭建可升级、可扩展、可兼容的系统应用平台，构建数字化、网络化和智能化的通讯系统。

2）可靠性：系统应支持对关键设备、关键数据、关键程序模块采取备份、冗余措施。支持集群技术和负载均衡技术，支持双机热备功能；软件采用模块化、分层隔离的设计思想，充分确保系统的高可靠性和稳定性。

确保系统具有高度的安全性，不易感染软件病毒；

对工作环境要求较低，环境适应能力要强；

系统设备安装使用简单，无需专业人员维护；

3）开放性：系统的建设在符合国家和行业相关标准要求的基础上，采用业界主流的硬件平台、操作系统平台、数据库平台以及标准的协议，保证与省高院数据信息共享平台对接和其他业务系统的信息共享。

4）实用性：系统的建设必须突出应用，选择实用性强的系列产品，采用模块化结构设计，既可满足当前的需要又可为今后系统发展扩展留有余地；系统客户界面友好，安装、操作、使用、维护简便。

5）安全性：应制定严密的安全管理机制，确保信息安全、系统安全、数据库安全和设备安全。

6）经济性：在确保实用性、可靠性、先进性、开放性和安全性的前提下，注重建设的成本和投入的阶段性，既能满足实际需要，又可尽量降低费用，以技术建设与应用机制的协调发展，确保系统效益。

###### 1.1.3.5.2接口需求

应采用模块化部署结构，可根据实际需要通过业务模块的增加来实现系统功能的扩展和系统容量的扩容，为今后系统的升级、扩建留有余地。

在产品的容量与处理能力等设计时应留有冗余量，应预留与其它业务系统或平台的信息互联接口，可对外提供标准的开放接口，方便扩展其它深度应用。本项目需实现信息交换内容包括：

1、海南法院智慧审判：对接法院统一身份认证系统接口、对接电子诉讼平台接口、对接审判系统接口、对接短信平台接口。

2、互联网庭审管理系统：需要与省政务短信平台对接，采用政务短信平台向当事人提供短信消息通知或身份认证码确认服务。

###### 1.1.3.5.3软件系统性能需求

软件系统必须有很强的健壮性，不能因为大量用户并发使用而造成系统崩溃。

采用合理的数据库结构和查询算法，以保证查询的响应速度不随记录数的增长显著下降。

（1）系统建成后，业务系统性能须不低于以下性能要求：

平均响应时间：100并发用户小于3秒；300并发用户小于5秒；500以上并发用户小于7秒。

CPU平均使用率小于80%；

数据库缓存命中率大于90%。

具体功能应满足的性能要求如下表所示：

系统功能划分及响应时间要求表

| 功能划分 | 响应时间要求 |
| --- | --- |
| 数据提取 | 可以按照一定格式，自动提取信息，并进行数据完整性、合法性检查；处理时间<5秒 |
| 数据保存 | 向数据库中更新的速度<5秒 |
| 数据关联 | 能够检查出重复的关联。建立关联的速度不大于5秒 |
| 数据信息编辑 | 对于关键字以外的字段能够修改。并检查数据的完整性、数值的合理性，有相似性和重复性检查；响应时间在5秒内 |
| 查询检索 | 简单查询响应速度<3秒；复杂和组合查询响应速度<30秒；能够对相关文件进行检索、模糊查询；查询结果可以按照一定原则进行排序、筛选、保存；查询结果可以显示为图形或图表，可以输出到通用的办公处理软件中。 |
| 汇总 | 简单汇总处理时间不大于10秒钟；固定制表处理时间不大于5秒 |
| 制表 | 组合制表处理时间不大于10秒，并有进度显示；动态、复杂制表处理时间不大于30秒，并有进度显示；报表格式，应当符合中国人的习惯。 |
| 数据分析 | 数据分析预测的处理时间一般在10秒以内，复杂情况处理时间不大于30秒 |
| 备份恢复 | 应用系统和数据库系统等的备份、恢复定期自动进行，也可以人工进行；提供数据库和表两级备份恢复。处理时间最好不大于30分钟 |
| 权限管理 | 根据用户类别，划分角色和权限。处理时间不大于5秒钟 |
| 系统日志 | 系统运行日志应记录对系统数据的修改、访问日志；可以定期清理；数据库应当有日志文件，以做备份恢复。处理时间不大于5分钟 |
| 接口管理 | 业务系统之间的数据交换时间不大于1分钟 |

###### 1.1.3.5.4网络性能需求

1. 法院专网

法院专网主要供全省法院五千多名干警、聘用人员及运维人员使用，承载电子卷宗、视频会议、庭审等业务。

（1）抖动要求

语音类型业务：流量随时间均匀分布，流量不大，对于抖动敏感。语音应用网络抖动标准应小于10ms。视频类型业务：突发流量大，长时间占用带宽，对于抖动敏感。视频应用网络抖动标准应小于50ms。

（2）时延要求

语音类型业务：流量随时间均匀分布，流量不大，对时延敏感。语音应用网络延迟标准应小于120ms。视频类型业务：突发流量大，长时间占用带宽，对时延敏感。视频应用网络延迟标准应小于150ms。

（3）丢包率要求

语音类型业务：流量随时间均匀分布，流量不大，对数据丢包敏感；语音应用网络丢包率标准应小于1%。视频类型业务：突发流量大，长时间占用带宽，对数据丢包敏感；视频应用网络丢包率标准应小于等于0.05%。

（4）网络通断要求

端口、设备以及线路故障率应满足以下要求：

——端口故障率≤5次/年；

——设备故障率≤5次/年；

——线路故障率≤5次/年。

（5）楼层接入需求

接入交换机在整体网络建设中主要用于用户接入，对于接入交换机的设计主要考虑支持高密度的接入、接入总带宽与上行带宽存在收敛比、线速两种模式，同时必须考虑接入的安全性，选用的交换机必须支持防ARP，IP+MAC绑定等安全特性，保证接入安全。

需要满足全院五百人同时访问，实现办公办案需求，实现千兆到桌面，规划5年以上有网络扩容的准备。

1. 核心交换需求

承受全省法院共有30家法院同时发起网络访问，实现办公办案需求，规划5年以上有网络扩容的准备。

1. 监控交换需求

需满足全院280个监控接入需求，最低满足400万像素接入。

1. 互联网

（1）抖动要求

语音类型业务：流量随时间均匀分布，流量不大，对于抖动敏感。语音应用网络抖动标准应小于10ms。视频类型业务：突发流量大，长时间占用带宽，对于抖动敏感。视频应用网络抖动标准应小于50ms。

（2）时延要求

语音类型业务：流量随时间均匀分布，流量不大，对时延敏感。语音应用网络延迟标准应小于120ms。视频类型业务：突发流量大，长时间占用带宽，对时延敏感。视频应用网络延迟标准应小于150ms。

（3）丢包率要求

语音类型业务：流量随时间均匀分布，流量不大，对数据丢包敏感；语音应用网络丢包率标准应小于1%。视频类型业务：突发流量大，长时间占用带宽，对数据丢包敏感；视频应用网络丢包率标准应小于等于0.05%。

（4）网络通断要求

端口、设备以及线路故障率应满足以下要求：

——端口故障率≤5次/年；

——设备故障率≤5次/年；

——线路故障率≤5次/年。

（5）楼层接入需求

接入交换机在整体网络建设中主要用于用户接入，选用的交换机必须支持防ARP，IP+MAC绑定等安全特性，保证接入安全。

需要满足全院五百人同时访问，规划5年以上有网络扩容的准备。

（6）汇聚接入需求

需要满足全院五百人同时访问互联网，规划5年以上有网络扩容的准备。

##### 1.1.3.6网络安全建设需求

###### 1.1.3.6.1安全技术保障体系需求

1.1.3.6.1.1安全物理环境

海南省高级人民法院的数据机房建设依据我国《数据中心设计规范》(GB50174-2017)的数据中心要求，满足B类机房防护要求。本次项目不涉及机房改造。

1.1.3.6.1.2安全通信网络

通信网络重点关注的安全问题主要涉及网络架构安全方面。保障通信网络安全的具体措施包括对网络区域的合理划分、对重要网络区域的可靠隔离、对网络设备性能和网络带宽的有效保障、对通信链路和节点设备的硬件冗余。

1.1.3.6.1.3安全区域边界

依据等级保护要求第三级中（安全区域边界）相关控制项，结合安全区域边界对于区域边界访问控制、区域边界包过滤、区域边界安全审计、区域边界完整性保护等安全要求，安全区域边界防护建设主要通过网络架构、安全区域划分，基于地址、协议、服务端口的访问控制策略等安全机制来实现区域边界的综合安全防护。

（1）边界入侵攻击防范

为了满足等级保护中“入侵防范”的安全功能需求，能够提供实时的网络监测、分析数据包内容、签名匹配、异常检测等，实现对异常行为和网络攻击的有效防御和响应。需要在法院专网-专享云接入区和法院专网-网络边界接入区部署入侵防御系统，两个区域分别部署两台设备，在主备模式下，实现负载均衡，同时提供冗余，增强可靠性，确保高可用性，保证网络边界的安全防护不间断。

（2）边界恶意代码防范

为了满足等级保护中“恶意代码防范”的安全功能需求，在部署的入侵防御系统中启用防病毒功能模块，并定期更新升级病毒特征库，能够对恶意代码进行识别和防御，有效防止病毒在法院专网中传播，保护网络安全。

1.1.3.6.1.4安全计算环境

依据等级保护要求第三级中（设备和计算安全、应用和数据安全）等相关安全控制项，结合安全计算环境对于用户身份鉴别、自主与标记访问控制、系统安全审计、安全接入连接、安全配置检查等技术要求，安全计算环境防护建设主要通过身份鉴别与权限管理、网络管理监控、安全配置核查、安全审计，数据防泄漏、重要节点设备冗余备份，以及系统和应用自身安全控制等多种安全机制实现。

（1）安全审计

为了满足等级保护中“安全审计”的安全功能需求，应对数据库的流量、用户行为等进行审计；审计记录应包括：事件的日期和时间、用户、事件类型、事件是否成功及其他与审计相关的信息；应能够根据记录数据进行分析，并生成审计报表；最后应对审计记录进行保护，避免受到未预期的删除、修改或覆盖等；需要在法院专网服务器区部署数据库审计系统，对法院专网服务器区数据库操作进行监测、记录和分析，保障数据的安全性和完整性。

1.1.3.6.1.5安全隔离交换平台区

目前外部专网、电子政务外网和互联网等采用独立链路接入平台，不应混合接入。互联网、监狱管理局专网采用专线方式与接入平台进行安全接入，其隔离区和接入区建设按照等级保护三级加以建设，对现有2条隔离交换平台进行等保3级（边界安全）网络加固。具体需求如下：

一、互联网安全隔离交换平台（数据&服务请求）

边界防护：为了抵御外部威胁，确保WEB服务的安全性和可用性，在安全隔离交换区边界部署WEB应用防火墙，并配置相关的访问控制策略，定期升级特征库，实现恶意特征识别与防护、常见攻击检测与阻断、内容过滤和应用层DDoS防护等。

二、减刑假释业务安全隔离交换平台（数据）

边界防护：在安全隔离交换区边界部署下一代防火墙，进行隔离和访问控制，严格控制外部网络对业务系统信息资源的访问，确保法院专网安全。

入侵防范：在下一代防火墙中启用入侵防御功能模块，对异常行为和网络攻击进行有效防御和响应。

恶意代码防范：在下一代防火墙中启用防病毒功能模块，对恶意代码进行识别和防御。

###### 1.1.3.6.2安全管理保障体系需求

为了保障海南省高级人民法院网络的长期健康运营，需要建立规范的信息安全管理体系。依据《GBT22239-2019信息安全技术网络安全等级保护基本要求》，海南省高级人民法院网络在管理制度、管理机构、管理人员、建设管理层面需求如下：

1.1.3.6.2.1安全管理制度需求

建立信息安全领导小组，信息安全领导小组定期对安全管理制度的合理性和适用性进行论证和审定，对存在不足或需要改进的安全管理制度进行修订。实现安全管理制度通过正式、有效的方式进行发布，并进行统一的版本控制。

1.1.3.6.2.2安全管理机构需求

* 加强各类管理人员、组织内部机构和网络安全管理部门之间的合作与沟通，定期召开协调会议，共同协作处理网络安全问题，并留存合作与沟通的证明材料，包括会议纪要，管理制度说明等。

###### 1.1.3.6.3安全管理人员需求

* 定期对不同岗位的人员进行技能考核。并将考核结果做好记录保存。

###### 1.1.3.6.4安全建设管理需求

* 留存软件设计文档和使用指南、安全检查报告。
* 留存工程实施方案。
* 留存测试验收方案和测试验收报告。
* 留存建设过程文档和运行维护文档。

1.1.3.6.4.1安全运维保障需求

* 安排人员对现网资产进行梳理，完成资产清单证明及资产识别。
* 对介质在物理传输过程中的管理进行控制，定期盘点存档介质的目录清单。存储介质的使用过程、送出维修以及销毁等进行严格的管理，输出相关记录文件。现重要介质的异地存储；
* 由安全管理员、网络管理员对通信线路、主机、网络设备和应用的运行状况进行监控和报警，输出相关的监测记录；
* 组织相关人员定期对监测和报警记录进行分析和评审。定期检查违反规定拨号上网或其他违反网络安全策略的行为，留存相应的检测记录；
* 通过安全漏洞扫描评估服务，定期对网络系统、主机系统等进行漏洞扫描，输出相关扫描记录；
* 利用堡垒机系统，定期对操作运维日志和审计数据进行分析，输出相应的分析报告；
* 安全事件报告和响应处理过程中的记录文件进行保存；
* 通过应急演练服务，对系统相关人员开展应急预案培训，并形成培训记录文件。通过应急演练服务，定期对应急预案开展演练，并形成演练记录文件。
* 利用终端杀毒系统，对网络和主机进行恶意代码检测，并出具相应的分析报告。通过人工服务定期检查信息系统内各种产品的恶意代码库的升级情况并进行记录，输出相应的记录文件；

###### 1.1.3.6.5密码应用建设需求

1.1.3.6.5.1海南法院智慧执行服务系统

一、物理和环境安全需求

* 海南省高级人民法院中心机房

采用国密算法对进出机房人员进行身份鉴别。

采用国密算法对电子门禁记录及视频监控记录进行完整性保护。

二、网络和通信安全需求

* 身份鉴别需求

采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对各通信信道中的通信实体进行身份鉴别，保证通信实体身份鉴别的真实性。

* 数据完整性和重要数据机密性保护需求

采用密码技术的加解密功能对各通信信道中传输的重要数据进行机密性保护。

采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对通信信道中传输的数据进行完整性保护。

* 网络边界访问控制信息完整性保护需求

采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对网络边界设备的访问控制信息列表进行完整性保护。

三、设备和计算安全需求

* 身份鉴别需求

采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备运维管理人员等登录设备的用户进行身份鉴别，保护登录设备用户的身份真实性。

* 安全通道需求

通过部署符合GM/T0026-2014《安全认证网关产品规范》要求的安全认证网关，建立国密SSLVPN隧道，从而实现安全的信息传输通道。

* 访问控制信息完整性保护需求

系统应用服务器、数据库服务器、安全设备等设备资源访问控制信息使用基于合规的密码技术进行完整性保护。

* 日志记录完整性保护需求

日志在存储过程中使用合规的密码技术对其进行完整性保护，确保在日志的存储状态下不会被恶意的篡改。

* 重要可执行程序完整性、来源真实性保护

需采用密码技术保证重要可执行程序的完整性和来源可靠性，利用合规的密码算法进行数字签名实现完整性保护，使用或读取这些程序或文件时，进行验签以确认完整性，从而实现重要可执行程序的完整性和来源可靠性的保护。

四、应用和数据安全需求

* **身份鉴别需求**

采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，在业务人员、系统管理人员登录智慧执行系统时对登录用户进行身份鉴别。

* **访问控制信息完整性需求**

采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对智慧审判、智慧执行、智慧诉服等系统的权限、标签等能够决定系统应用访问控制的措施等信息进行完整性保护。

* **重要信息资源安全标记完整性需求**

本系统不存在重要信息资源安全标记。

* **重要数据传输、存储过程机密性需求**

采用密码技术的加解密功能，对智慧审判、智慧执行、智慧诉服等系统中的鉴别数据、重要业务数据、重要审计数据、个人敏感信息等重要数据进行传输和存储过程中的机密性保护。

* **数据传输、存储过程完整性需求**

采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对信息系统应用中的鉴别数据、重要业务数据、重要审计数据、个人敏感信息等重要数据进行传输和存储过程中的完整性保护。

五、密钥管理安全需求

（1）密钥需由安全合规的密钥管理系统产生，保证密钥高质量。

（2）密钥安全存储在安全合规的密钥管理系统或以密文的形式存储在安全合规的商用密码产品外部，分发过程采用非对称算法的形式进行加密，保证传输的安全性。

（3）建立完善的密钥备份和归档机制，确保密钥不会被泄露，不会被密钥被恢复到非法的设备中。

（4）指定合理的密钥销毁机制，及时销毁不适用的密钥，确保被销毁的密钥不会被恶意恢复。

六、安全管理需求

制定密码应用安全管理制度，包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。根据密码应用方案建立相应密钥管理规则。

对管理人员或操作人员执行的日常管理操作建立操作规程。定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订。

明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制，并对密码应用操作规程的相关执行进行记录并妥善保存。

业务系统的相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度，建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限，建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能，并定期对密码应用安全岗位人员进行考核，建立关键人员保密制度和调离制度，签订保密合同，承担保密义务。

制定密码应用应急处置方案，做好应急资源准备，当密码应用安全事件发生时，能够立即启动应急处置方案，做好应急资源准备，当密码应用安全事件发生时，能够立即启动应急处置方案，结合实际情况及时处置。事件发生后，及时向信息系统的上级主管部门进行报告。事件处置完成后，及时向上级主管部门及归属的密码管理部门报告事件发生情况及处置情况。

### 1.1.4详细技术要求

#### 1.1.4.1软硬件设备详细性能需求（本项目核心产品为（监狱管理局接入区）-防火墙（三合一））

##### 表1：硬件设备

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **技术参数** | **单位** | **数量** |
| **一** | **网络安全** |  |  |  |
| **一）** | **安全等保** |  |  |  |
| 1 | **法院专网区** |  |  |  |
| 1.1 | 法院专网（专享云接入区）-入侵防御 | 1、网络层吞吐量≥20G；入侵检测吞吐≥3Gbps；并发连接≥900万；每秒新建连接数≥20万；冗余电源；  2、≥1个MGT管理接口；≥1个HA接口；≥8个10/100/1000M自适应电口（支持4对Bypass），≥4个SFP插槽，≥2个万兆SFP+插槽；≥1个接口板卡扩展插槽；≥1个Console口；≥2个USB接口；≥1T硬盘；  3、能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；  4、支持防御基于安全域的IP地址欺骗攻击，指定IP或网段必须从特定安全域流入；  5、支持基于MD5的自定义病毒签名；  6、支持设置例外特征，对特定的病毒特征不进行查杀；  7、国产化产品,提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章； | 台 | 2 |
| 防病毒模块功能参数要求：  1、支持通过授权扩展支持对HTTP、FTP、SMTP、POP3、IMAP协议的病毒检测和过滤功能；  2、支持支持VLAN、VoIP数据流病毒过滤；  3、支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于30万；  4、支持HTTP协议和邮件协议防病毒，通过信息替换功能，用以通知用户病毒被阻断，管理员可以自行设置替换信息； | 套 | 2 |
| 1.2 | 法院专网（网络边界接入区）-入侵防御 | 1、网络层吞吐量≥20G；入侵检测吞吐≥3Gbps；并发连接≥900万；每秒新建连接数≥20万；冗余电源；  2、≥1个MGT管理接口；≥1个HA接口；≥8个10/100/1000M自适应电口（支持4对Bypass），≥4个SFP插槽，≥2个万兆SFP+插槽；≥1个接口板卡扩展插槽；≥1个Console口；≥2个USB接口；≥1T硬盘；  3、能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；  4、支持防御基于安全域的IP地址欺骗攻击，指定IP或网段必须从特定安全域流入；  5、支持基于MD5的自定义病毒签名；  6、支持设置例外特征，对特定的病毒特征不进行查杀；  7、国产化产品,提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章； | 台 | 2 |
| 防病毒模块功能参数要求：  1、支持通过授权扩展支持对HTTP、FTP、SMTP、POP3、IMAP协议的病毒检测和过滤功能；  2、支持支持VLAN、VoIP数据流病毒过滤；  3、支持对文件感染型病毒、蠕虫病毒、脚本病毒、宏病毒、木马、恶意软件等过滤，病毒库数量不少于30万；  4、支持HTTP协议和邮件协议防病毒，通过信息替换功能，用以通知用户病毒被阻断，管理员可以自行设置替换信息； | 套 | 2 |
| 1.3 | 法院专网（专网服务区）数据库审计 | 1、≥4TB磁盘存储空间，≥1个RJ45接口,≥2个USB接口，≥10个千兆电口，≥4个千兆光口，≥2个万兆光口。  2、支持的数据库：达梦、人大金仓、南大通用Gbase等主流国产化数据库；  3、审计选项支持配置按规则审计和全审计两种模式；  4、可根据事件的时间范围、客户端IP、关键字、进程名、规则名、客户端端口号、返回内容等多种条件进行事件回放，回溯事件过程；  5、国产化产品,提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章； | 台 | 1 |
| 2 | **安全隔离交换区** |  |  |  |
| 2.1 | (互联网业务隔离交换区)WEB应用防火墙 | 1、网络吞吐量≥7Gbps，HTTP吞吐量≥4Gbps，HTTP新建连接数≥65000/秒，HTTP并发连接数≥550万/秒；  2、≥4TB硬盘，冗余电源，≥1个独立HA口，≥1个独立MGT管理口，≥4个扩展卡插槽，≥1个console口，≥2个USB口；  3、具备Web业务控制防御功能，提供针对爬虫、黑链、内网代理以及盗链的防护功能；  4、具备敏感信息检测防护，检测类型包括：中间件信息保护，数据库信息保护，敏感文件保护，代码错误信息保护，隐私信息保护；  5、具备非法URL外联检测功能，针对特定外联URL进行监控或阻断，并且支持自定义URL地址；  6、具备移动终端管理功能，不需要安装APP和第三方插件，通过手机浏览器即可管理设备，并可查看设备CPU、内存使用情况；  7、国产化产品,提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章； | 台 | 1 |
| 2.2 | （监狱管理局接入区）-防火墙（三合一）（核心产品） | ▲1、网络层吞吐量≥19G；并发连接≥3000万；每秒新建连接数≥45万；  2、冗余电源；≥1个MGT管理接口；≥1个HA接口；≥4个10/100/1000M自适应电口；≥4个SFP插槽；≥2个万兆SFP+插槽；≥2个接口板卡扩展插槽；≥1个Console口；≥2个USB接口；≥1TB硬盘；  3、支持应用识别，应用特征库包含的应用数量（非应用协议的规则总数）大于2800种，可深度识别每种应用的属性，为每种应用提供预定义的风险系数，并将应用基于类型、使用场景、数据传输、风险等级等特征分类；  4、支持共享上网检测功能，支持共享接入检测和共享接入管控功能，可以通过设置管控地址和例外地址优化管控功能，同时支持阻断或告警动作；  5、能够对HTTP/FTP/POP3/SMTP/IMAP/SMB六种协议进行病毒查杀；  6、本地病毒库规模大于3000万；  7、国产化产品,提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章； | 台 | 1 |
| **二）** | **网络建设** |  |  |  |
| **1** | **内网** |  |  |  |
| 1.1 | 广域网核心交换机 | ▲1、采用国产化CPU及转发芯片，自主可控,提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  ▲2、交换容量不低于500Tbps；包转发率不低于96000Mpps；  ▲3、主控引擎不少于2个；独立交换网板不少于4个；整机业务板槽位数不少于8个,提供官方证明材料截图及链接，并加盖原厂公章或投标专用章；  4、支持整机MAC地址不少于1M，整机ARP表项不少于384K，IPv4路由转发FIB表项不少于3M，IPv6路由转发FIB表项不少于1M；  5、支持VxLAN功能，支持VxLAN网络的自动化部署；  6、支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；  7、支持4KVLAN；支持1：1，N：1VLANmapping；  8、支持MPLSL3VPN、MPLSL2VPN(VPLS，VLL)、MPLS-TE、MPLSQoS；  9、支持通过命令行、中文图形化配置软件等方式进行配置和管理；  10、双主控、双电源，万兆光口不少于24个，千兆光口不少于24个，千兆电口不少于48个，万兆单模模块不少于24个，千兆单模模块不少于24个； | 台 | 2 |
| 1.2 | 广域网路由器 | ▲1、交换容量不低于115Tbps，支持包转发率不低于14400Mpps；  ▲2、采用国产化CPU及转发芯片，自主可控，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  3、支持双主控且满配，支持电源冗余，要求所有业务板卡及电源、风扇均可热插拔；  4、整机业务载板插槽不少于6个；  ▲5、支持100GE、10GE、40GE、GE、FE、E1、CPOS等接口类型，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  6、支持RIP、OSPF、IS-IS、BGP等路由协议；  7、支持L2VPN、L3VPN、EVPN等VPN技术；  ▲8、支持IPv4路由表容量不低于10M,IPv6路由表容量不低于5M，IPv4转发表容量不低于4M,IPv6转发表容量不低于2M，VRF容量不低于4K，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  9、支持ISISforSRv6；  10、支持VRRP、Eth-Trunk、E-Trunk等可靠性技术；  11、支持Console、Telnet、SSH、SNMP等管理方式；  12、双主控、双电源，万兆光口不少于4个，千兆光口不少于10个，千兆电口不少于8个，万兆光模块不少于4个，千兆光模块不少于10个； | 台 | 2 |
| 1.3 | 48口楼层接入交换机 | 1、交换容量不低于670Gbps，包转发率不低于200Mpps；  2、支持能效以太网EEE节能环保；  ▲3、采用国产化CPU及转发芯片，自主可控，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  ▲4、提供不少于48个千兆电口，4个万兆光口，2个12GE专用堆叠口，提供官方证明材料截图及链接，并加盖原厂公章或投标专用章；  5、支持统一用户管理功能，支持802.1X/MAC/Portal等多种认证方式；  6、支持4KVLAN，支持VoiceVLAN、支持端口VLAN、协议VLAN、IP子网VLAN；  7、支持静态路由、RIP、OSPF、RIPng、OSPFv3；  8、支持MAC表项不少于32K，IPv4路由表不少于4K，IPv6路由表不少于1K，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  9、支持防ARP攻击、DOS攻击、ICMP防攻击、CPU保护；  10、支持G.8032（ERPS）标准以太环网协议；  11、支持堆叠，主机堆叠数不小于9台；  12、支持IPv6、支持IPv4/IPv6双栈；  13、支持基于第二层、第三层和第四层的ACL、支持双向ACL；  14、支持SNMPv1/v2/v3、Telnet、RMON、SSHv2；支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；  15、不少于2个万兆单模模块； | 台 | 33 |
| 1.4 | 24口楼层接入交换机 | 1、交换容量不低于670Gbps，包转发率不低于170Mpps；  2、支持能效以太网EEE节能环保；  ▲3、采用国产化CPU及转发芯片，自主可控，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  ▲4、提供不少于24个千兆电口，4个万兆光口，2个12GE专用堆叠口，提供官方证明材料截图及链接，并加盖原厂公章或投标专用章；  5、支持统一用户管理功能，支持802.1X/MAC/Portal等多种认证方式；  6、支持4KVLAN，支持VoiceVLAN、支持端口VLAN、协议VLAN、IP子网VLAN；  7、支持静态路由、RIP、OSPF、RIPng、OSPFv3；  8、支持MAC表项不少于32K，IPv4路由表不少于4K，IPv6路由表不少于1K，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  9、支持防ARP攻击、DOS攻击、ICMP防攻击、CPU保护；  10、支持G.8032（ERPS）标准以太环网协议，故障倒换收敛时间小于50ms；  11、支持堆叠，主机堆叠数不小于9台；  12、支持IPv6、支持IPv4/IPv6双栈；  13、支持基于第二层、第三层和第四层的ACL、支持双向ACL；  14、支持SNMPv1/v2/v3、Telnet、RMON、SSHv2，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；  15、不少于2个万兆单模模块； | 台 | 6 |
| 1.5 | 域名解析服务器 | 1、CPU和操作系统：通过中国信息安全测评中心测评的产品（提供中国信息安全测评中心官网截图加盖原厂公章或投标专用章）。  2、软硬件一体化DNS设备，支持不低于6个千兆电口，硬盘存储不低于2TB。  3、开启解析日志（Querylog）时的QPS不低于80000。  4、具备系统级、软件功能级冗余备份能力，支持HA部署或ANYCAST集群部署，实现双设备中单一设备故障时的高可用。  5、支持通过统一的管理平台上完成所有服务的配置，支持分布式部署，可针对指定的单一节点或多个节点下统一下发配置，并保证数据一致性。下发的数据进行加密，保障数据的安全性。  6、支持为指定用户组设定权限，权限至少分为WEB管理权限、CLI权限、API权限；支持对用户进行精细权限定义，可以创建多个账号，每个帐号针对不同的功能模块分别分配不同的权限。  7、支持通过Web前台查看集群内所有节点的设备型号、序列号、内存大小、磁盘数量/容量、CPU主频/内核/线程数量。  8、支持用户操作日志记录，支持系统日志记录，支持DNS解析日志。支持日志通过Syslog方式发送到指定日志服务器，支持日志以FTP方式自动备份至指定服务器的指定目录。  9、支持审核工作流，审核人员可对被审核人员在DNS系统中所有的新建，编辑，删除，批量变更等操作进行审批，审批结果支持邮件通知，且可指定审核人员与被审核人员的对应关系，审核记录支持追溯。  10、管理中心具备自动备份所有节点的配置，支持备份周期设置，支持异地备份方式，包括但不限于FTP、SCP、SFTP。  ▲11、支持定时将DNS服务器的权威域主区配置同步给一级网，解析日志进行同步汇总，至少每5小时同步一次，归档整理后发送至最高法院指定的加密存储服务器。日志格式内容应包括但不限于以下字段内容：时间、请求域名、请求源 IP、请求源端口、查询视图、Class 类别、请求记录类型等，涉及开发费包含在此项中，厂商需提供免费开发承诺函加盖原厂公章或投标专用章。  12、支持查看指定节点设备和所有节点设备当前及与最近6小时、12小时、1天、1周、1个月、3个月的DNS关键运行指标，指标通过曲线图、柱状图等进行清晰展现，统计数据可在WEB直接下载为PDF或CSV格式文件，提供官方证明材料截图，并加盖原厂公章或投标专用章。  ▲13、符合“法院统一DNS系统建设及接入规范”要求，支持通过一级网特定API接口，将数据由特定API命令同步一级网DNS系统，实现同步与备份，涉及开发费包含在此项中，厂商需提供免费开发承诺函加盖原厂公章或投标专用章。  14、支持主辅区域一致性校验，DNS作为主区或辅区时，支持在WEB界面手动触发主辅区数据一致性校验，保证数据一致性。支持主辅区域一键切换，辅区切换为主区前的区记录保留，无须重新逐条配置。  15、支持动态调度算法，且多种调度算法可以进行组合，并支持二级调度，即优先按照某策略调度到某应用服务器池，然后再根据某策略调度到该池内具体服务器，提供官方证明材料截图，并加盖原厂公章或投标专用章。  16、递归查询支持多种智能算法，可配置First、only等转发方式，同时支持转发失败后通过递归迭代继续查询;支持转发服务器分组，支持转发服务器健康探测和异常告警，对异常服务器支持复检，保证异常服务器恢复后快速可用，提供官方证明材料截图，并加盖原厂公章或投标专用章。  17、支持基于视图对任一域名和域进行缓存设置，并可以通过前台立即刷新对应的缓存结果。  18、支持对隧道攻击进行拦截，拦截策略包含告警及告警并拦截，支持隧道攻击事件告警，支持隧道攻击日志记录，可事后对攻击进行溯源。 | 台 | 2 |
| 1.6 | 24口跨网接入交换机 | 1、交换容量不低于670Gbps，包转发率不低于170Mpps；  2、支持能效以太网EEE节能环保；  3、采用国产化CPU及转发芯片，自主可控，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  4、提供不少于24个千兆电口，4个万兆光口，2个12GE专用堆叠口，提供官方证明材料截图及链接，并加盖原厂公章或投标专用章；  5、支持统一用户管理功能，支持802.1X/MAC/Portal等多种认证方式；  6、支持4KVLAN，支持VoiceVLAN、支持端口VLAN、协议VLAN、IP子网VLAN；  7、支持静态路由、RIP、OSPF、RIPng、OSPFv3；  8、支持MAC表项不少于32K，IPv4路由表不少于4K，IPv6路由表不少于1K，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  9、支持防ARP攻击、DOS攻击、ICMP防攻击、CPU保护；  10、支持G.8032（ERPS）标准以太环网协议，故障倒换收敛时间小于50ms；  11、支持堆叠，主机堆叠数不小于9台；  12、支持IPv6、支持IPv4/IPv6双栈；  13、支持基于第二层、第三层和第四层的ACL、支持双向ACL；  14、支持SNMPv1/v2/v3、Telnet、RMON、SSHv2，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；  15、不少于2个万兆单模模块； | 台 | 4 |
| **2** | **外网** |  |  |  |
| 2.1 | 汇聚交换机 | ▲1、交换容量不低于2.5Tbps，包转发率不低于450Mpps，提供官方证明材料截图及链接，并加盖原厂公章或投标专用章；  2、为了提高设备可靠性，支持模块化可插拔双电源；  ▲3、采用国产化CPU及转发芯片，自主可控，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  4、提供不少于24个千兆电口，4个万兆光口，2个40GE光口，不少于1块业务扩展槽位；  5、支持融合AC管理功能，整机可管理1KAP；  6、支持静态路由、RIPV1/2、OSPF、IS-IS、BGP、RIPng、OSPFv3、BGP4+、ISISv6；  ▲7、支持MAC地址规格不少于128K，ARP表项规格不少于140K，Ipv4路由FIB表不少于192K，Ipv6路由FIB表不少于80K，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  8、支持基于第二层、第三层和第四层的ACL、支持双向ACL；  9、支持MPLSL3VPN、MPLSL2VPN(VPLS/VLL)、MPLS-TE、MPLSQoS；  10、支持防ARP攻击、DOS攻击、ICMP防攻击、CPU防攻击；  11、支持G.8032（ERPS）标准以太环网协议，故障倒换收敛时间小于50ms；  12、支持堆叠，主机堆叠数不小于9台；  13、支持SNMPv1/v2/v3、Telnet、RMON、SSHv2；支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；  14、双电源，不少于2个万兆单模模块； | 台 | 1 |
| 2.2 | 汇聚交换机 | 1、交换容量不低于670Gbps，包转发率不低于160Mpps；  2、支持能效以太网EEE节能环保；  3、采用国产化CPU及转发芯片，自主可控，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  4、提供不少于48个千兆电口，4个千兆光口；  5、支持统一用户管理功能，支持802.1X/MAC/Portal等多种认证方式；  6、支持4KVLAN，支持VoiceVLAN、支持端口VLAN、协议VLAN、IP子网VLAN；  7、支持静态路由、RIP、OSPF、RIPng、OSPFv3；  8、支持MAC表项不少于32K，IPv4路由表不少于4K，IPv6路由表不少于1K，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  9、支持防ARP攻击、DOS攻击、ICMP防攻击、CPU保护；  10、支持G.8032（ERPS）标准以太环网协议，故障倒换收敛时间小于50ms；  11、支持堆叠，主机堆叠数不小于9台；  12、支持IPv6、支持IPv4/IPv6双栈；  13、支持基于第二层、第三层和第四层的ACL、支持双向ACL；  14、支持SNMPv1/v2/v3、Telnet、RMON、SSHv2，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；  15、不少于2个千兆单模模块； | 台 | 2 |
| 2.3 | 楼层接入交换机 | 1、交换容量不低于670Gbps，包转发率不低于160Mpps；  2、支持能效以太网EEE节能环保；  3、采用国产化CPU及转发芯片，自主可控，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  4、提供不少于48个千兆电口，4个千兆光口；  5、支持统一用户管理功能，支持802.1X/MAC/Portal等多种认证方式；  6、支持4KVLAN，支持VoiceVLAN、支持端口VLAN、协议VLAN、IP子网VLAN；  7、支持静态路由、RIP、OSPF、RIPng、OSPFv3；  8、支持MAC表项不少于32K，IPv4路由表不少于4K，IPv6路由表不少于1K，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  9、支持防ARP攻击、DOS攻击、ICMP防攻击、CPU保护；  10、支持G.8032（ERPS）标准以太环网协议，故障倒换收敛时间小于50ms；  11、支持堆叠，主机堆叠数不小于9台；  12、支持IPv6、支持IPv4/IPv6双栈；  13、支持基于第二层、第三层和第四层的ACL、支持双向ACL；  14、支持SNMPv1/v2/v3、Telnet、RMON、SSHv2，支持通过命令行、Web、中文图形化配置软件等方式进行配置和管理；  15、不少于2个千兆单模模块； | 台 | 12 |
| **3** | **监控网** |  |  |  |
| 3.1 | 核心交换机 | ▲1、交换容量不低于38Tbps，包转发率不低于7200Mpps；  ▲2、采用国产化CPU及转发芯片，自主可控；提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  3、主控引擎不少于2个；整机业务板槽位数不少于3个，整机电源槽位数不少于2个，电源功率不少于3000W；  4、支持整机MAC地址不低于1M，整机ARP表项不低于256K，整机ACL表项不低于256K；  5、支持MPLSL3VPN、MPLSL2VPN(VPLS，VLL)、MPLS-TE、MPLSQoS；  6、持VxLAN功能，支持VxLAN二层网关、三层网关，支持BGPEVPN，支持分布式Anycast网关，支持VxLANFabric的自动化部署；  7、支持IPv6过渡技术，IPv4/IPv6双栈、6over4隧道、4over6隧道；  8、支持静态路由、RIP、RIPng、OSPF、OSPFv3、BGP、BGP4+、ISIS、ISISv6；  9、支持4KVLAN；支持1：1，N：1VLANmapping；  10、支持DHCPsnoopingbindingtable(DAI,IPsourceguard),防止ARP攻击、DDOS攻击、中间人攻击；  11、支持G.8032标准环网协议；  12、支持通过命令行、中文图形化配置软件等方式进行配置和管理；  13、双主控、双电源，万兆光口不少于24个，千兆光口不少于24个，千兆电口不少于48个，万兆光模块不少于24个，千兆光模块不少于24个； | 台 | 1 |
| 3.2 | 监控POE交换机 | 1、标准机架式交换机；  2、设备交换容量≥670Gbps，包转发率≥200Mpps；  3、设备提供≥48个自适应千兆电口，≥4个万兆光口，≥2个独立堆叠光口；  ▲4、采用国产化CPU及转发芯片，自主可控，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  5、设备支持802.3af、802.3at供电协议；  6、设备支持4K个VLAN，支持Access、Trunk、Hybrid方式；  7、设备支持RIP、OSPF、ISIS、BGP等IPv4动态路由协议；  8、设备支持RIPng、OSPFv3、ISISv6、BGP4+等IPv6动态路由协议；  9、支持MAC表项不少于32K，IPv4路由表不少于4K，IPv6路由表不少于1K，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  10、设备配置≥2个千兆单模光模块。 | 台 | 6 |
| **二** | **信任体系建设** | |  |  |
| 1 | 增强型密钥管理系统 | 1、提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件加盖原厂公章或投标专用章。  2、由密钥生产系统、分发系统和管理系统组成，支持SM2、SM3、SM4算法，具有密钥生成、分发、存储、管理等功能。  3、SM4加/解密速率为≥149Mbps/131Mbps；SM2密钥对生成速率为≥321对/秒，加/解密速率为≥133Kbps/114Kbps；签名速率为≥127次/秒，验签速率为≥108次/秒；SM3运算速率为≥197Mbps。  4、支持KEY介质序列号功能，在开启介质序列号控制时，密钥分发可以验证介质序列号是否在授权之内，只有已授权的介质允许签发证书。  5、支持密钥恢复：密钥管理系统可为用户提供密钥恢复服务和为司法取证提供密钥恢复服务。密钥恢复需按管理策略进行审批，一般用户只限于恢复自身密钥。  6、支持各个功能模块的运行事件记录、服务器状态记录、系统重要策略、密钥操作记录、操作人员信息必须有相应的审计机制，日志支持签名验证。  7、密钥管理中心要支持预产生密钥功能,可以通过设定策略定时产生，也可以支持手动产生。  8、支持CA接入管理，支持CA冻结功能，支持CA密钥分发数设置，支持阀值超限。  9、密钥生成服务可以根据密钥类型独立运行、停止。  10、支持密钥使用汇总、密钥使用查询、密钥服务汇总、密钥服务查询、密钥时间分段、日志数量分析等报表生成。  ▲11、支持密钥不落地，提供非对称密钥传输过程中用户加密密钥的保护方法证书等相关证明材料复印件加盖原厂公章或投标专用章。  12、提供公安部计算机信息系统安全产品质量监督检验中心检测报告加盖原厂公章或投标专用章。 | 套 | 1 |
| 2 | 增强型数字证书认证系统 | 1、提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件加盖原厂公章或投标专用章。  2、由证书签发系统、注册审核系统、证书状态查询系统、目录服务系统等组成。支持SM2、SM3、SM4算法。  3、具有用户注册管理、证书签发、CRL签发、证书更新、证书状态查询、日志管理等功能。  4、SM4加/解密速率≥131Mbps/116Mbps；SM2密钥对生成速率≥1340对/秒，加/解密速率≥26Mbps/29Mbps，签名速率≥239次/秒，验签速率≥145次/秒；SM3运算速率为183Mbps；证书签发性能≥3秒/次。  5、支持一键四证（RSA双证书、SM2双证书）证书发放模式；  6、兼容飞腾或兆芯或海光等处理器；  ▲7、兼容主流银河麒麟、统信UOS、中科方德操作系统；提供互认证明文件加盖原厂公章或投标专用章；  8、兼容主流数据库达梦数据库、金仓数据库；提供互认证明文件加盖原厂公章或投标专用章；  9、支持双证书（加密证书和签名证书）和双中心（证书管理中心和密钥管理中心）结构；  10、支持加密密钥安全传输，支持密钥不落地机制；  11、支持证书策略管理，对密钥用法、扩展密钥用法、有效期、生效时间进行配置管理。  12、证书支持基于HTTP式和LDAP模式的CRL发布点和AIA发布点。  13、黑名单（CRL）支持分块CRL与增量CRL，支持FreshCRL扩展点。  14、支持多种内置证书模板，支持签发普通用户单双证书、机构证书、设备证书、VPN证书、代码签名证书、微软域证书。  15、系统中的各个服务组件都应具备独立的审计模块，可以对日志操作进行签名验证。  16、提供证书查询、证书统计等证书管理功能。  17、提供证书归档功能，支持证书当前库、历史库。  ▲18、能实现与最高人民法院离线部署的人民法院根CA无缝对接，满足全国法院跨级、跨区域安全访问的需求。提供二级CA中心与最高人民法院根CA（一级CA中心）无缝对接的所投产品厂商的案例以及厂商的对接承诺加盖原厂公章或投标专用章;  ▲19、证书签发性能SM2单证不低于2000次/秒、SM2双证不低于1000次/秒，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章。 | 套 | 1 |
| 3 | 安全认证网关 | 1、提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件加盖原厂公章或投标专用章。  2、支持SM1、SM2、SM3、SM4、SM9算法，具有身份鉴别、安全报文传输等功能。  3、最大并发数≥10000，最大并发连接数≥9000，每秒新建连接数为500，吞吐率≥800Mbps。  4、支持设备管理、远程管理功能。  5、产品支持IPv6功能，提供IPv6ReadyLogo认证证明材料并加盖原厂公章或投标专用章。  6、支持在同一个服务实例中，配置RSA和SM2两张站点证书，并同时启动，根据客户端的算法能力进行自动适应。  ▲7、支持超过100万条目数的证书黑名单。提供快速检索海量数字证书黑名单的方法证书等相关证明材料复印件加盖原厂公章或投标专用章。  ▲8、支持用户管理、身份鉴别、应用管理、访问控制、单点登录、信息审计、随机数质量检测、密钥交互、安全报文传输、密钥更新、NAT穿越、抗重放攻击，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章。  9、提供中国软件测评中心的安全产品测试报告加盖原厂公章或投标专用章。  ▲10、支持SM9（IBC)-SM1-SM3服务端最大并发用户数≥40000，服务端吞吐率≥1000Mbps，提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章。 | 套 | 4 |
| 4 | 签名验签服务器 | 1、提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件加盖原厂公章或投标专用章。  2、支持SM2、SM3、Sm4算法。  3、具有密钥协商、身份认证、SSL隧道加密等功能。  4、SM2签名速率≥6000次/秒，验签速率≥6000次/秒。  5、产品支持IPv6功能，提供IPv6ReadyLogo认证证书并加盖原厂公章或投标专用章。  6、提供国家网络与信息系统安全产品质量监督检验中心颁发的《信息技术产品安全测试证书》复印件加盖原厂公章或投标专用章。  7、产品的CPU、操作系统符合中国信息安全测评中心、国家保密科技测评中心的安全可靠测评要求。 | 套 | 2 |
| 5 | 服务器密码机 | 1、提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件加盖原厂公章或投标专用章。  2、采用由国家密码管理局批准使用的双物理噪声源生成随机数，可生成各类对称密钥（SM1、SM4、AES等）和非对称密钥（SM2、RSA2048/4096等），支持基于国密SM1、SM3、SM4算法，以及国际算法SHA-2系列、SHA1的MAC产生和验证。  3、具有密钥管理、密码运算、身份认证等功能。  4、SM4加/解密速率≥800Mbps；SM2密钥对生成速率≥20000对/秒，加/解密速率≥20000次/秒，签名/验签速率≥20000次/秒；SM3运算速率≥500Mbps。  5、支持通过物理开关对设备内全部密钥进行销毁。  6、支持多级密钥保护模式。 | 套 | 3 |
| 6 | 在线证书管理系统 | 1、提供资源管理、证书管理、终端管理；  2、提供发证策略配置、发证统计；  3、提供详细的证书生命周期管理。单次请求处理时间（用户管理、证书管理等功能）<0.3秒；  4、算法支持RSA1024、2048位密钥长度及SM2密钥；  5、支持证书的在线更新、延期功能；  6、支持使用个人证书自助登录系统；  7、支持已过期证书的更新请求；  8、提供在线管理页面及参数配置管理功能（可设置包括证书更新有效期、快过期时限等设置）；  9、提供在线客户端证书链检测；  10、提供在线客户端证书链及控件自动安装；  11、提供在线证书更新申请及申请准入判断功能；  12、提供在线证书申请功能，要求用户信息不变，具体失效时间可根据参数设置；  13、系统架构应采用B/S管理模式以及B/S应用模式，提供第三方开发接口，并能够与应用系统集成。 | 套 | 1 |
| 7 | 时间戳服务器 | 1、提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件加盖原厂公章或投标专用章。  2、支持SM2、SM3、SM4算法。  3、具有时间戳生成、应答、验证等功能。  4、时间戳生成速率≥150次/秒，验证速率≥100次/秒。 | 套 | 2 |
| 8 | 可信身份管控平台 | 1、包含身份汇聚管理、身份信息上报、统一身份认证、部省认证级联、访问控制策略管理、操作审计与身份风险分析、接口服务和应用集成开发。  2、以密码为基石、融合多种身份认证方式，采用微服务化架构，为业务系统提供统一身份认证和单点登录服务。  3、支持数字证书、动态令牌、帐号口令、生物特征、第三方标准协议等多种身份认证方式，支持认证组合配置；支持策略化的多因子认证，支持应用级多因子认证；  ▲4、支持基于环境属性的动态认证，支持二次认证，提供产品功能截图并加盖原厂公章或投标专用章。  ▲5、支持认证会话的管理，支持应用和认证会话的保持；支持应用属性的灵活扩展，提供产品功能截图并加盖原厂公章或投标专用章。  6、支持身份数据汇聚，支持从现有统一用户等多个身份源同步身份数据，对身份数据汇聚管理；  7、支持向部级统一用户系统上报身份数据，实现身份数据部省级联。  ▲8、支持以拉取方式为应用系统提供身份数据同步服务，提供产品功能截图并加盖原厂公章或投标专用章。  9、支持配置同步策略，可实现按需对身份数据范围、身份字段，敏感数据脱敏等控制手段；支持对用户、设备进行风险评分，评分支持风险模型配置，包括但不限于按照风险等级进行基线配置、按照风险类型进行占比配置、按照发生次数进行扣分标准配置等；  10、支持身份风险大屏，能够展示出持续信任评估到动态访问控制间的数据流动、用户触发的实时风险、风险用户TOP5、阻断应用TOP5、用户访问趋势等；  11、支持零信任动态访问控制，提供访问控制策略管理配置，策略属性支持主客体属性、时间，IP，认证方式以及身份风险评分等多种静态和动态属性。  12、支持与应用安全网关集成，作为访问控制策略的执行点，实现对应用基于访问控制策略的强管控。  13、支持用户认证，访问等行为日志的审计，支持阅后即审；  ▲14、支持用户综合审计概览，包括僵尸账号、认证情况、告警情况、活跃用户统计、用户告警处置统计、风险用户排行、用户告警类型分布、用户最新告警列表等,提供产品功能截图并加盖原厂公章或投标专用章。  ▲15、支持与RA的证书管理深度融合联动，完成一体化用户证书管理，实现用户证书全生命周期与用户身份全生命周期强绑定关联，提供产品功能截图并加盖原厂公章或投标专用章。  16、具备完整的证书业务分析能力和证书生命周期监控； | 套 | 1 |
| 9 | 数据加密网关 | 1、提供数据资产发现，数据加密密钥管理；  2、支持数据加密策略管理，数据透明加密，数据加密密钥更换等；  ▲3、系统可以对数据字段项设置加密规则，提供数据库列级加密，并支持对不同字段列设置不同的密钥和加密算法，提供产品功能截图并加盖原厂公章或投标专用章。  4、系统支持Mysql、Oracle、DB2、SqlServer、达梦、人大金仓等多种数据库。  5、敏感数据发现能力，提供可视化的敏感数据发现，支持自定义发现算法，支持敏感数据变化跟踪。  6、数据域发现能力开箱即用，内置丰富的发现算法，如：姓名、地址、电话、公司、身份证号、卡号等。  ▲7、支持应用系统免改造加密，支持字段级别的数据内容加密，支持图形化自定义能力，提供历史数据管理；提供灵活的加密状态和非加密状态的双向转换，提供产品功能截图并加盖原厂公章或投标专用章。  8、提供加密数据查询客户端，支持表、视图、物化视图，存储过程函数的查询、管理能力，提供明文方式进行数据维护的功能，提供灵活的数据管理服务能力。  9、提供图形化的数据加密配置，可以对指定数据表列的全部数据进行一次性加密进行加密，加密初始化时使用与字段加密配置一样的加密算法和密钥。  10、数据加密网关SM4算法加解密速率≥200Mbps。  11、支持JAVA/C语言等多种开发语言。  12、提供信创产品评估认证证明材料并加盖原厂公章或投标专用章。  13、兼容主流数据库达梦数据库、金仓数据库；提供互认证明文件并加盖原厂公章或投标专用章； | 套 | 2 |
| 10 | IPSecVPN | 1、提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件加盖原厂公章或投标专用章。  2、支持SM2、SM3、SM4算法，具有签名验签、身份认证等功能。  3、加解密吞吐率≥2000Mbps，每秒新建连接数≥90。 | 套 | 2 |
| 11 | 智能密码钥匙 | 1、提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件加盖原厂公章或投标专用章。  2、SM4加/解密速率为≥110Kbps；SM2密钥对生成速率为15对/秒，加/解密速率≥36Kbps/24Kbps，签名速率≥50次/秒，验签速率≥40次/秒；SM3运算速率≥320Kbps。 | 套 | 4000 |
| 12 | 浏览器密码模块 | 1、由浏览器内核、SSL安全协议模块、渲染进程、插件进程等组成。  2、支持SM2、SM3、SM4算法，与Web服务器之间建立安全通道，实现Web网页安全访问功能。  3、支持360浏览器。 | 套 | 100 |
| 13 | 门禁管理系统 | 1、提供国家密码管理局商用密码检测中心颁发的商用密码产品认证证书复印件加盖原厂公章或投标专用章。  2、采用国产密码算法，遵循中华人民共和国密码行业标准《GM/T0036—2014采用非接触卡的门禁系统密码应用技术指南》以及国家密码局《重要门禁系统密码使用指南》规范要求。  3、采用国产密码算法对门禁数据进行完整性保护。  4、对重要人员身份信息进行保护。  5、系统具备日记审计功能，操作日志具备完整性验证与保护功能。  6、生物识别+国密读卡多识别方式组合。  单门门禁控制器：  7、支持国密CPU卡读卡器读卡功能。  8、支持语音提示功能。支持单门单向控制。  9、支持多门互锁功能。  10、支持火警接入与输出；匪警接入与输出。  11、数据保存：断电状态可保存10年。  12、联网方式：支持Wiegand（韦根）协议、RS485、RS232、TCP/IP。  13、支持多种报警功能：胁迫报警功能，读非法卡报警功能，开门超时报警功能等。  14、身份识别方式：刷卡、刷卡+密码、单人单卡、刷卡（+密码）+双生物识别、刷卡（+密码）+本地（远程）授权。  人脸国密机：  15、提供商用密码产品型号认证证书复印件加盖原厂公章或投标专用章；  16、采用基于SM1的对称加解密技术实现门禁用户身份鉴别；  17、识别方式：国密读卡+人脸+指纹；  18、配置卡密钥更新。  19、包含1套国密CPU卡读卡器、国密发卡器、密钥发卡体系、门禁网关、出门开关。2把单门磁力锁。10张国密CPU卡。 | 套 | 1 |
| 14 | 基于国密算法的安全视频监控系统 | 1、产品支持8路视频接入；  2、内置国密安全芯片，支持SM1/SM2/SM3/SM4算法；  3、至少支持8路1080P视频接入；  4、支持UDP协议，兼容H.264和H.265编码协议；  5、支持对符合GB/T28181的视频流进行传输的机密性保护；  6、支持对NVR存储的视频数据进行机密性保护；  7、支持对视频流进行传输的完整性保护；  8、对视频监控记录进行存储完整性保护；  9、存储支持不少于120天。 | 套 | 1 |
| **三** | **安防监控系统与门禁** |  |  |  |
| **安防监控系统** | | |  |  |
| **主楼** | | |  |  |
| 一）主楼8楼 | | |  |  |
| 1 | 200万高清网络防暴半球 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：≤0.002Lux(彩色模式);≤0.0002Lux(黑白模式);≤0Lux(补光灯开启)；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离50米，最大暖光监控距离15米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67、IK10防护等级；  15、支持人脸侦测功能，可对经过设定区域的行人进行人脸检测,当栓测到人脸后,可联动抓拍人脸图片、录像及给出报警提示；  16、支持对齐刘海遮挡眉毛、头发遮挡眼镜、戴眼镜、戴帽子、戴头戴式耳机、半边人脸、戴口罩、侧脸方式的人脸进行检测；  17、可对出现在监控场景内的两眼瞳距不小于12像素的人脸进行检测，同时叠加目标提示框。 | 台 | 3 |
| 二）主楼1楼 | | |  |  |
| 1 | 200万高清网络防暴半球 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：≤0.002Lux(彩色模式);≤0.0002Lux(黑白模式);≤0Lux(补光灯开启)；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离50米，最大暖光监控距离15米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67、IK10防护等级；  15、支持人脸侦测功能，可对经过设定区域的行人进行人脸检测,当栓测到人脸后,可联动抓拍人脸图片、录像及给出报警提示；  16、支持对齐刘海遮挡眉毛、头发遮挡眼镜、戴眼镜、戴帽子、戴头戴式耳机、半边人脸、戴口罩、侧脸方式的人脸进行检测；  17、可对出现在监控场景内的两眼瞳距不小于12像素的人脸进行检测，同时叠加目标提示框。 | 台 | 4 |
| 三）主楼负1楼 | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 13 |
| 2 | 枪机支架 | 定制 | 套 | 13 |
| 3 | 400万高清网络球机 | 1、内置GPU芯片，支持深度学习算法，有效提升检测准确率；  2、支持人脸检测；支持优选；支持抓拍；支持上报最优的人脸抓图；支持人脸增强，支持人脸属性提取，不低于6种属性8种表情；  3、支持绊线入侵、区域入侵、穿越围栏、徘徊、物品遗留、物品搬移、快速移动、停车、人员聚集检测；支持人车分类报警；支持联动跟踪；  4、支持不低于32倍光学变倍，16倍数字变倍；  5、采用不低于400万像素1/2.8英寸CMOS传感器；  6、支持超星光级超低照度，不低于彩色：0.005Lux@F1.6，黑白：0.0005Lux@F1.6；  7、支持H.265编码，实现超低码流传输；  8、内置不低于150米红外灯补光，30米暖光灯补光，采用倍率与补光灯功率匹配算法；  9、支持报警联动白光警戒，对目标进行跟踪；  10、水平方向360°连续旋转，垂直方向-20°～90°自动翻转180°后连续监视,无监视盲区；  11、支持不少于300个预置位，8条巡航路径，5条巡迹路径；  12、支持不少于1路音频输入和1路音频输出；  13、内置不少于2路报警输入和1路报警输出，支持报警联动功能；  14、支持IP66防护等级，6000V防雷、防浪涌和防突波保护；  15、支持DC24V±25%宽电压输入。 | 台 | 2 |
| 4 | 球机吊装支架 | 定制 | 套 | 2 |
| **南楼** | | |  |  |
| 一）南2楼 | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 2 |
| 2 | 枪机支架 | 定制 | 套 | 2 |
| 二）南3楼 | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 3 |
| 2 | 枪机支架 | 定制 | 套 | 3 |
| 三）南4楼 | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 3 |
| 2 | 枪机支架 | 定制 | 套 | 3 |
| 四）南5楼 | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 3 |
| 2 | 枪机支架 | 定制 | 套 | 3 |
| 五）南6楼 | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 3 |
| 2 | 枪机支架 | 定制 | 套 | 3 |
| 六）南7楼 | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 3 |
| 2 | 枪机支架 | 定制 | 套 | 3 |
| 七）南8楼 | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 3 |
| 2 | 枪机支架 | 定制 | 套 | 3 |
| **北楼** | | |  |  |
| 一)北6楼 | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 1 |
| 2 | 枪机支架 | 定制 | 套 | 1 |
| **外围** | | |  |  |
| 1 | 200万高清网络枪机 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：0.002Lux(彩色模式);0.0002Lux(黑白模式);0Lux(补光灯开启)，电动变焦，镜头焦距：6mm~24mm；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离100米，最大暖光监控距离30米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、≥1个电源返送接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67；  15、支持自动聚焦、一键聚焦，可通过IE浏览器在预览画面框选出聚焦区域，以该区域作为参考区域聚焦；  16、同一静止场景相同图像质量下，设备在H.265编码方式时，开启智能编码功能和不开启智能编码相比，码率节约90%；  17、具有宽动态自动切换功能，在环境亮度变化时,可自动进行关闭/开后切换；  18、应具有自动白平衡功能，当使用环境实际色温在2800K-10000K范围内变化时，应能自动或手动调整白平衡，使输出图像准确重现出观察场景的实际色彩。 | 台 | 5 |
| 2 | 枪机支架 | 定制 | 套 | 5 |
| 3 | 800万全景网络摄像机 | 1、传感器：不低于1/1.8英寸CMOS；  2、像素：全景：不低于800万；球机：不低于400万；  3、最大分辨率：不低于4096×1800；  4、最低照度：全景：不低于0.0005Lux（彩色模式）；不低于0.0002Lux（黑白模式）；球机：不低于0.001LuxF1.4（彩色模式）；不低于0.0005LuxF1.4（黑白模式）；0Lux（红外灯开启）；  5、最大补光距离：全景：NA；球机：≥400米；  6、镜头类型：全景：定焦球机：变焦；  7、镜头焦距：全景：2.8mm球机：5.5mm～220mm；  8、周界防范：绊线入侵；区域入侵；停车检测；  9、人脸识别：全景NA球机NA；  10、视频压缩标准：H.265；H.264；H.264H；H.264B；MJPEG（仅辅码流支持）；  11、智能编码：H.264:支持；H.265:支持；  12、宽动态：全景：120dB；球机：120dB；  13、透雾功能：全景：NA；球机：光学透雾；  14、报警事件：无SD卡；SD卡空间不足；SD卡出错；网络断开；IP冲突；非法访问；动态检测；视频遮挡；绊线入侵；区域入侵；停车检测；场景变更；音频异常侦测；电压检测；外部报警；人脸识别；视频结构化；安全异常；人群拥堵、车辆拥堵、停车上限；  15、接入标准：ONVIF（ProfileS/ProfileG/ProfileT）；CGI；GB/T28181（双国标）；GA/T1400（只有中文带人脸或结构化才有）；GB/35114；  16、最大MicroSD卡：不低于512GB；  17、RS-485接口：不低于1个（波特率范围:1200bps~115200bps）；  18、音频输入：不低于2路（接线端子）；  19、音频输出：不低于2路（接线端子）；  20、报警输入：不低于7路（湿节点,支持直流3V~5V电位,5mA电流）；  21、报警输出：不低于3路（干节点,支持直流最大30V电位,1A电流/交流最大50V电位,0.5A电流）；  22、模拟输出接口：不低于1路（CVBS输出BNC接口）；  23、供电方式：DC36V；  24、防护等级：IP66。 | 台 | 2 |
| 4 | 弱电箱 | 定制 | 个 | 2 |
| 5 | 电源避雷器 | 二级防护，与被保护设备匹配。 | 个 | 2 |
| 6 | 200万高清网络防暴半球 | 1、支持三种智能资源切换：通用行为分析、人脸检测、人数统计；  2、支持人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光；  3、支持智能侦测：区域入侵，绊线入侵，快速移动（可人车分类及精准检测），物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，热度图；  4、支持声光报警联动，当报警产生时，可触发联动声音警报和灯光闪烁；  5、支持人数统计：支持进入/离开人数统计，并可生成人数统计日/月/年报表，导出使用；支持排队管理；支持区域内人数统计；  6、采用星光级低照度不低于200万像素1/1.8英寸CMOS图像传感器，最低照度：≤0.002Lux(彩色模式);≤0.0002Lux(黑白模式);≤0Lux(补光灯开启)；  7、最大可输出不低于200万(1920×1080)@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、内置高效暖光灯和红外补光灯，最大红外监控距离50米，最大暖光监控距离15米；  10、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  11、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  12、内置GPU芯片，靶面尺寸1/1.8英寸，具有≥1个RJ45接口、≥2个报警输入接口、≥2个报警输出接口、≥1个音频输入接口、≥1个音频输出接口、内置扬声器；  13、支持DC12V/POE供电方式；  14、支持IP67、IK10防护等级；  15、支持人脸侦测功能，可对经过设定区域的行人进行人脸检测,当栓测到人脸后,可联动抓拍人脸图片、录像及给出报警提示；  16、支持对齐刘海遮挡眉毛、头发遮挡眼镜、戴眼镜、戴帽子、戴头戴式耳机、半边人脸、戴口罩、侧脸方式的人脸进行检测；  17、可对出现在监控场景内的两眼瞳距不小于12像素的人脸进行检测，同时叠加目标提示框。 | 台 | 5 |
| 7 | 1拖2针孔网络摄像机盒子 | 1、内置GPU芯片，支持深度学习算法，有效提升检测准确率；  2、支持智能资源切换：通用行为分析、人脸检测；  3、支持不少于2路同时开启人脸检测：支持跟踪，支持优选，支持抓拍，支持上报最优的人脸抓图，支持人脸增强，人脸曝光，支持人脸属性提取，支持不少于6种属性；  4、支持不少于1路通用行为分析：绊线入侵，区域入侵，快速移动，物品遗留，物品搬移，徘徊检测，人员聚集，停车检测，人脸检测，人数统计；  5、支持二码流功能；  6、采用星光级低照度不少于200万像素1/2.8英寸CMOS图像传感器，低照度效果好，图像清晰度高；  7、最大可输出不少于2路200万1920×1080@25fps；  8、支持H.265编码，压缩比高，实现超低码流传输；  9、支持走廊模式，宽动态，3D降噪，强光抑制，背光补偿，数字水印，适用不同监控环境；  10、支持ROI，SMARTH.264/H.265，灵活编码，适用不同带宽和存储环境；  11、支持报警不少于2进2出，音频1进1出，485，最大支持256GMicroSD卡；  12、支持DC12V/POE供电方式，方便工程安装。 | 台 | 3 |
| 8 | 200万定焦针孔网络摄像机（方锥） | 1、采用星光级低照度不少于200万像素1/2.8英寸CMOS图像传感器；  2、最大可输出不少于200万像素1920×1080@25fps；  3、分离式针孔镜头，搭配盒子使用。 | 个 | 5 |
| **门禁系统** | | |  |  |
| 1 | 门禁控制器 | 1、安装方式：明装；  2、报警输入：不少于6路（开关量）；  3、报警输出：不少于4路（继电器）；  4、门锁控制：不少于2路，默认常开；  5、门状态检测：不少于2路；  6、非法卡超次报警：支持；  7、主处理器：高性能嵌入式处理器；  8、防反潜：支持；  9、非法闯入报警：支持；  10、开门模式：支持刷卡/远程/密码/指纹开门模式；  11、远程验证：支持；  12、黑白名单设定：支持；  13、多门互锁：支持；  14、网络协议：TCP;UDP;IPv4；  15、OSDP协议：支持；  16、是否支持SDK和API：支持；  17、外壳材料：SECC钢板；  18、多重认证：支持；  19、用户容量：不少于100000个用户；  20、指纹容量：不少于3000枚；  21、卡片容量：不少于100000张；  22、存储记录数量：不少于500000条。 | 台 | 26 |
| 2 | 读卡器 | 1、蓝色背光效果；  2、支持卡、卡+指纹、指纹、卡或指纹四种身份识别模式；  3、非接触式读卡，可读取Mifare卡（IC卡）卡号、CPU序列号、身份证序列号；  4、读卡频率13.56MHz；  5、指纹模块支持手指平面360度识别，1：N指纹验证，指纹容量最大可存储3000枚；  6、指纹认证响应时间≤0.5s，指纹识别时间≤1.5s；  7、指纹认假率（FAR）≤0.00004％，指纹拒真率（FRR）≤0.15％；  8、具有双通讯协议设计，同时支持RS485协议；  9、支持在线升级，升级失败可重新升级；  10、支持防拆报警，内置看门口狗程序，能够检控设备的异常运行状态，并执行修复处理，确保设备长期运行；  11、所有连接端口均具备过流和过压保护；  12、工作温度：-10℃～＋55℃，工作湿度：≤95%。 | 台 | 52 |
| 3 | 发卡器 | 支持IC卡(Mifare卡)的发卡。 | 台 | 1 |
| 4 | 电插锁 | 1、光电控制技术，防止机械故障；  2、超低温设计，更安全更耐用；  3、超低功耗设计，更耐用更环保；  4、50万次通电老化测试；  5、内置反向电流保护电路；  6、采用微处理芯片控制电路；  7、高强度铝合金锁体，不绣钢锁舌；  8、延时设置：0/3/6/9秒可调。 | 台 | 43 |
| 5 | 电插锁电源 | DC12V/2A | 个 | 43 |
| 6 | 单门磁力锁 | 定制 | 套 | 7 |
| 7 | 磁力锁电源 | DC12V/2A | 个 | 7 |
| 8 | 磁力锁支架（ZL型） | 定制 | 套 | 5 |
| 9 | 出门按钮 | 定制 | 个 | 52 |
| 二)存储系统 | | |  |  |
| 1 | 网络视频存储 | 1、操作系统：嵌入式操作系统；  2、主处理器：64位高性能多核处理器；  3、控制器：单控制器；  4、高速缓存：不低于8GB，可扩展至128GB；  5、网络接口：不低于1个千兆管理电口，4个千兆数据电口；  6、视频直存（私有协议）：最大支持不低于400路（800Mbps）前端接入、存储、转发，32路（64Mbps）网络回放；  7、硬盘接口：不低于48个，SATA，单盘最大支持不低于16TB，支持热插拔，支持CMR；  8、具有液晶屏提示、报警指示灯提示、SNMPTrap、声音提示、Email报警等报警方式，可对IP冲突、网口降速、电源故障、风扇故障、无硬盘、存储错误、存储空间满、RAID异常、录像丢帧、Mac冲突、登陆锁定、网络安全异常、SSD健康异常、无热备盘等情况进行报警；  9、整机默认支持1个千兆管理电口，4个千兆数据电口，可选配扩展支持电口或光口；  10、最大支持不低于400路（800Mbps）前端接入、存储、转发，32路（64Mbps）网络回放；  11、接入支持ONVIF、GB28181、主动注册等协议接入，保障了对不同厂家前端设备的兼容性；  12、支持JBOD、RAID0/1/5/6/10/50/60、SRAID支持全局热备和局部热备；  13、支持视频流直存，减少流媒体服务器的成本；  14、支持存储配额管理，支持基于通道的维度进行存储周期管理；  15、支持通用存储协议：ISCSI/SAMBA/NFS/FTP；  16、针对关键重要的视频，提供对实时流和历史视频进行加锁，确保不被循环覆盖；  17、配套支持统一云管理节点；  18、支持N+M模式下的视频和图片集群功能；  19、主机支持专用的存储硬盘，可升级专用硬盘固件，支持实时监测专用硬盘的健康状态；  20、可对被监测的硬盘健康状态进行分级分类，类别包含“硬盘良好状态”、“硬盘告警状态”、“硬盘错误状态”、“硬盘即将损坏”和“硬盘损坏状态”；  21、主机单控可通过更换板卡方式可支持不低于13个千兆电口，或者9个千兆电口+4个万兆光口,或者11个千兆电口+2个万兆光口主机可采用双控制器结构，双控制器结构最多支持26个千兆电口，或者10个千兆电口+8个万兆光口,或者18个千兆电口+4个万兆光口；  22、支持对用户操作设备过程中涉及到的敏感数据采用数字信封技术加密后在网络中传输，提供公安部及下属检测机构有效检测报告复印件加盖原厂公章或投标专用章;  23、设备支持配置文件和数据导出功能，且支持配置文件和数据加密导出；提供公安部及下属检测机构有效检测报告复印件加盖原厂公章或投标专用章。  24、存储支持不少于120天 | 台 | 1 |
| 2 | 8T硬盘 | 8TB，256MB，7200RPM | 块 | 30 |
| 三)非结构化管理平台 | | |  |  |
| 1 | 视频国标网关扩容模块 | 1、支持加密狗授权机制；  2、支持Web方式访问、配置、管理网关设备；  3、支持多平台多层次级联，跨域互联互通与资源共享；  4、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；  5、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；  6、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；  7、支持至少3级级联部署，最大可支持16个外域的接入；  8、不少于2000路授权接入。 | 个 | 1 |
| 2 | 视频监控融合对接平台 | 1、软硬件一体化。  2、支持加密狗授权机制。  3、支持Web方式访问、配置、管理网关设备。  4、支持多平台多层次级联，跨域互联互通与资源共享。  5、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。  6、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。  7、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。  8、支持至少3级级联部署，最大可支持16个外域的接入。  9、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（包括海康、科达、宇视、大华、天地伟业等）视频监控系统的接入。  10、支持不少于2万路视频级联和汇聚。  11、可接入全省法院其他厂家视频资源，推送至最高法平台。  12、支持平台上下级联网络拓扑，支持展示级联的连接、数据推送状态的展示，提供公安部及下属检测机构有效检测报告复印件加盖原厂公章或投标专用章；  13、支持外置安全数据库，可切换至不同安全等级的数据库，提供不同等级的数据存储、传输和计算加密，提供公安部及下属检测机构有效检测报告复印件加盖原厂公章或投标专用章； | 台 | 1 |
| **四、科技法庭升级改造** | | |  |  |
| 一）科技法庭（新增1套法庭设备） | | |  |  |
| 1 | 签名+捺印(手持终端) | 1、屏幕显示率≥1280×800；  2、面板LED寿命≥30000小时；  3、输入端口和接口支持USB2.0；  4、采用电容式传感器式指纹识别技术，具有活体指纹探测功能，指纹录入时间应<1s。 | 台 | 1 |
| 2 | 庭审输出设备 | 1、分辨率：不低于1920×1080；  2、刷新率：不低于60HZ；  3、亮度：不低于250cd/m2；  4、对比度：不低于1000：1；  5、可视角度：不低于178°/178°；  6、支持不低于10点触控。 | 台 | 4 |
| 3 | 一体机 | 1、CPU和操作系统：通过中国信息安全测评中心测评的产品（提供中国信息安全测评中心官网截图加盖原厂公章或投标专用章）。；  2、屏尺寸不小于21.5寸；  3、支持≥256G固态硬盘；  4、内存支持≥8G；  5、支持视频双输出接口；  6、DVD刻录光驱；  7、还可以支持2560\*1080分辨率。 | 台 | 3 |
| 4 | 庭审电脑 | 1、CPU和操作系统：通过中国信息安全测评中心测评的产品（提供中国信息安全测评中心官网截图加盖原厂公章或投标专用章）。；  2、支持≥256G固态硬盘；  3、内存支持≥8G；  4、支持视频双输出接口；  5、DVD刻录光驱。 | 台 | 2 |
| 5 | 展台 | 1、像素：不低于1800万；  2、分辨率：不低于4800×3600以上；  3、图像色彩：不低于24位；  4、USB类型：USB2.0；  5、光源：自然光+LED补光+侧补光；  6、输出接口：HDMI、USB。 | 台 | 2 |
| 6 | 千兆交换机 | 自适应千兆口\*16 | 台 | 1 |
| 7 | 庭审主机 | 基础模块：  1.19"标准单一机箱，设备高度不大于2U；  2.使用国产处理器，主频≥1.4GHz，提供第三方检验报告并加盖原厂公章或投标专用章； | 模块 | 1 |
| 视频矩阵模块：  1.不低于6路高清SDI数字视频摄像机接入；  2.不低于6路证据信号接入，支持VGA/DVI/HDMI等不同信号类型输入；  3.不低于4路高清信号输出，支持VGA/HDMI输出；  4.具备内置矩阵，支持多路信号的同步切换，支持1080P高清以及1280x1024信号。 | 模块 |
| 语音模块：  1.内置音频矩阵，支持多路音频信号的同步切换；  2.不低于11路麦克风接入端口，提供48V幻象电源支持；（提供CMA或CNAS标志的检验报告并加盖原厂公章或投标专用章）  3.支持语音激励功能，自动将对准发言人的摄像机画面切换到画面分割模式中的主画面窗口；  4.每路输入具有平衡/非平衡处理、+48V幻象电源供电开关、支持激励灵敏度调节、音量调节；  5.不少于5路线路音频专用输入接口，用于证据输入；  6.线路音频输入需支持自动混音，并可进行音量调节；  7.不少于4路音频信号输出端口；  8.每路输出都带有音量调节、静音调节、均衡器、延时等功能；（提供CMA或CNAS标志的检验报告并加盖原厂公章或投标专用章）  9.内置多端口数字音频处理器，避免回授啸叫现象，支持回声消除、自动降噪、保持足够音量和良好音质；支持远程三方庭审模式；（提供CMA或CNAS标志的检验报告并加盖原厂公章或投标专用章）  10.支持本地/远程音频切换混音处理；  11.支持每支话筒独立音频PCM编码，提供第三方检验报告并加盖原厂公章或投标专用章；  12.内置2通道100W高保真专业级音频功放，满足中小法庭扩声应用，减少外围设备配置，提供第三方检验报告并加盖原厂公章或投标专用章。 | 模块 |
| 画面融合模块：  1.具备硬件高清分割图像合成器，可提供2/4/6/8等多种合成画面格式，合成画面分辨率不低于1080P；  2.分割输入信号需支持3G/HD-SDI、VGA、YPbPr、YCbCr、DVI等不同信号混合进行画面合成；  3.高清画面分割器可同时支持输出不少于2路不同分割模式的合成画面； | 模块 |
| 集中控制模块：  1.具备全双工可编程RS-232端口，端口数不少于2路；  2.具备全双工可编程RS-485端口；  3.可连接强电开关控制器、控制面板等多种集控设备；  4.具备自适应网络RJ45接口；  5.可通过网络采用浏览器以WEB页面方式对主机进行远程控制、管理、系统升级；  6.具备内置硬盘，可提供主机庭审数据备份功能；  7.庭审主机具备扩展语音识别采集功能模块；  8.不增加外设的情况下，同时支持RSTP协议和H.323协议。 | 模块 |
| 远程庭审模块：  1.支持不低于4路1080P格式同时编码输出，支持高清证据图像编码，码流速率可设，提供第三方检验报告并加盖原厂公章或投标专用章；  2.支持不低于2路远程1080P格式解码能力，可用于远程提讯、远程三方庭审（嫌疑人、公诉人均在远端），提供第三方检验报告并加盖原厂公章或投标专用章；  3.输出格式：符合最高院要求的H.264编码，符合最高院要求的MPEG4文件存放格式；  4.音视频完全同步，直播延时小于200毫秒（LAN内）。  5.支持法庭纪律播报：内置法庭纪律播报功能，分担书记员庭前准备工作，默认可选男声版本或女声版本，提供第三方检验报告并加盖原厂公章或投标专用章。 | 模块 |
| 8 | 画面切换面板（含底座） | 8键可编程输入控制面板，产品每个按键功能可自定义，与MCP或中控主机配合使用。 | 套 | 1 |
| 9 | 旁听辅助支持硬件 | 不小于2G内存，用于安装旁听辅助模块。 | 个 | 1 |
| 10 | 球机 | 1、不低于200万像素；  2、支持不低于20倍光学变倍；  3、焦距:4.7-94mm；  4、水平视角：58.3-3.2度；  5、支持Smart功能；  6、支持VISCA控制协议支持遥控器控制支持重力感应；  7、支持DVI-I(可转HDMI、YPbPr输出)、网口、BNC(DB15口转出)、HD-SDI输出；  8、支持人脸马赛克和变声；  9、DC12V供电。 | 个 | 4 |
| 11 | 音响 | 1、系统类型：4×4寸全频音箱；  2、灵敏度(1W/1m)：不低于96dB；  3、频率响应：140Hz~18kHz(-10dB)；  4、额定功率(AES)：160W；  5、最大声压级(连续/峰值)：118dB/124dB；  6、标称覆盖角(H×V)：80°×30°；  7、标称阻抗：8Ω；  8、全频单元：4×4"(1"音圈)；  9、连接件：2×SPEAKON四芯音箱插座1+1-；  10、吊挂硬件：2×M8吊点。 | 个 | 4 |
| 12 | 强电控制器 | 1、不低于8通道电源时序打开/关闭；  2、远程控制（上电+24V直流信号）；  3、不低于8通道电源时序打开/关闭—当电源开关锁处于off位置时有效；  4、当远程控制有效时同时控制后板ALARM（报警）端口导通—起到级联控制ALARM（报警）功能；  5、单个通道最大负载功率不低于3500W，所有通道负载总功率不低于6000W；  6、输入连接器：大功率电源连接器；  7、输出连接器：不低于4个16A电源插座和4个10A电源插座；  8、额定输出电压:AC220V/50Hz额定输出电流:30A可控制电源:8路每路动作延时时间:1秒供电电源:VAC220V50/60Hz30A单路额定输出电源:≥16A。 | 台 | 1 |
| 13 | 高清矩阵 | 1. 不低于8路HDMI视频输入，16路HDMI输出，完全交叉切换； 2. 支持高清1080P、支持3D、支持4K； 3. 长线输入自动均衡——确保能对每个输入进行独立的自动的补偿由于长距离传输或者使用低质量线村造成的信号损耗； 4. 在理想的环境下，标准线缆支持输入距离不低于25米，输出距离不低于40米；带放大器的线缆支持输入距离不低于50米，输出距离不低于80米。 5. 支持蓝光DVD24/50/60fs/HD-DVD/xvYCC。 6. 支持音频格式DTS-HD/Dolby-trueHD/LPCM7.1/DTS/DOLBY-AC3/   DSD。  7.支持HDMI1.3a、HDCP1.3、HDCP1.4、以及DVI1.0协议。支持高色深，以及高达6.5Gbps速率；  8.HDCP兼容——确保有内容保护的媒体能正常显示与其它HDCP兼容设备的协同使用；  9.全贴片SMD工艺，特有ESD静电保护功能；  10.本产品带有断电现现场切换记忆保护；  11.具有不低于2路RS-232通讯接口；支持RS-232转RS-485通信接口；  12.不低于8路全解密HDCP，可以通过所有格式的HDMI信号；  13.可以同时支持8路蓝光播放器的HDMI信号输入；  14.自动读取保存EDID，适合所有品牌的显示设备；  15.支持高清分辨1024\*768---2048\*1600，支持1080P，支持3D；  16.高亮蓝光液晶显示屏，铝拉丝面板材质；  17.宽幅电源110-240V，双串口设置，配置一个网口；  18.支持高清1080P、支持3D、支持4K；  19.接口：HDMI-D母接口。 | 台 | 1 |
| 14 | 电视 | 1、屏幕尺寸不小于65英寸；  2、具备HDMI接口；  3、分辨率：3840×2160。 | 台 | 2 |
| 15 | 庭前展示机 | 1、视频接口：标准HDMI1.3，2.5mm复合视频输出、音频接口：数字音频输出、网络接口：以太网RJ45接口，10M/100M自适应、WIFI802.11b/g/n  其它接口：USB接口，SD卡，SATA硬盘接口,HDMI接口；  2、最大分辨率不低于1920\*1080；  3、最大色深不低于24bit；  4、画板类型不低于32”LEDPanel；  5、显示尺寸不低于698×394.0mm(W\*H)；  6、显示比例16:9；  7、背光类型CCFL；  8、分辨率1920×1080或1366×768；  9、显示色彩不低于16.7M；  10、亮度不低于400cd/m2对比度4000:1；  11、可视角度175°(H)/175°(V)；  12、使用寿命不低于60000小时；  13、电源输入AC100V～240V电源功耗≤65W待机功耗≤3W；  14、展示法庭当前及后续排期及相关案件信息、支持当前法庭庭审直播画面。 | 台 | 1 |
| 16 | ups | 主机电池一体，内置电池断电支持时间30分钟。 | 台 | 1 |
| 17 | 辅材线缆 | 包含法庭线缆，布线等。 | 项 | 1 |
| 18 | 功放 | 1、8Ω立体声功率：100W×24Ω；  2、立体声功率：50W×2；  3、频响范围：20Hz-20KHz+/-1dB；  4、输入阻抗：20KΩ(平衡)/10KΩ(不平衡)。 | 台 | 1 |
| 19 | 话筒 | 1、类型：鹅颈式会议话筒；  2、换能方式：电容式；  3、指向性：心形单指向性；  4、频率响应：50Hz-20KHz；  5、灵敏度：不低于20mV/Pa(-50dBV)；  6、信噪比：﹥62dB；  7、最大承受音压：不低于120dB；  8、输出阻抗：200Ω±30%；  9、电流消耗：4mA幻象供电。 | 个 | 9 |
| 20 | 打印机 | 1、类型：彩色激光打印机；  2、最高分辨率：600×600dpi以上；  3、打印速度：A4黑白/彩色21页/分钟；  4、纸张容量：不低于250页进纸盒；  5、内存：不低于256MBDDR，256MBNAND闪存；  6、接口：高速USB2.0端口，内置高速以太网10/100Base-TX网络端口。 | 台 | 1 |
| 21 | 庭审专用支架 | 定制显示器可调节支架 | 台 | 4 |
| 二）互联网法庭7套 | | |  |  |
| 1 | 互联网庭审音视频交互网关 | 1、支持≥9个互联网端庭审参与人同时参与庭审；  2、支持CIF/720P/1080P多分辨率显示，支持软编软解功能；  3、支持≥1路本地信号的编码,分辨率不低于640x480；  4、音视频交互时，可以根据网络带宽自己调节编码参数，以达到流畅的效果；  5、支持≥4路DVI输出接口；  6、每个接口输出的画面可控制；  7、支持≥2路DVI信号采集；  8、支持≥1路音频的输入；  9、支持≥1路音频输出；  10、支持自动同步系统时间功能，支持控制系统硬件/软件重启功能；  11、支持其他厂家标准庭审主机接入功能，支持RTSP和互联网协议实时互转功能；  12、支持将解码的互联网端当事人声音的混音或独立输出。 | 台 | 7 |
| 2 | 光端机 | 支持HDMI/DVI信号输入/输出，支持平衡音频输入/输出。 | 对 | 14 |
| **五** | **电源部分** |  |  |  |
| 1 | 模块化UPS | 1、模块化UPS类型为在线式双变换式，制式为三相输入，三相输出，主机容量不小于120KVA。  2、单功率模块的额定输出功率应介于20kVA-40kVA之间，并支持热插拔，当功率模块故障时，应及时退出系统而不能影响其他模块正常工作，不允许输出中断。  3、输入电压范围（Vac）：138-485VAC；线电压305V-485V支持满载。  4、额定频率（Hz）：50Hz/60Hz。  5、输入频率范围（Hz）：40Hz-70Hz。  6、输入功率因数：>0.99满载。  7、输出电压波形畸变率：<1%(100%线性载）<3%（100%非线性载）。  8、输出功率因数：1。  9、市电模式下，UPS系统效率在50%负载时应达到96%。ECO模式下，UPS系统效率应达到99%。  10、模块的风扇应有冗错设计。  ▲11、UPS系统的监控模块和功率模块应具有热插拔功能。提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  12、抗震性能：满足YD5096-2016《通信用电源设备抗震性能检测规范》的要求。提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  13、UPS系统应支持电池节数可调，具有定期对电池组进行自动浮充、均充转换、自动温度补偿、电池组放电及记录功能。  14、满载音频噪声不大于65dB；提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  15、UPS系统应具有人机交互性能，应支持中/英文界面，参数设置与人工操作应满足如下要求：1)参数设置：监控模块和参数设置开放，具备密码分级权限保护，设置参数支持掉电存储功能。2)人工操作：重要操作进行密码保护和警示提醒；异常情况下具备人工干预的操作方式。  ▲16.风扇故障时，应发出声光报警；提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  ▲17.输出负载短路时，系统应自动关闭输出，同时发出声光报警。提供具备检测资质的第三方机构出具的测试报告并加盖原厂公章或投标专用章；  ▲18.UPS系统应满足网络安全要求，通过网络安全认证，提供权威第三方机构产品社会公共安全认证证书复印件，并加盖原厂公章或投标专用章。 | 台 | 2 |
| 2 | 功率模块 | 1.单个UPS功率模块≥30kVA，高度≤3U；  ▲2.UPS功率模块具备智能休眠功能，需提供功能截图，并加盖原厂公章或投标专用章。 | 个 | 6 |
| 3 | 铅酸蓄电池 | 12V/200AH | 节 | 64 |
| 4 | 并机线缆 | 配套 | 套 | 1 |
| 5 | 电池开关箱 | 定制 | 套 | 2 |
| 6 | 输入输出线缆 | 配套 | 米 | 30 |

##### 表2：成品软件

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **序号** | **名称** | **子系统** | **技术参数** | **单位** | **数量** | **备注** |
| **一** | **科技法庭升级改造-智慧庭审** |  |  |  |  |  |
| 1 | 智慧庭审应用系统 | 笔录智能辅助制作模块 | 1.依据案件要素分析，根据案件类型、庭审的不同阶段，自动生成规范式笔录纲要；  2.将系统记录的案件基本信息以及根据对起诉材料信息进行智能提取，形成包含了首部、宣布法庭纪律、宣布开庭、核实当事人及诉讼代理人身份、宣布法庭组成人员和书记员名单、告知当事人有关的诉讼权利和义务、法庭调查、法庭辩论、最后陈述、法庭调解内容的全过程庭审笔录纲要内容；  3.纲要内容可一次插入笔录正文，也可以逐项进行插入，应用灵活、便捷，同时在质证阶段，结合业务特性支持多次将质证相关内容插入到庭审笔录；  4.通过笔录纲要能够快速定位笔录正文内容位置；  5.庭审系统集成了语音识别能力，能够自动识别庭审发言并转换成文字内容，生成的文字内容可直接插入正文使用，也可以选择性的进行插入。 | 模块 | 1 |  |
| 2 | 法律智能推送模块 | 1.在庭审阶段，通过对立案材料、实时笔录、语音识别等文本分析而获取的要素，向法官推送与本案相关的法律法规的法律条文，所推送的法律法规包括实体法律依据和程序法律依据；  2.在向法官推送相关法律法规的同时，展示被推送法律法规的引用次数和法律全文；  3.在自动推送之外，可通过法官输入相关检索词即可对法律法规进行快速定位，且支持快速模糊查询;  4.推送和查询的法条支持“一键”式、多格式的输出；  5.推送和查询的条文支持对关键字的高亮显示。 | 模块 | 1 |  |
| 3 | 案例智能推送模块 | 1.在庭审阶段，经过提供给法官针对法官当前案件相关案例；  2.在庭审阶段，通过对立案材料、实时笔录、语音识别文本分析而获取的要素分析，向法官推送与本案相关的案例，所推送的案例包括案例的全部内容，包括标题、当事人信息、案件由来、事实部分、本院认为、裁判结果等；  3.根据案件的要素推送出的条文支持对关键字的高亮显示；  4.系统具备相关案例查询功能，相关案例是指在案件的审理过程中，根据法官当前所审理案件的案由与案件类型自动推送与其相关的案例数据；  5.推送的相关案例应分为本院、本省和全国的案例分别显示。 | 模块 | 1 |  |
| 4 | 电子质证模块 | 1.在庭审阶段，实现法官对本案电子卷宗的全部材料，并进行实时查阅；  2.提供个人查阅功能，按最高人民法院档案管理要求形成的卷宗目录，按卷宗来源、正/副卷内容等多种查阅方式；  3.法官可以进行卷宗检索，也可以查看不同来源的卷宗材料，为法官进行网上电子阅卷提供最大的便利；  4.根据法官的庭审掌控节奏，以及诉讼参与人的质证应答结合语音识别的功能，当识别到证据名称时，系统自动进行智能匹配，并将最终匹配到的证据文件推送到审判长和诉讼参与人；  5.提及不同的证据名称，推送的电子证据也应随之改变；  6.在审判长及诉讼参与人提及的法律法规条目名称时，系统应推送出庭审发言识别结果相符的法律法规条文，自动审判长及诉讼参与人的显示端；  7.具备审判长控制庭审节奏的功能，审判长调阅电子证据进行质证同屏比对时，向诉讼参与人的显示端均需推送同样的信息内容画面。 | 模块 | 1 |  |
| 5 | 文书智能辅助制作模块 | 1.提供统一的“左看右写”的编辑界面，同一界面提供各类卷宗及文书的查看和复制粘贴等应用界面和文书编辑界面；  2.辅助支持生成程序性文书：系统可以支持刑事和民事一审、二审所涉及的程序性文书智能辅助生成；  辅助生成裁判文书：  3.根据案件的类别及要素分析，推送与案件相适应的文书模板供法官进行选择；  4.文书自动生成的内容应包括文书首部、当事人基本信息部分、案件由来及审理经过、诉称、辩称以及文书尾部，格式内容必须符合最高院对法律文书的格式要求，文书的审理查明、本院认为、裁判结果等内容需由承办人根据卷宗等相关内容进行人工编写；  5.向审判长提供备忘录功能，法官每个案件进行备忘录的新增、删除和修改操作。 | 模块 | 1 |  |
| 6 | 旁听辅助模块 | 1.庭前推送法庭及审判组成人员信息，包括姓名、性别、工作背景等信息；  2.庭中推送当事人身份身份信息、庭审人员名单信息，包括审判人员及合议庭组成人员名单及简介；  3.庭审中对当事人进行全力义务告知，展示当事人权利义务；  4.在法庭调查阶段以及法庭辩论阶段推送相关法条及普法常识；  5.在法庭质证阶段随审判人员节奏以此推送电子化证据信息；  6.在案件评议阶段展示合议庭信息以及当事人信息，在调解阶段展示当事人信息；  7.在宣判阶段推送判决时涉及法条以及案件信息公示的查询路径信息。 | 模块 | 1 |  |
| 7 | 电子签名捺印模块 | 1.与电子签名捺印系统融合，获取当事人电子手写签名及指纹并添加至系统中需签名、捺印位置，位置可根据实际情况调整 | 模块 | 1 |  |
| **以上有320个法庭授权。** | | | | | |  |
| 1 | 音视频综合管理模块 |  | 1、首页展示互联网开庭数据、远程开庭数据、扫黑除恶开庭数据、狱内数据，展示庭审排期、正在庭审、等待庭审、休庭、闭庭状态，展示海南法院地图。展示模式为饼状图、列表。数据可选今日、本月、本年数据。  2、子模块开庭公告：展示全省法院的庭审排期。包括互联网排期，远程开庭排期，本地排期。  3、子模块正在庭审:展示全省法院庭审直播信息，展示模式为框图和列表。视频可进行实时观看视频和笔录信息；  4、子模块庭审点播：展示全省法院的本地庭审、互联网庭审、远程庭审录音录像及笔录，可进行下载、收藏、推荐。  5、子模块法庭建设:展示全省法院的法庭建设情况；  6、子模块监控管理：监控各个法院服务器情况；  7、子模块法庭配置:配置全省法庭内容；  8、子模块巡回法庭：对接巡回法庭，展示排期，直播、点播功能；  9、子模块精品案件:展示精品案件；  10、子模块统计功能：统计法庭数量建设对比、法庭建设数量、数字法庭建设率、数字法庭建设数量对比；统计科技法庭接入情况；统计点击量top10案件；统计直播量top10案件；统计法院排名开庭数；统计法院排名，开庭数统计，开庭数量趋势，开庭与排期对比，开庭率，开庭率趋势；  11、子模块安防监控:可对接全省法院监控进行查看；  12、平台管理功能:用户管理、角色组管理、部门结构配置、单位结构配置、前置机管理、历史数据重传、流媒体服务器配置、日志管理、回收站等 | 套 | 1 |  |
| 2 | 智慧法庭综合支撑平台 | 法律支持模块 | 收录新中国成立以来现行有效与废止的法律、行政法规、司法解释、国务院部门规章，地方性法规、地方政府规章及司法文件。支持智能模糊查询、分类主题导引、主题词树查询、立法机关导引、法规目录查询、近日生效法规等主要功能及一些个性功能。  智能模糊查询不仅限于对关键词的检索，还会通过独有的智能查询技术，自动分析相同涵义的词语，进而尽可能地避免查询过程中的遗漏；系统的智能过滤功能会自动过滤掉干扰词句，从而删除垃圾条文，使查询结果更加准确，极大的提升了检索软件的实用性。  可按照法律部门设多层级法律主题词树，用户可以依使用需要将其逐级展开，查询具体某一方面的法律法规，方便而且快捷。用户所查询的结果均为条文显示，在结果集里系统会告知使用者所查询的结果数量，并且还可在法律文件中用窗口的方式显示，点击主题词即可链接到与该主题词相关的结果列表页面。现行系统设置了上千万个主题词窗口，链接数百万个法律条文。 | 模块 | 1 | 满足全省法院使用要求。 |
| 案例支持模块 | 收录最高人民法院指导案例、各省高院参考案例以及各省法院裁判文书。根据最高人民法院标准案由和相关司法文件，建立了案由主题词树，并自主加工整理四万余个下级案由主题,形成了全面、规范的案例数据和科学、严谨的案由分类，保证了查询的全面准确和高效便捷。包含智能模糊查询，案由主题查询，优秀司法文书查询，法律数据库，我的办公桌等功能。 | 模块 | 1 |
| 文本识别模块 | 通过最新的文字识别技术和端到端模型训练的经验积累提取了大量字符特征和模板特征，并建立了专业法院业务特征的模板库。 | 模块 | 1 |
| 语音识别模块 | 该模块能实现与海南法院现有语音识别系统对接，以配合应用系统提供智能化语音识别应用。 | 模块 | 1 |
| 分布式存储 | 具备良好的扩展性，文件系统管理的物理存储资源不直接与本地节点相连，而是分布于计算网络中的一个或者多个节点的计算机上。当客户端需要存储数据时，服务器指引其将数据分散的存储到多个存储节点上，以提供更快的速度，更大的容量及更好的冗余特性，同时也提高了系统的性能和可靠性。 | 模块 | 1 |
| 3 | 互联网庭审管理系统 |  | 部署在高院互联网区，用于统一管理全省互联网法庭数据 | 套 | 1 |  |
| **二** | **证券纠纷代表人诉讼服务系统** | |  |  |  |  |
| 1 | 证券纠纷代表人诉讼服务系统 | 证券纠纷代表人诉讼服务系统（当事人端） | 用户登录 | 套 | 1 | 满足全省法院使用要求。 |
| 2 | 代表人诉讼在线平台首页 | 套 | 1 |  |
| 3 | 公示公告信息 | 套 | 1 |  |
| 4 | 权利登记 | 套 | 1 |  |
| 5 | 代表人推选 | 套 | 1 |  |
| 6 | 调解草案异议 | 套 | 1 |  |
| 7 | 提起上诉 | 套 | 1 |  |
| 8 | 放弃上诉 | 套 | 1 |  |
| 9 | 退出诉讼 | 套 | 1 |  |
| 10 | 消息提醒 | 套 | 1 |  |
| 11 | 证券纠纷代表人诉讼服务系统（法官端） | 用户登录 | 套 | 1 |  |
| 12 | 启用代表人诉讼 | 套 | 1 |  |
| 13 | 公告公示 | 套 | 1 |  |
| 14 | 登记信息审核 | 套 | 1 |  |
| 15 | 代表人推选 | 套 | 1 |  |
| 16 | 第三方接口 | 对接法院统一身份认证系统接口 | 套 | 1 |  |
| 17 | 对接电子诉讼平台接口 | 套 | 1 |  |
| 18 | 对接审判系统接口 | 套 | 1 |  |
| 19 | 对接短信平台接口 | 套 | 1 |  |

##### **★**表3：定制开发软件

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **编号** | **功能模块** | **功能子模块** | **功能点名称** | **数量** | **单位** |
| 一、 | 海南法院智慧审判系统 |  |  |  |  |
| （一） | CA及密评要求设计 |  |  |  |  |
| 1 | 智慧审判系统密码改造 | 采用密码技术保证信息系统应用的访问控制信息的完整性 | 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制的密码技术对应用的访问控制信息进行完整性保护 | 1 | 项 |
| 2 | 采用基于公钥密码算法的数字签名机制的密码技术对应用的访问控制信息进行完整性保护 | 1 | 项 |
| 3 | 系统开发支持网关登录校验 | 1 | 项 |
| 4 | 系统管理员 | 1 | 项 |
| 5 | 安全保密管理员 | 1 | 项 |
| 6 | 安全审计员 | 1 | 项 |
| 7 | 采用密码技术保证信息系统应用的重要数据在存储过程中的机密性 | 重要数据采用密码技术的加密功能对该数据在存储过程中进行机密性保护 | 1 | 项 |
| 8 | 重要数据采用密码技术的解密功能对该数据在存储过程中进行机密性保护 | 1 | 项 |
| 9 | 采用密码技术保证信息系统应用的重要数据在存储过程中的完整性 | 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制的密码技术对重要数据在存储过程中进行完整性保护 | 1 | 项 |
| 10 | 采用基于公钥密码算法的数字签名机制的密码技术对重要数据在存储过程中进行完整性保护 | 1 | 项 |
| 11 | 采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性 | 安全审计日志采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为实现不可否认性 | 1 | 项 |
| 12 | 安全审计日志采用基于公钥密码算法的数字签名机制等密码技术对数据接收行为实现不可否认性 | 1 | 项 |
| 13 | 应用日志采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为实现不可否认性 | 1 | 项 |
| 14 | 应用日志采用基于公钥密码算法的数字签名机制等密码技术对数据接收行为实现不可否认性 | 1 | 项 |
| 15 | 开发基于安全管理员的日志完整性检查，检查日志是否完整 | 1 | 项 |
| 16 | 开发基于安全管理员的日志一致性检查，以判断日志是否被篡改过 | 1 | 项 |
| 二、 | 海南法院智慧诉服业务 |  |  |  |  |
| （一） | CA及密评要求设计 |  |  |  |  |
| 1 | 电子诉讼系统密码改造 | 采用密码技术保证信息系统应用的访问控制信息的完整性 | 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制的密码技术对应用的访问控制信息进行完整性保护 | 1 | 项 |
| 2 | 采用基于公钥密码算法的数字签名机制的密码技术对应用的访问控制信息进行完整性保护 | 1 | 项 |
| 3 | 系统开发支持网关登录校验 | 1 | 项 |
| 4 | 系统管理员 | 1 | 项 |
| 5 | 安全保密管理员 | 1 | 项 |
| 6 | 安全审计员 | 1 | 项 |
| 7 | 采用密码技术保证信息系统应用的重要数据在存储过程中的机密性 | 重要数据采用密码技术的加密功能对该数据在存储过程中进行机密性保护 | 1 | 项 |
| 8 | 重要数据采用密码技术的解密功能对该数据在存储过程中进行机密性保护 | 1 | 项 |
| 9 | 采用密码技术保证信息系统应用的重要数据在存储过程中的完整性 | 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制的密码技术对重要数据在存储过程中进行完整性保护 | 1 | 项 |
| 10 | 采用基于公钥密码算法的数字签名机制的密码技术对重要数据在存储过程中进行完整性保护 | 1 | 项 |
| 11 | 采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性 | 安全审计日志采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为实现不可否认性 | 1 | 项 |
| 12 | 安全审计日志采用基于公钥密码算法的数字签名机制等密码技术对数据接收行为实现不可否认性 | 1 | 项 |
| 13 | 应用日志采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为实现不可否认性 | 1 | 项 |
| 14 | 应用日志采用基于公钥密码算法的数字签名机制等密码技术对数据接收行为实现不可否认性 | 1 | 项 |
| 15 | 开发基于安全管理员的日志完整性检查，检查日志是否完整 | 1 | 项 |
| 16 | 开发基于安全管理员的日志一致性检查，以判断日志是否被篡改过 | 1 | 项 |
| 三、 | 海南法院智慧执行系统 |  |  |  |  |
| （一） | 智慧执行系统密码改造 |  |  |  |  |
| 1 | 智慧执行系统密码改造 | 采用密码技术保证信息系统应用的访问控制信息的完整性 | 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制的密码技术对应用的访问控制信息进行完整性保护 | 1 | 项 |
| 2 | 采用基于公钥密码算法的数字签名机制的密码技术对应用的访问控制信息进行完整性保护 | 1 | 项 |
| 3 | 系统开发支持网关登录校验 | 1 | 项 |
| 4 | 系统管理员 | 1 | 项 |
| 5 | 安全保密管理员 | 1 | 项 |
| 6 | 安全审计员 | 1 | 项 |
| 7 | 采用密码技术保证信息系统应用的重要数据在存储过程中的机密性 | 重要数据采用密码技术的加密功能对该数据在存储过程中进行机密性保护 | 1 | 项 |
| 8 | 重要数据采用密码技术的解密功能对该数据在存储过程中进行机密性保护 | 1 | 项 |
| 9 | 采用密码技术保证信息系统应用的重要数据在存储过程中的完整性 | 采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制的密码技术对重要数据在存储过程中进行完整性保护 | 1 | 项 |
| 10 | 采用基于公钥密码算法的数字签名机制的密码技术对重要数据在存储过程中进行完整性保护 | 1 | 项 |
| 11 | 采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性 | 安全审计日志采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为实现不可否认性 | 1 | 项 |
| 12 | 安全审计日志采用基于公钥密码算法的数字签名机制等密码技术对数据接收行为实现不可否认性 | 1 | 项 |
| 13 | 应用日志采用基于公钥密码算法的数字签名机制等密码技术对数据原发行为实现不可否认性 | 1 | 项 |
| 14 | 应用日志采用基于公钥密码算法的数字签名机制等密码技术对数据接收行为实现不可否认性 | 1 | 项 |
| 15 | 开发基于安全管理员的日志完整性检查，检查日志是否完整 | 1 | 项 |
| 16 | 开发基于安全管理员的日志一致性检查，以判断日志是否被篡改过 | 1 | 项 |
| 四、 | 海南法院智慧管理系统 |  |  |  |  |
| （一） | 智慧教学管理系统 |  |  |  |  |
| 1 | 教育培训管理后台 | 后台登录 | 管理员登录 | 1 | 项 |
| 2 | 后台登录验证功能/后台登录验证码功能 | 1 | 项 |
| 3 | 后台登录错误超次数账号锁定功能 | 1 | 项 |
| 4 | 多端登录设置 | 1 | 项 |
| 5 | 管理员管理 | 管理员信息 | 1 | 项 |
| 6 | 管理员的添加功能 | 1 | 项 |
| 7 | 管理员列表功能开发 | 1 | 项 |
| 8 | 管理员的修改功能 | 1 | 项 |
| 9 | 管理员的删除功能 | 1 | 项 |
| 10 | 角色（权限）管理 | 角色管理信息 | 1 | 项 |
| 11 | 角色列表功能 | 1 | 项 |
| 12 | 角色添加功能 | 1 | 项 |
| 13 | 角色的修改功能 | 1 | 项 |
| 14 | 角色的删除功能 | 1 | 项 |
| 15 | 角色的编码 | 1 | 项 |
| 16 | 角色的权限信息 | 1 | 项 |
| 17 | 角色的权限添加设置 | 1 | 项 |
| 18 | 角色的权限修改设置 | 1 | 项 |
| 19 | 角色的权限删除设置 | 1 | 项 |
| 20 | 角色权限查看 | 1 | 项 |
| 21 | 用户组管理 | 用户组信息 | 1 | 项 |
| 22 | 用户组的添加功能/用户组的修改功能/用户组的删除功能 | 1 | 项 |
| 23 | 用户组的检索功能 | 1 | 项 |
| 24 | 用户组的列表启用禁用 | 1 | 项 |
| 25 | 用户组内成员查看功能 | 1 | 项 |
| 26 | 用户组禁用 | 1 | 项 |
| 27 | 用户组启用 | 1 | 项 |
| 28 | 学员信息管理 | 学员信息 | 1 | 项 |
| 29 | 学员信息列表功能 | 1 | 项 |
| 30 | 学员信息添加功能、学员信息的修改功能 | 1 | 项 |
| 31 | 学员信息的单个学员删除功能 | 1 | 项 |
| 32 | 学员信息的预览功能 | 1 | 项 |
| 33 | 学员信息的检索功能 | 1 | 项 |
| 34 | 学员信息的批量添加功能 | 1 | 项 |
| 35 | 学员信息的批量删除功能 | 1 | 项 |
| 36 | 学员账号启用 | 1 | 项 |
| 37 | 学员账号禁用 | 1 | 项 |
| 38 | 学员信息导出功能 | 1 | 项 |
| 39 | 学习信息管理 | 档案信息 | 1 | 项 |
| 40 | 学员登录统计 | 1 | 项 |
| 41 | 获得荣誉 | 1 | 项 |
| 42 | 参与互动 | 1 | 项 |
| 43 | 参与培训项目统计 | 1 | 项 |
| 44 | 参与课程统计 | 1 | 项 |
| 45 | 参与考试统计 | 1 | 项 |
| 46 | 学习轨迹查看 | 1 | 项 |
| 47 | 师资库管理 | 师资库信息 | 1 | 项 |
| 48 | 师资增加功能/师资批量添加 | 1 | 项 |
| 49 | 师资信息编辑功能 | 1 | 项 |
| 50 | 师资删除功能 | 1 | 项 |
| 51 | 检索查询功能 | 1 | 项 |
| 52 | 师资禁用功能 | 1 | 项 |
| 53 | 师资课程查看功能 | 1 | 项 |
| 54 | 师资类型列表功能 | 1 | 项 |
| 55 | 师资类型添加功能 | 1 | 项 |
| 56 | 师资类型修改功能 | 1 | 项 |
| 57 | 师资的类型删除功能 | 1 | 项 |
| 58 | 课程管理 | 课程信息 | 1 | 项 |
| 59 | 课程查看 | 1 | 项 |
| 60 | 课程列表 | 1 | 项 |
| 61 | 课程添加功能/课程修改功能/课程删除功能 | 1 | 项 |
| 62 | 课程笔记管理 | 1 | 项 |
| 63 | 课程弹题管理 | 1 | 项 |
| 64 | 课程列表排序功能 | 1 | 项 |
| 65 | 课程列表设置审核状态功能 | 1 | 项 |
| 66 | 课程列表检索功能 | 1 | 项 |
| 67 | 音视频课程点播配置功能 | 1 | 项 |
| 68 | 音视频课程防下载防截屏防泄漏添加水印功能 | 1 | 项 |
| 69 | 课程资料信息 | 1 | 项 |
| 70 | 课程资料上传功能 | 1 | 项 |
| 71 | 课程资料编辑功能 | 1 | 项 |
| 72 | 课程资料添加功能 | 1 | 项 |
| 73 | 课程资料删除功能 | 1 | 项 |
| 74 | 课程资料下载控制 | 1 | 项 |
| 75 | 课程分类信息 | 1 | 项 |
| 76 | 课程分类列表功能 | 1 | 项 |
| 77 | 课程分类管理的添加功能 | 1 | 项 |
| 78 | 课程分类管理的删除功能 | 1 | 项 |
| 79 | 课程分类管理的编辑功能 | 1 | 项 |
| 80 | 培训班管理 | 培训项目信息 | 1 | 项 |
| 81 | 培训项目列表功能 | 1 | 项 |
| 82 | 新建培训项目添加功能 | 1 | 项 |
| 83 | 培训项目信息编辑管理功能 | 1 | 项 |
| 84 | 培训项目删除功能 | 1 | 项 |
| 85 | 培训项目列表检索功能 | 1 | 项 |
| 86 | 培训项目资源信息 | 1 | 项 |
| 87 | 培训项目阶段管理功能 | 1 | 项 |
| 88 | 新建/删除/编辑培训课程任务 | 1 | 项 |
| 89 | 课程资源检索选择 | 1 | 项 |
| 90 | 新建/删除/编辑培训考试任务 | 1 | 项 |
| 91 | 考试资源检索选择 | 1 | 项 |
| 92 | 新建/删除/编辑问卷任务 | 1 | 项 |
| 93 | 问卷资源检索选择 | 1 | 项 |
| 94 | 新建/删除/编辑线上作业任务 | 1 | 项 |
| 95 | 线上作业检索选择 | 1 | 项 |
| 96 | 新建/删除/编辑实操作业任务 | 1 | 项 |
| 97 | 实操作业批阅管理 | 1 | 项 |
| 98 | 新建/删除/编辑考勤任务 | 1 | 项 |
| 99 | 考勤学员列表维护管理 | 1 | 项 |
| 100 | 新建/删除/编辑心得作业 | 1 | 项 |
| 101 | 心得作业批阅管理 | 1 | 项 |
| 102 | 新建/删除/编辑练习 | 1 | 项 |
| 103 | 练习资源检索选择 | 1 | 项 |
| 104 | 培训项目学员维护管理 | 1 | 项 |
| 105 | 培训证书管理 | 1 | 项 |
| 106 | 培训资料 | 1 | 项 |
| 107 | 培训统计报表 | 1 | 项 |
| 108 | 讨论管理/评价管理/消息管理 | 1 | 项 |
| 109 | 实操作业关联培训班功能 | 1 | 项 |
| 110 | 学习通过策略 | 1 | 项 |
| 111 | 培训招生 | 培训报名信息 | 1 | 项 |
| 112 | 新闻公告处发布报名信息功能 | 1 | 项 |
| 113 | 新闻公告处修改报名信息功能 | 1 | 项 |
| 114 | 新闻公告处删除报名信息功能 | 1 | 项 |
| 115 | 报名信息指定向学员推送消息 | 1 | 项 |
| 116 | 培训报名信息发布功能 | 1 | 项 |
| 117 | 培训报名信息修改功能 | 1 | 项 |
| 118 | 培训报名信息增加功能 | 1 | 项 |
| 119 | 培训报名信息删除功能 | 1 | 项 |
| 120 | 显示已报名学员信息 | 1 | 项 |
| 121 | 培训报名人员范围设置 | 1 | 项 |
| 122 | 培训报名人数限制 | 1 | 项 |
| 123 | 培训报名是否允许退出配置 | 1 | 项 |
| 124 | 报名起止时间设置 | 1 | 项 |
| 125 | 报名学员信息表 | 1 | 项 |
| 126 | 报名学员导出 | 1 | 项 |
| 127 | 报名审核配置 | 1 | 项 |
| 128 | 报名审核人员配置 | 1 | 项 |
| 129 | 删除报名审核学员 | 1 | 项 |
| 130 | 报名审核学员列表筛选功能 | 1 | 项 |
| 131 | 报名学员详情信息 | 1 | 项 |
| 132 | 报到管理 | 学员签到信息 | 1 | 项 |
| 133 | 学员签到信息列表查看功能 | 1 | 项 |
| 134 | 学员签到信息删除功能 | 1 | 项 |
| 135 | 生成签到二维码 | 1 | 项 |
| 136 | 考勤管理 | 考勤二维码信息 | 1 | 项 |
| 137 | 考勤时间列表功能 | 1 | 项 |
| 138 | 考勤时间修改功能/考勤时间删除功能 | 1 | 项 |
| 139 | 考勤编辑 | 1 | 项 |
| 140 | 考勤记录列表功能 | 1 | 项 |
| 141 | 考勤导出 | 1 | 项 |
| 142 | 试题管理 | 考试系统信息 | 1 | 项 |
| 143 | 试题列表功能 | 1 | 项 |
| 144 | 试题增加功能 | 1 | 项 |
| 145 | 试题编辑功能 | 1 | 项 |
| 146 | 试题删除功能 | 1 | 项 |
| 147 | 试题列表查询功能 | 1 | 项 |
| 148 | 试题批量删除功能 | 1 | 项 |
| 149 | 试题预览功能 | 1 | 项 |
| 150 | 试题检索功能 | 1 | 项 |
| 151 | 试题上传功能/试题批量上传功能 | 1 | 项 |
| 152 | 试题上传流程审核 | 1 | 项 |
| 153 | 考试管理 | 考试管理信息 | 1 | 项 |
| 154 | 试卷关联培训项目 | 1 | 项 |
| 155 | 试卷列表功能 | 1 | 项 |
| 156 | 试卷列表检索功能 | 1 | 项 |
| 157 | 试卷列表修改功能/试卷列表删除功能 | 1 | 项 |
| 158 | 随机组卷功能/手动组卷功能 | 1 | 项 |
| 159 | 试卷的预览功能 | 1 | 项 |
| 160 | 试卷导出 | 1 | 项 |
| 161 | 试题相似度管理 | 1 | 项 |
| 162 | 考试统计报表管理 | 统计报表信息 | 1 | 项 |
| 163 | 成绩汇总统计报表功能 | 1 | 项 |
| 164 | 成绩综合查询功能/试卷分数统计功能 | 1 | 项 |
| 165 | 考试试题分析 | 1 | 项 |
| 166 | 结业证书管理 | 自动生成培训班结业证书 | 1 | 项 |
| 167 | 管理员手动发放证书功能 | 1 | 项 |
| 168 | 证书模板的导入/在线模板编辑 | 1 | 项 |
| 169 | 教学评估管理 | 教学评估信息 | 1 | 项 |
| 170 | 调查问卷列表 | 1 | 项 |
| 171 | 调查问卷的增加功能 | 1 | 项 |
| 172 | 调查问卷的修改功能/调查问卷的删除功能 | 1 | 项 |
| 173 | 调查问卷的发布功能 | 1 | 项 |
| 174 | 问卷统计分析 | 1 | 项 |
| 175 | 管理员后台查阅学员调查问卷功能 | 1 | 项 |
| 176 | 法院层级统计 | 法院统计信息 | 1 | 项 |
| 177 | 按时间筛选查看信息功能 | 1 | 项 |
| 178 | 参加培训项目统计 | 1 | 项 |
| 179 | 自定义统计字段 | 1 | 项 |
| 180 | 单位学习综合指标统计 | 1 | 项 |
| 181 | 统计报表导出下载功能 | 1 | 项 |
| 182 | 培训班统计 | 培训项目统计信息 | 1 | 项 |
| 183 | 按培训类型统计功能 | 1 | 项 |
| 184 | 按时间筛选功能 | 1 | 项 |
| 185 | 按参训类型统计 | 1 | 项 |
| 186 | 按实际参加培训人数统计功能 | 1 | 项 |
| 187 | 按完成人数统计的功能 | 1 | 项 |
| 188 | 按未完成人数统计的功能 | 1 | 项 |
| 189 | 按特定维度筛选统计功能 | 1 | 项 |
| 190 | 统计数据穿透查看 | 1 | 项 |
| 191 | 课程统计 | 课程统计信息 | 1 | 项 |
| 192 | 按课程类型类别统计功能 | 1 | 项 |
| 193 | 按单个课程学习人数统计 | 1 | 项 |
| 194 | 按课程学时统计 | 1 | 项 |
| 195 | 按课程学次统计 | 1 | 项 |
| 196 | 按个人分析 | 个人统计信息 | 1 | 项 |
| 197 | 学员总学习时长 | 1 | 项 |
| 198 | 按学员参与学习各培训项目统计 | 1 | 项 |
| 199 | 按学员综合指标培训统计 | 1 | 项 |
| 200 | 学员登录活跃统计 | 1 | 项 |
| 201 | 学员统计自定义报表 | 1 | 项 |
| 202 | 智慧教学管理子系统 | 登录功能 | 学员登录功能/登录验证码功能 | 1 | 项 |
| 203 | 多端登录访问，新登录会之前登录挤下线 | 1 | 项 |
| 204 | 超出错误次数账号锁定功能 | 1 | 项 |
| 205 | 首页模块 | 首页展示单个课程加入学习数据显示 | 1 | 项 |
| 206 | 最新推荐课程轮播模块 | 1 | 项 |
| 207 | 课程的系列展示 | 1 | 项 |
| 208 | 优秀师资的轮播展示/课程加入学习人数 | 1 | 项 |
| 209 | 通知公告模块 | 通知列表页面内容展示功能 | 1 | 项 |
| 210 | 课程展示模块 | 课程展示信息 | 1 | 项 |
| 211 | 课程页面关键字搜索功能 | 1 | 项 |
| 212 | 课程授课师资基本信息展示功能 | 1 | 项 |
| 213 | 教师推荐模块 | 教师推荐列表查看功能/教师排行榜 | 1 | 项 |
| 214 | 课程展示推荐课程模块 | 1 | 项 |
| 215 | 教师推荐详情展示功能 | 1 | 项 |
| 216 | 教师推荐详情页相关课程展示功能 | 1 | 项 |
| 217 | 课程评价 | 课程评价信息 | 1 | 项 |
| 218 | 对授课教师添加评价功能 | 1 | 项 |
| 219 | 对所学课程评价功能 | 1 | 项 |
| 220 | 学习记录 | 学习记录信息 | 1 | 项 |
| 221 | 学习时长统计 | 1 | 项 |
| 222 | 学习积分统计 | 1 | 项 |
| 223 | 学习获取证书查看 | 1 | 项 |
| 224 | 学习日历 | 1 | 项 |
| 225 | 我的档案 | 1 | 项 |
| 226 | 学习轨迹 | 1 | 项 |
| 227 | 学员基本信息管理 | 学员基本信息 | 1 | 项 |
| 228 | 个人信息查看功能 | 1 | 项 |
| 229 | 个人信息修改功能 | 1 | 项 |
| 230 | 消息模块 | 查看消息详情功能 | 1 | 项 |
| 231 | 消息分类显示功能 | 1 | 项 |
| 232 | 未读消息显示功能 | 1 | 项 |
| 233 | 消息列表功能 | 1 | 项 |
| 234 | 收藏模块 | 收藏信息功能 | 1 | 项 |
| 235 | 添加收藏培训项目功能 | 1 | 项 |
| 236 | 培训项目收藏列表展示功能 | 1 | 项 |
| 237 | 培训项目收藏删除功能 | 1 | 项 |
| 238 | 添加课程的收藏 | 1 | 项 |
| 239 | 课程收藏列表展示功能 | 1 | 项 |
| 240 | 课程收藏删除功能 | 1 | 项 |
| 241 | 专项培训 | 培训信息 | 1 | 项 |
| 242 | 培训报名功能 | 1 | 项 |
| 243 | 培训课程列表展示功能 | 1 | 项 |
| 244 | 培训课程详情页介绍及展示功能 | 1 | 项 |
| 245 | 视频播放学习信息 | 1 | 项 |
| 246 | 培训课程音视频播放功能 | 1 | 项 |
| 247 | 视频播放断点续播功能 | 1 | 项 |
| 248 | 培训课程教学评估功能 | 1 | 项 |
| 249 | 小程序平台 | 报到模块 | 报到二维码后台生成前台展示 | 1 | 项 |
| 250 | 小程序与后台数据交互 | 1 | 项 |
| 251 | 验证功能 | 1 | 项 |
| 252 | 登录模块 | 学员登录页面 | 1 | 项 |
| 253 | 学员身份验证功能 | 1 | 项 |
| 254 | 登录成功页面跳转提示功能 | 1 | 项 |
| 255 | 学习模块 | 移动端学习信息 | 1 | 项 |
| 256 | 培训在线报名功能 | 1 | 项 |
| 257 | 课程列表查看功能 | 1 | 项 |
| 258 | 课程详情查看功能 | 1 | 项 |
| 259 | 培训列表查看功能 | 1 | 项 |
| 260 | 培训详情页查看功能 | 1 | 项 |
| 261 | 培训课程列表展示功能 | 1 | 项 |
| 262 | 课程播放记录观看时长功能 | 1 | 项 |
| 263 | 签到模块 | 签到页面展示开发 | 1 | 项 |
| 264 | 签到二维码嵌入展示 | 1 | 项 |
| 265 | 签到提示功能 | 1 | 项 |
| 266 | 考试模块 | 小程序端考试信息 | 1 | 项 |
| 267 | 进入考试前验证考试资格功能 | 1 | 项 |
| 268 | 小程序端答题功能 | 1 | 项 |
| 269 | 查看答案功能 | 1 | 项 |
| 270 | 查看得分功能 | 1 | 项 |
| 271 | 问卷调查 | 课程评价信息 | 1 | 项 |
| 272 | 课程评价信息展示功能 | 1 | 项 |
| 273 | 添加课程评价信息功能 | 1 | 项 |
| 274 | 课程评分的展示功能 | 1 | 项 |
| 275 | 添加课程评分功能 | 1 | 项 |
| 276 | 接口开发 | 单点登录 | 用户名唯一值验证接口 | 1 | 项 |
| 277 | 用户部门验证接口 | 1 | 项 |
| 278 | 用户法院验证接口 | 1 | 项 |
| 279 | 验证通过完成登录后写入缓存并跳转首页接口 | 1 | 项 |
| 280 | 用户信息同步接口 | 全量用户同步接口 | 1 | 项 |
| 281 | 增量用户定时同步接口 | 1 | 项 |
| 282 | 某一个用户信息同步接口 | 1 | 项 |
| 283 | 查询某一个用户信息接口 | 1 | 项 |
| 284 | 内外网数据交换 | 内外网数据合并脚本开发 | 1 | 项 |

##### 表4：其他服务

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **名称** | **相关指标或用途说明** | **单位** | **数量** |
| 1 | 实人认证服务包 | 实人认证服务目前仅支持对拥有中华人民共和国第二代居民身份证的居民进行认证。本服务包含1万次的身份实人认证，通过实人认证服务以判断当事人与其身份证信息是否匹配。 | 年 | 1 |
| 2 | 短消息服务包 | 短消息服务包含10万条短信发送服务，采用短信应用平台向当事人提供短信消息通知或身份认证码确认服务。 | 年 | 1 |
| 3 | 数字证书信息采制作/电子印章重新注册方法测试 | 1）采用原有签章的KEY介质，现场收回制作数字证书，采集全省31家法院所有工作人员信息，并录入到登录认证系统中，到各个法院现场，制作数字证书导入到Ukey中，并实现登录证书的测试登录；  2）数字证书注册完成后，电子印章重新制作发放，X86端盖章测试或信创电脑盖章测试，测试完成后使用单位用户确认总计表。  3）以上证书的制作与发放需要拿到使用用户的密码或者当面制作，用户输入密码确认。 | 套 | 3400 |
| 4 | 原有国密信创印章的续购 | 目前全省国密改造涉及原有2200套印章升级改造，改造后支持国产化终端的OFD文件盖章、HTML5签章格式的盖章，支持所有国产化终端的技术路线。 | 套 | 2200 |
| 5 | 新增登录证书KEY制作 | 采用新KEY介质，制作除签章人员以外的登录证书，采集全省31家法院需要登录工作人员信息，并录入到登录认证系统中，到各个法院现场，制作数字证书导入到Ukey中，并实现登录证书的测试登录. | 套 | 1000 |
| 6 | 互联庭审云视频接入服务 | 提供互联网庭审云视频接入服务，服务期3年。 | 套 | 7 |
| 7 | 集成费 | 含基础环境集成实施费、硬件集成实施费、软件集成实施费（含本项目所建设的门禁、监控、约35㎡科技法庭信息化建设等相关的墙面、地面开槽及修复，线路敷设等费用） | 项 | 1 |

### **★**1.2 商务要求

### 1.2.1支付方式

（1）本合同签订后15个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同金额的30%作为项目的首付款；

（2）项目初验通过后15个工作日内，甲方凭乙方开具的正式有效发票向乙方支付合同金额的40%；

（3）项目终验通过后，乙方提交以甲方为受益人、履约保证金金额为合同总金额的3%、担保期限为项目终验通过之日起3年的履约保证金给甲方。

（4）甲方在收到乙方提交的履约保证金及尾款的有效发票后的3个工作日内，向乙方支付合同金额的30%；

（5）项目终验通过3年后无质量问题，甲方向乙方退还乙方所提交的履约保证金。

### 1.2.2本包采购预算（报价不得超过最高限价）：12796753.29元

### 1.2.3工期及交货地点

1）工期：自合同签订之日起24个月。

2）交货地点：用户指定地点。

### 1.2.4运维服务要求

1、项目整体运维服务说明：

（1）由于项目建设的特点，为保证本次项目的正常运行，硬件设备、业务系统等主要设备（系统）的运行维护由设备（系统）供应商承诺原厂提供服务，辅助设备的运行维护由系统集成商负责，运维服务由承建商统筹提供。

（2）本项目通过竣工验收之日起提供不少于3年整体免费维保（含所有网络安全设备3年病毒库升级授权和特征库服务）。项目免费维保期间，投标人需提供至少1人（5\*8小时）在海南省高级人民法院驻场提供运维服务,重点负责密码设施运维。

（3）中标人及其相关人员对提供与本项目有关的服务时接触到的甲方信息负有保密义务。

2、保修期间，中标人应提供但不限于下述服务：

（1）在保修期间提供免费保修，提供7×24小时技术支持和服务，1小时内响应，通过远程方式无法解决的，海口市内2小时、海口市外6小时到达故障现场进行处理。使用单位认为故障存储部件存有涉密信息或敏感数据的，中标人不回收故障存储部件；

（2）指定专门技术人员负责系统的技术支持；

（3）服务方式除现场技术支持外，还应包括电话、互联网、E-MAIL等方式；

（4）服务范围包括系统安装、升级（含升级服务包）、调试、性能调优、系统管理等；

（5）每年不少于两次巡检；

（6）中标人应根据使用单位要求，提供现场免费使用及维护培训。

### 1.2.5培训服务要求

投标人须承诺负责本项目培训的讲师都为拥有多年技术支持、市场经验的资深专业人员。培训内容包括软硬件系统的配置、安装环境、系统架构，以及实际操作、应用、管理维护、安全防护、应急处理等方面知识，帮助用户单位培训维护队伍，建立维护规章制度，提高维护水平。

在培训的同时，中标人须向用户单位提供软硬件系统操作说明、相关技术文档、培训内容PPT等多种资料。

### 1.2.6设备安装、验收

1、设备安装及调试：

（1）中标人应负责将设备运至用户指定处并提供设备的免费安装调试。

（2）中标人在设备安装前应派员进行实地勘察，设计安装调试方案，确保设计合理、设备运行可靠、维护方便。

（3）中标人负责组织专业技术人员进行设备安装调试，用户应提供必备的基本条件和专人配合，保证各项安装工作顺利进行。

（4）安装调试到位后的设备由中标人、监理人员、用户单位代表（如需要）共同进行质量签验。

（5）中标人向用户提供安装和维修所需特殊专用的工具、备件及清单和中文说明书，其费用包括在投标价格内。

（6）中标人应提供免费安装现场培训。

2、验收与提供材料要求：

（1）验收标准：本项目及所采购货物应按生产厂家的产品出厂检验标准、招标文件、项目可研报告、初步设计方案以及国家和行业验收规范要求及合同中的相关条款等进行数量及质量的验收。

（2）验收步骤：

第一步：出厂检验。中标人负责所提供产品的出厂检验，保证产品原产地和技术指标的真实性、完整性、合法性，负责在采购人指定地点进行软件设置和安装，负责将产品送达交货地点，并向采购人提供货物制造厂的出厂检验报告、质量合格证书等。采购人（或采购人授权单位）在设备（含软件）到货后，将按合同规定对所交货物进行清点、核对和商检。

第二步：安装调试和初步验收。货物送至采购人指定的安装现场后，由采购人（或采购人授权单位、监理单位）和中标人共同对货物的数量、基本质量、外包装等逐项检验，并由中标人负责安装调试、集成，系统集成完成后，由采购人（或采购人授权单位、监理单位）对设备和系统集成组织初验。

第三步：项目终验：系统通过试运行并达到试运行目标后（试运行期间，出现的任何软硬件问题，应由中标人及时处理修正），由采购人根据有关规定报请相关主管部门组织验收，对所购货物主要指标（如设备配置、品牌指标、可靠性、稳定性等）、集成情况和培训情况进行验收，如设备测试不合格，或中标人提供的培训服务未能满足招标文件和投标文件规定要求，验收将不予通过。

2）若验收不能符合要求，采购人将按合同商务条款的有关规定执行。

3、技术材料

中标后应提供的技术资料：中标人至少应向采购人提供以下列标明的中文（或英文）技术资料，其费用应包括在投标内。

(1)产品技术说明书；

(2)安装手册（含所需的软件安装序列号）；

(3)操作手册；

(4)维修手册；

(5)货物相应的软件和光盘、授权使用文件；

(6)出厂明细表（装箱单）；

(7)产品技术标准（含验收标准）和测试方法；

(8)出厂检验报告和合格证书。

若技术资料不全，采购人有权拒绝验收。

### 1.2.7其它要求

（1）本项目实施阶段，中标人应制作整体实施方案报采购人批准后执行，整体实施方案应严格遵照海南省信息化主管部门批复的项目可行性研究报告和项目初步设计方案等相关解决方案。中标人应对项目定制开发内容的业务需求进行调研，并制作用户需求书报采购人同意后开发。

（2）投标人进场后应开展详细需求调研，结合初步设计方案等，形成详细设计方案做为项目建设的重要依据。如因实际需求发生重大变化，采购人有权变更或停止部分货物和服务的采购。

（3）中标人承建本项目需接受采购人委托的监理公司的监理。

（4）本项目定制开发的软件或软件构件、接口（含方案描述为定制开发但投标人所投为软件成品的），知识产权属于采购人，中标人需向采购人提交包括软件源代码在内的所有技术资料。

（5）本项目所含信息系统由中标方按网络安全等级保护三级要求建设、运维，根据等级保护要求，需要采购方提供非本项目资产的安全保护资源（含服务或能力）的，中标方应在建设时提出，在采购方或采购方指定的第三方提供商提供安全保护资源后，由中标方负责集成安装运维或配合集成安装运维。中标人应接受采购方或其授权方关于本项目信息系统安全等级保护建设的指导，并在系统测评工作提供必要的配合和协助。

（6）基于项目建设目标的需要，本招标文件对本工程建设要求描述不详的，中标方工程实施时，应以海南省政务信息化项目建设有关规定和本项目初步设计方案》等载明的要求为准。

（7）投标人必须根据所投产品的技术参数、资质资料编写投标文件。在中标结果公示期间，采购人有权对中标候选人所投产品的技术参数、资质证书等进行核查，如发现与其投标文件中的描述不一，采购人将报政府采购主管部门严肃处理。

**（8）中标单位因自身原因不能在约定的工期内完成项目建设内容（因采购方原因或不可抗力造成工期延误的除外），不论项目实施到任何阶段，须全额退还甲方已支付的全部款项。中标单位已投入的软件开发成本费用、集成费等自行承担，并无偿回收采购方已签收的所有硬件设备、成品软件及辅材，同时承担相应的法律责任及采购方损失。**

**（9）通用办公设备（一体机、庭审电脑、电视、打印机）的投标报价不得超过《海南省财政厅关于印发海南省省直行政事业单位通用办公设备家具配置标准（2020年版）的通知》（琼财资【2020】491号）中的资产配置价格标准：**

**1）一体机、庭审电脑最高限价为6500元/台**

**2）电视最高限价为6000元/台**

**3）打印机最高限价为2000元/台**

**注：投标报价超过上述最高限价的，视为无效投标处理。**

## 采购包2采购需求

### 1.项目名称

海南智慧法院综合办公办案平台（一期）项目监理服务（采购包2）。

### 1.1本包采购预算

采购预算：159282.38元人民币（报价不得超过采购预算）。

### 1.2监理内容

监理范围为海南智慧法院综合办公办案平台（一期）项目的建设内容。

### **★**1.3监理技术要求

#### 1.3.1监理服务周期

本项目监理服务周期自签订合同之日起，至建设项目完成竣工验收。

#### 1.3.2监理范围

重点对项目建设过程中设备/材料的采购、设备安装调试、系统集成、软件开发及应用技术培训、试运行、测试、验收等全过程进行监督管理，从硬件监理、软件监理、系统集成监理等三个方面梳理该项目建设的工程监理应如何通过切实有效方式、方法、手段达到建设方所要求的深度、广度，最终实现工程监理的目标。实现对质量、进度、经费、变更的控制及合同管理和文档管理。当工程质量或工期出现问题或严重偏离计划时，应及时指出，并提出对策建议，同时督促承建单位尽快采取措施。

#### 1.3.3监理目标控制方案

以工程建设合同、监理委托合同、国家（GB/T19668.1-19668.7《信息技术服务监理》及有关法规、技术规范与标准、项目建设单位需求为依据，通过专业的控制手段，协助建设单位全面地进行技术咨询和技术监督，对工程全过程进行监督、管理、指导、评价，并采取相应的组织措施、技术措施、经济措施和合同措施，确保建设行为合法、合理、科学、经济，使建设进度、投资、质量达到建设合同规定的目标。

1.监理质量目标控制

监理质量目标控制是监理技术服务的核心所在，也是监理单位综合实力的最好反映，所以做好监理质量目标控制方案，确保本项目建设质量能达到建设单位要求的质量目标。

确保本项目建设质量达到工程合同中规定的功能、技术参数等目标。确保工程建设中的设备和各个节点满足相关国家（GB/T19668.1-19668.7《信息技术服务监理》、地方或行业质量标准和技术标准，按照承建合同要求进行基于总体方案的细化设计、开发、安装、调试和运行；系统集成和软件开发过程涉及用户需求调研分析、概要设计、详细设计、系统实现、系统测试和系统运行等比较复杂、制约因素多的工作内容，应该成为质量控制的重点；深化设计方案的确定、开发平台选定，也要进行充分论证。要求监理在整个工程实施过程中做好对工程质量的事前控制，事中监督和事后评估，以确保工程质量合格。供应商应针对本项目建设中软硬件设备采购、设备安装调试、系统集成、软件开发、工程培训等提出工程监理的质量控制原则、方法、措施、工作流程和目标。

2.监理进度目标控制

确保本项目按合同规定的工期完工。依据合同所约定的工期目标，在确保质量和安全的原则下，采用动态的控制方法，对进度进行主动控制，确保项目按规定的工期完工。通过对本项目概要设计的分析、研究，提出针对本项目建设的、有代表性的信息工程监理进度控制的主要原则、方法、内容、措施、工作流程和目标。

3.监理投资目标控制

协助用户控制本项目建设总投资在项目预算及审计范围内，减少项目建设中的额外开支。以项目建设方和承建单位实际签订的合同金额为准，确保项目费用控制在合同规定的范围内。在项目建设中，合理减少项目变更，保护建设单位的经济利益。

#### 1.3.4工程监理重点难点分析

供应商应根据建设的特点，从实际出发分析本项目监理工作的重点、难点，并根据分析的结果制定相应的监理工作规划、对策和策略，以便日后有针对性的开展建设工程的监理服务工作。

1.项目组织及总体技术方案的质量控制

1. 协助审查项目建设方的投标书、合同及实施方案；
2. 在技术上、经济上、性能上和风险上进行分析和评估，为采购人提供建议；
3. 协助审查项目建设方提交的组织实施方案和项目计划等相关文档；
4. 协助审查项目建设方的工程质量保证计划及质量控制体系；
5. 参与制定项目质量控制的关键节点及关键路径。

2.项目质量控制

组织措施：建立质量管理系统，完善职责分工及有关质量监督制度，落实质量控制责任。

3.系统集成质量控制

1. 审核系统总集成方案；
2. 对采购的硬件设备及网络环境的综合质量进行检验、测试和验收；
3. 参与制定系统验收大纲；
4. 对设备安装、调试进行验收；
5. 对系统进行总体验收。

4.人员培训的质量控制

1. 协助审查并确认培训计划，审定培训大纲；
2. 监督审查建设方实施其培训计划，并征求采购人的意见反馈；
3. 监督审查考核工作，评估培训效果；
4. 协助审核并确认培训总结报告。

5.文档、资料的质量控制

监督审查建设方提供的设备型号、数量、到货时间以及设备的技术资料、系统集成和软件安装在实施过程中所有相关文件的标准性和规范化，在各项目验收时，应监督项目建设方提交符合规定的成套资料，包括印刷本和电子版。

对监理项目实施过程中的文档进行标准化、规范化管理，在监理项目验收时，应提交符合规定的监理项目的成套资料，包括印刷本和电子版。

6.进度协调控制

组织措施：建立进度控制协调制度，落实进度控制责任。

1. 编制项目控制进度计划：编制项目总进度计划和网络图。按各子系统实际情况进行编制，包括系统建设开工、设备的采购、设备的安装调试、软件的编制、试运行等各方面内容,做到既要保证各子系统、各阶段目标的顺利实现，又要保证项目间、阶段间的衔接、统一和协调。
2. 审查各子系统建设方编制的工作进度计划：分析系统建设进度计划是否能满足合同工期及系统建设总进度计划的要求，特别要对照上阶段计划工程量完成情况进行审查,对为完成系统建设进度计划所采取的措施是否恰当、设备能否满足要求、管理上有无缺陷进行审查。要根据建设方所能提供的人员及设备性能复核、计算设备能力和人员安排是否满足要求等，分析判断计划是否能落实，审查建设方提出的设备供应计划能否落实。如发现供应计划未落实，应及时报告采购人，要求建设方采取应急措施满足系统建设的需求。
3. 系统建设进度的现场检查：随时或定期、全面地对进度计划的执行情况跟踪检查，发现问题及时采取有效措施加以解决。加强系统建设准备工作的检查，在工程项目或部分工序实施前，对情况进行检查，要加强检查设备、人员安排、各项措施的落实情况，确保准备工作符合要求，不影响后续工程的进行。
4. 进度计划的分析与调整:要保证建设进度与计划进度一致，经常对计划进度与实际进度进行比较分析，发现实际进度与计划进度不符时，即出现进度偏差时，首先分析原因，分析偏差对后续工作的影响程度，并及时通知建设方采取措施，向建设方提出要求和修改计划的指令。

7.投资控制

组织措施：建立健全项目管理组织，完善职责分工及有关质量项目管理制度，落实投资控制的责任。

1. 审查设计图纸和文件，审查建设方的施工组织设计和各项技术措施，深入了解设计意图，在保证系统建设质量和安全的前提下尽可能优化设计。
2. 严格督促建设方按合同实施，严格控制合同外项目的增加，协助采购人严格控制设计变更，制定设计变更增加工作量的报批制度；及时了解系统建设情况，协调好各方矛盾，减少索赔事件的发生。对发生的事件严格按合同及法律条款进行处理，认真进行索赔调解。

8.合同管理

合同管理是加快系统建设进度、降低系统建设造价、保证系统建设质量的有效途径之一。通过合同管理，可以督促建设方在各个阶段按照合同要求保证设备、人员的配备及投入，保证各阶段目标按合同实施，减少索赔事件，控制系统建设结算等。具体要求如下：

1. 以合同为依据，本着“实事求是、公正”的原则，合情合理地处理合同执行过程中的各种争议。
2. 分析、跟踪和检查合同执行情况，确保项目建设方按时履约。
3. 对合同的工期的延误和延期进行审核确认。
4. 对合同变更、索赔等事宜进行审核确认。
5. 根据合同约定，审核项目建设方的支付申请。
6. 建立合同目录、编码和档案。
7. 合同管理坚持标准化、程序化，如设计变更、延期、索赔、计量支付等应规定出固定格式和报表。合同价款的增减要有依据，合同外项目增加要严格审批制度。重大合同管理问题的处理，如大的变更、索赔、复杂的技术问题等，组成专门小组进行研究。不符合实际情况的合同条款及时向采购人报告，尽早处理，以免造成损失。

9.信息、工程文档管理

在项目管理过程中，为了实现对进度、质量、投资的有效控制，处理有关合同管理中的各种问题，监理方需要收集各种有用的信息。信息的来源主要包括采购人文件、设计图纸和文件、建设方的文件、建设现场的现场记录（或项目管理日志）、会议记录、验收情况及备忘录等等。其中项目管理日志是进行信息管理的一个最重要的方面。项目管理日志主要包括当天的工作项目和工作内容、投入的人力和设备运行情况、计划的完成情况及进度情况、停工和返工及窝工情况。信息管理主要措施要求如下：

1. 制定详细的信息收集、整理、汇总、分析、传递和利用制度，力求信息管理的标准化和制度化。由专人负责系统建设信息的收集、分类、整理储存及传递工作。信息传递以文字为主，统一编号，利用计算机进行管理，力求信息管理的高效、迅速、及时和准确，为系统建设提供及时有用的信息和决策依据。
2. 在项目实施过程中做好工程监理日记和工程大事记。
3. 做好双方合同、技术建设方案、测试文档、验收报告等各类往来文件的存档。
4. 建立必要的会议、例会制度，整理好会议纪要，并监督会议有关事项的执行情况。
5. 立足于建设现场，加强动态信息管理，对现场的信息进行详细记录和分析，做到以文字为基础，以数据说明问题。根据收集到的信息与合同进行比较，督促建设方的人员和设备到位，促使承包商按合同完成各项目标，从而实现对进度、质量、投资的控制。
6. 建立完整的各项报表制度，规范各种适合本项目的报表。定期将各种报表、信息分类汇总，及时向采购人及有关各方报送。
7. 监理项目验收时，应提交符合规定的有关工程的成套资料，包括印刷本和电子版。

10.日常监理

1. 掌握监理范围内涉及的各种技术及相关标准；
2. 安排足够的监理人员，按工程需要派驻相应的专业人员进行项目监理，至少保证1名专职信息系统监理工程师在现场，随时为采购人提供服务，总监理工程师必需专职于本项目；
3. 制定工程管理的组织机构方案并协助采购人组建相关机构，并提供相关培训；
4. 熟悉了解项目的业务需求，协助采购人对项目的目标、范围和功能进行界定，参与并协助项目的设计方案交底审核工作；
5. 建立健全科学合理的会议制度，并予以贯彻落实；
6. 建立健全科学合理的文档管理制度，制订开发过程中产生的各类文档制作、管理规范，并予以贯彻落实；
7. 与采购方一起制定评审机制，在工程实施全过程中随时关注隐患苗头，如发现将会导致工程失败的情况出现时，应及时启动评审机制，组织专家对工程实施情况进行评审，对评审不合格的，应向采购方提出终止合同意见。此外，还应组织定期评审（阶段性评审、里程碑评审、验收评审），对评审结果为优的，提出奖励意见，评审不合格的，则向采购方提出处理意见；

#### 1.3.5工程各阶段的监理规划、实施

供应商应对本项目从设计施工到项目竣工验收阶段制定一整套工程监理的工作流程，并叙述各阶段主要监理工作内容。

本项目监理工作主要分为设备/材料采购、施工阶段、验收阶段、质保期阶段等。

1.设备/材料采购监理

建设项目由承包单位承担设备/材料采购任务，工程监理单位在设备/材料采购阶段监理工作主要有：

审核承包单位的设备采购计划和设备采购清单；

订货进货验证；

组织到货验收；

鉴定、设备移交等；

2.施工阶段监理

一、工前的监理

（1）审核施工设计方案：开工前，由监理单位组织实施方案的审核，内容包括设计交底，了解需求、质量要求，依据设计招标文件，审核总体设计方案和有关的技术合同附件，以避免因设计失误造成实施的障碍；

（2）审核实施方案的合法性、合理性、与设计方案的符合性；

（3）审批施工组织设计：对施工单位的实施工作准备情况进行和监督；

（4）审核施工进度计划：对施工单位的施工进度计划进行评估和审查；

（5）审核实施人员：确认施工方提交的实施人员与实际工作人员的一致性，如有变更，则要求叙述其原因；

（6）审核《软件项目开发计划》。

二、施工准备阶段的监理

（1）审批开工申请，确定开工日期；

（2）了解承包商设备订单的定购和运输情况；

（3）了解施工条件准备情况；

（4）了解承建单位实施前期的人员组织、施工设备到位情况；

（5）编制各个子项目监理细则；

（6）签发开工令。

三、施工阶段的监理

（1）审核软件开发各个阶段文件；

（2）协助采购人组织软件开发阶段评审；

（3）材料、硬件设备、系统软件的供货计划的审核；

（4）材料、硬件设备、系统软件的进场、开箱和检验；

（5）促使项目中所使用的产品和服务符合合同及国家相关法律法规和标准；

（6）对施工各个阶段的安装工艺进行检查；

（7）审核项目各个阶段进度计划；

（8）督促、检查承建单位进度执行情况；

（9）审查项目变更，提出监理意见；

（10）审查承建单位阶段款支付申请，提出监理意见；

（11）按周（月、旬）定期报告项目情况；

（12）组织召开项目例会和专项会议。

四、试运行阶段的监理

（1）协助建设方确认项目进入试运行；

（2）监查系统的调试和试运行情况，记录系统试运行数据；

（3）进行试运行期系统检测或测试，做出检测或测试报告；

（4）对试运行期间系统出现的质量问题进行记录，并责成有关单位解决。解决问题后，进行二次监测；

（5）进行试运行时间核算；

（6）协助业主确认试运行通过。

3.验收阶段监理

一、验收阶段

（1）对承建单位在试运行阶段出现的问题的整改情况进行监督和复查；

（2）监督检查承建单位作好用户培训工作，检查用户文档；

（3）组织系统初步验收；

（4）审查承建单位提交的竣工文档；

（5）参与项目竣工验收；

（6）竣工资料收集整理齐全并装订，签署验收报告；

（7）审核项目结算；

（8）审查承建单位阶段款支付申请，提出监理意见；

（9）向建设单位提交监理工作总结；

（10）将所有的监理材料汇总，编制监理业务手册，提交采购人；

（11）系统验收完毕进入保修阶段的审核与签发移交证书。

二、项目移交阶段

（1）系统的设计方案、设计图纸和竣工资料的全部移交；

（2）设备、软件、材料等的验收文档核实；

（3）施工文档的移交；

（4）竣工文档的移交；

（5）项目的整体移交。

4.质保期阶段监理

监理单位承诺依据委托监理合同约定的工程质量保修期规定的时间、范围和内容开展

工作主要有：

1. 定期对项目进行回访，协助解决技术问题；
2. 对项目建设单位提出的质量缺陷进行检查和记录；
3. 对质量缺陷原因进行调查分析并确定责任归属；
4. 检查承建单位质保期履约情况，督促执行；
5. 审查承建单位阶段款支付申请，提出监理意见。

供应商应根据上述监理工作内容（但不局限于上述内容），分别制定详细的监理工作流程，使监理工作流程化、制度化。

#### 1.3.6监理工作要求

1.监理工作制度要求

根据本项目的特色，本项目要求以现场监理为主要方式进行，在施工现场主要监理人员必须具备所从事监理业务的专业技术和类似系统经验，并具有丰富的项目管理经验。监理工作必须由具有相应资质和职称的人员来担任。本次监理项目实行总监理工程师负责制，且必须在建设期间全程常驻至少1名监理工程师在甲方现场。监理公司应建立项目监理小组，负责整个项目的全程监理工作，本项目必须配备不少于1名的现场专业工程师。监理人员的确定和变更，须事先经业主方同意。监理人员必须奉公守法，具有高度的责任心。

2.监理项目组织要求

工程监理组织形式应根据工程项目的特点、工程项目承包模式、业主委托的任务以及监理单位自身情况而确定，结构形式的选择应考虑有利于项目合同管理、有利于目标控制、有利于决策指挥、有利于信息沟通。

要求供应商在报价方案中要明确工程监理的各项运作，包括监理人员的相关资料、职能分配、监理组织的构成及工作流程、各项监理工作的相关负责人等。

3.监理信息管理要求

供应商应制定有关本项目信息管理流程，规范各方文档并负责整理记录归档业主单位与承建单位来往的文件、合同、协议及会议记录等各种文档，并定期以监理月（周/季）报形式提交业主。包括下列监理工作：

1. 做好监理日记及工程大事记；
2. 做好合同批复等各类往来文件的批复和存档；
3. 做好项目协调会、技术专题会等各项会议纪要；
4. 管理好实施期间的各类、各方技术文档；
5. 做好项目周报；
6. 做好监理建议书、监理通知书存档；
7. 阶段性项目总结。

供应商应针对项目特点，制定相应的信息分类表、信息流程图、信息管理表格、信息管理工作流程与措施，同时要求采用先进的项目信息管理软件对项目信息进行综合管理。

4.监理合同管理要求

本项目建设过程中会与承建单位签订各种合同，供应商应该针对项目特点制定合同从草案到签署的管理工作流程与措施，规范合同管理，并在具体项目合同执行时进行下列监理工作：

1. 跟踪检查合同的执行情况，确保承建单位按时履约；
2. 对合同工期的延误和延期进行审核确认；
3. 对合同变更、索赔等事宜进行审核确认；
4. 对合同终止进行审核确认；
5. 根据合同约定，审核承建单位提交的支付申请，签发付款凭证。要求对项目合同进行合理的管理，以完善整个项目建设的过程。

### 1.3.7监理服务准则

遵照国家GB/T19668.1-19668.7《信息技术服务监理》的规定，以“守法、诚信、公正、科学”的准则执业，维护建设方与承建方的合法权益。具体应做到：

1. 执行有关项目建设的法律、法规、规范、标准和制度，履行监理合同规定的义务和职责
2. 不收受被监理单位的任何礼金
3. 不泄漏所监理项目各方认为需要保密的事项
4. 遵守国家的法律和政府的有关条例、规定和办法等
5. 坚持公正的立场，独立、公正地处理有关各方的争议
6. 坚持科学的态度和实事求是的原则
7. 在坚持按监理合同的规定向建设单位提供技术服务的同时，帮助被监理者完成起担负的建设任务
8. 不泄漏所监理的项目需保密的事项

### 1.3.8监理依据

1. 国家GB/T19668.1-19668.7《信息技术服务监理》、海南省有关信息系统项目建设和监理管理规范
2. 建设单位与承建单位签订的承包工程合同
3. 建设单位与监理单位签订的委托监理合同
4. 本工程招标书、招标过程文件、各中标商的投标书
5. 国家有关合同、招投标、政府采购的法律法规
6. 部颁、地方政府的信息工程、信息工程监理的管理办法和规定
7. 建设工程和信息工程相关的国家、行业标准和规范
8. 建设工程和信息工程技术监督、工程验收规范
9. 与工程相关的技术资料
10. 其他与本项目适用的法律、法规和标准
11. 国家、地方及行业相关的技术标准

### 1.3.9安全保密要求

本项目要求供应商制定一整套工程监理安全保密制度，确定工程保密责任人，同时要求供应商：

1. 按照国家、省、市的有关法规文件规定，要求监理履行保密责任，并与建设单位签订保密协议
2. 监理单位各级组织严格履行保密职责
3. 按照公司内部保密规定开展监理工作

### 1.3.10监理验收要求

1. 审核监理方应提交的各类监理文档和最终监理总结报告，综合评估监理方在系统开发进度、质量把关、重难点问题解决、项目投资等方面的监理情况。只有文档齐全，系统开发工作中没有出现重大质量事故才予验收。
2. 本监理工作的最终验收由委托方组织。

### **★**1.4商务要求

#### 1.4.1采购标的所属行业

本次采购标的所属行业为软件和信息技术服务业。

#### 1.4.2实施地点

采购人指定地点（海南省内）。

#### 1.4.3支付方式

1、签订合同后，采购人收到监理单位开具的正式有效发票之日起3个工作日内向监理单位支付合同款的30%（预付款）；

2、项目通过终验后，采购人收到监理单位开具的正式有效发票之日起3个工作日内向监理单位支付合同款的70%。

注：监理单位每次申请付款应提供付款申请书、符合采购人要求的等额发票及采购人报账所必须的相关材料。监理单位申请付款时，如监理单位提供的材料不完整、不真实，采购人有权暂缓付款而不视为违约。

### 1.4.4其它相关要求

#### （1）工作要求

监理单位须提供详尽的监理技术方案，包括但不限于施工组织部署、项目管理目标、施工准备、进度控制、质量管理、验收方法等内容。

#### （2）项目组人员要求（需按要求提供相应的证明材料并加盖公章）

监理单位应建立项目监理小组，负责整个项目的全程监理工作，本项目必须配备不少于5名具有信息系统监理师资格证书的专业工程师，其中包含1名总监理工程师及4名监理工程师，项目实行总监理工程师负责制，在整个项目建设期间，总监理工程师必须保证有三分之一工作日以上的时间到甲方现场，且必须在项目建设期间，项目全程常驻至少1名监理工程师在甲方现场。总监理工程师的变更，须事先经业主方同意。**所有人员必须属于供应商在册员工（在投标文件中提供在本单位2024年6月至今任意三个月的社保缴纳证明为认定依据或出具承诺函），并提供相应人员相关简历信息（提供身份证、毕业证或学历证、信息系统监理师资格证书），相关证明须加盖监理单位公章。**如中标后提供的项目团队与投标提供的团队名单材料不符，将追究法律责任。

#### （3）安全保密要求

本项目要求监理单位制定一整套监理安全保密制度，确定保密责任人，同时要求监理单位：

1、按照国家、省、市的有关法规文件规定，要求监理履行保密责任，并与建设单位签订保密协议；

2、监理单位各级组织严格履行保密职责；

3、按照公司内部保密规定开展监理工作。