哈尔滨市数字政府一期工程技术要求

一、自主可控要求

为落实党中央、国务院有关自主可控政策，本期完成部分应用系统的自主可控替代，其他应用系统须全部完成自主可控操作系统、数据库、中间件以及浏览器产品的兼容适配工作。

（一）本期新建系统，需进行自主可控，投标人需提供自主可控方案，包括政务数据资源中心建设（含主题库专题库建设、数据安全）、网格化管理平台、城市运行监测系统、运维服务平台、政务云运维平台、一体化安全运营（管理）中心。

（二）本期利旧升级系统，需逐步进行自主可控，投标人需提供自主可控的迁移计划，包括人口法人库应用升级、政务数据共享交换平台建设、统一身份认证升级改造、电子证照升级改造、电子印章升级及场景应用、统一政务服务网网站及移动端特色内容建设、一体化政务服务及创新应用建设、智慧政务大厅管理系统、数字政府运营大屏展示专题（省建市用）。投标人须在合同期内完成全部利旧升级系统的自主可控迁移部署。

（三）所有建设内容，需完成自主可控操作系统、数据库、中间件以及浏览器产品的兼容适配工作。

二、售后服务要求

本项目售后服务期自验收合格之日起至合同期满。投标人须提供本项目售后服务期间的人员驻场服务，并承担运维服务、运营服务。

（1）运维工作方式

1）主动监控：需支持实时、全面的系统监控，确保对硬件、软

件和网络状况有准确的数据展示，能针对发现的潜在问题采取应对措施。

2）预防性维护：需定期对系统进行整体巡检，根据检查结果优化系统性能，减少故障发生，优化方式包括但不限于更新补丁、检查安全漏洞、维护备份等。

3）一线响应：需提供 7x24 小时在线技术支持服务，确保软硬件的正常使用，在接到维修要求后应立即作出响应。

4）故障恢复与变更管理：需提供并执行详细的故障恢复计划，针对系统故障问题能做出快速响应。同时，需支持对系统变更进行记录与管理，确保系统整体的稳定性和可靠性。

（2）运维团队

1）组织结构：团队需制定扁平化、高效的组织结构，提供组织结构图，确保团队成员能快速进行联系及沟通。

2）提升培训：运维期内，每年需提供至少一次的培训，培训内容包括但不限于系统原理、操作使用、维护管理等，以提高项目组人员的技术水平，应对变化的技术环境。

3）运维记录：需定期提交以下记录报告，包括但不限于日常监控记录、月报告、软硬件日常维护报告、软硬件系统配置记录、软硬件改善建议、年度总结报告，应该按照系统运行维护要求及验收要求提交最终纸质材料。

（3）运维响应时间

1）一般问题响应时间：针对一般性问题，如用户咨询或系统常见故障等，响应时间须不大于 1 小时。

2）重大事件响应时间：针对重大事件，如系统宕机或安全漏洞

等，响应时间须不大于 15 分钟，确认设备出现故障时，须在 2 小时内提出解决方案。

3）故障恢复时间：恢复时间须满足线上故障 1-2 小时内、线下故障 4-6 小时内。

4）服务质量指标：针对与用户达成一致的服务质量指标，如系统稳定性、可用性等。

（4）人员驻场、运维服务、运营服务具体要求：

建设内容			驻场人员数量不少于（人）	运维工作内容及要求	运营工作内容及要求
1	数据资源中心建设	政务数据资源中心建设	4	要求提供技术支持服务 3 年，结合大数据平台建设情况，提供现场支持服务和远程支持服务。技术支持服务 1 年提供不少于 9 次的现场服务，每次现场服务不少于 5 天；每季度 1 次的日常巡检服务，每半年 1 次的深度巡检服务；不限次数的远程支持服务。技术支持服务要求包括方案类、支持类、使用类、保障类。方案类包括组件选型指导、应用对接、第三方平台对接、数据库设计指导；支持类包括产品能力咨询、组件/数据库开发指导、特性/工具使用指导、集群参数优化、组件/数据库优化指导；使用类包括变更支持、集群问题处理、日常巡检、深度巡检；提供重要时期保障服	无。

				务（上线保障及重大活动/节日保障）。要求提供 3 年协助运维服务，结合平台现网情况，提供定期协助运维服务。协助运维服务要求包括现网的故障远程/现场处理、现网设备的软件升级、现网日常巡检及现网风险管理和隐患排查服务。	
		人口、法人库应用升级	1	基础软件、支撑软件、应用软件、数据资源的服务响应、日常巡检、故障处理、数据维护。	无。
		主题库专题库建设	0	无。	要求自合同签订后针对本期建设的主题库专题库提供售后服务期内的主题库专题库运营服务，结合主题库专题建设情况，提供现场支持服务或远程支持服务。服务内容包含数据对接服务：汇聚通过 ETL、数据交换等技术以及人工数据填报、数据导入、数据接口接入解析；系统对接服务：实现不同系统接的数据整合；数据集成服务：基于各类数据的存在形式，提供多种数据集成方式。数据资源集成汇聚通过 ETL、数

					据交换等技术以及人工数据填报、数据导入、数据接口接入解析；日常性数据维护服务：要求处理数据资源变更维护需求，一旦数据资源出现如数据库表结构调整、元数据信息调整等情况，需要对目录、接口、数据汇聚采集任务、数据资源存储结构、数据服务内容、数据服务形式等进行综合调整。
		数据安全	1	无。	数据安全日常运营工作。
		政务数据共享交换平台建设	4	1、政务数据共享交换平台建设项目的运维实施主要是利用平台的各项功能，实现数据资源目录梳理、目录编制、资源挂接、共享对接、级联对接的数据服务过程，是数据共享交换平台建设的重要组成。 2、提供数据的实施服务，包括目录梳理、数据采集汇聚、数据质量治理、共享对接、级联对接的数据服务过程；提供对平台的日常性运维工作。	1、负责数据共享交换建设工作的整体谋划、组织协调和日常管理； 2、制定数据共享交换建设方案、技术方案，并组织实施； 3、组织人员培训； 4、制定数据共享交换有关规章制度；做好相关工作的监督检查等； 5、负责建立目标考核机制，对各部门承担任务的进展情况进行适时检查和通报；

					6、封装提供各级各部门数据共享使用需求接口； 7、完成与省级数据共享平台对接； 8、使用数据共享资源分析完成相关大数据统计功能更新与维护； 9、根据各部门提供数据共享汇聚情况完成数据共享系统目录编制、应用集成； 10、根据各部门电子证照应用需求提供电子证照使用能力。
		统一身份认证升级改造	0	1、升级维护：对哈尔滨市统一身份认证系统现有企业法人、自然人身份信息进行维护，能够对现有注册数据进行维护及管理。 2、接口维护：对哈尔滨市统一身份认证系统已对接的业务系统接口进行管理及维护，保证原有业务正常运行。 3、性能调优：根据系统监控或健康检查情况等情况，定期对系统进行配置修改或者调整来优化系统性能，避免系统在大业务量的情况下出现异常状况。 4、运行分析：通过定期安全巡检检查系统运行状况，除了解决应急故障，还需要对发现的问题进行定期汇总分	无。

				析，统计系统运行规律，为系统运行改进计划提供依据。	
		电子证照升级改造	4	1、按照项目服务规定完成相应项目打包部署工作，检查项目可用情况，项目文件禁止随意拷贝、复制到移动介质中。 2、检查并掌握应用服务进程运行情况、进程连接数、服务的正常启停。 3、检查并掌握应用服务参数配置更新前是否备份，日常日志是否按时检查。 4、检查并掌握应用服务器运行 CPU 利用率、内存使用情况、硬盘存储使用情况、网络连接情况、操作系统版本等相关指标项。 5、检查并掌握各应用系统数据库实例、监听运行状态，数据库是否能正常连接，数据库进程数，会话锁状态、死锁等异常状态情况。 6、检查生产应用系统数据库的变更、故障处理以及日常故障维护记录是否完整及抓取日志信息工作。 7、检查生产应用系统数据库参数配置文件备份，数据库数据备份清理，数据库归档日志清理脚本运行情况，数据库其他日志备份与清理。 8、按照要求规范项目运维相关内容，及时调整完善项目风险项。 9、掌握并检查项目服务器防火墙状态、开放端口情况、文档服务器限制	1、根据各部门电子证照应用需求提供电子证照使用能力； 2、与省级电子证照对接汇聚电子证照数据进行报送、上报； 3、根据各部门提供电子证照汇聚情况完成电子证照系统目录编制、模板制作、应用集成。

				情况。 10、严格按照运维工单要求，完成所有对互联网暴露开放服务器重点监管，保证互联网服务器内无敏感、涉密、项目、数据等文件暴露。 11、项目服务器中禁止存在跳板机及临时性中转服务器，文件、数据等项目相关文件禁止随意迁出当前服务器。 12、备份文件、项目文件留存应当保证运维工作完成后的备份清理工作，严格执行及备及还及清理。 13、检查并发现服务器中的常见病毒，如挖矿等，及时上报，并按应急预案要求将当前服务器断网隔离。	
		电子印章升级及场景应用	4	1、升级维护：对原有政府单位印章名称、印章编号、有效起始时间、有效结束时间、印章状态信息进行维护。 2、证书运维：能够对已发放电子印章及后期发放的电子印章配套的数字证书进行维护，提供数字证书的解锁、更新、补办等生命周期服务。 3、接口维护：对哈尔滨市统一电子印章系统已对接的业务系统接口进行管理及维护，保证原有业务正常运行。 4、性能调优：根据系统监控或健康检查情况等情况，定期对系统进行配置修改或者调整来优化系统性能，避免系统在大业务量的情况下出现异常状	1、业务服务 提供电子印章申请、审核、备案、激活、印章验证、以及电子印章冻结、解冻、更新、注销、删除等服务。 2、咨询服务 咨询服务贯穿于平台的数字证书、电子印章、云服务和注册用户生命周期的各个阶段，分析解决客户和用户提出的问题，包括售前、实施、运维、产品服务、服务使用操作

				况。 5、日常运维：提供技术人员的驻场服务，负责电子印章服务平台日常运行维护工作，并对项目其他节点提供远程技术支持服务。 6、运行分析：通过定期安全巡检检查系统运行状况，除了解决应急故障，还需要对发现的问题进行定期汇总分析，统计系统运行规律，为系统运行改进计划提供依据。	等各方面的问题。 3、工程服务 围绕客户解决方案而实施的各类活动，主要是云章服务的集成、产品方案实施。 4、支持服务 针对数字证书、电子印章和注册用户生命周期管理过程中的各种维护支持、电话支持、系统变更、应急响应等活动。 5、用户/客户/渠道自服务 提供业务查询、开通、业务应用配置管理、客户服务等自助服务。 6、热线服务、在线服务支持 向客户和用户提供热线、在线支持服务，对于云章平台相关技术问题，客户可拨打服务热线或在线提交问题，包括业务咨询、问题解决、使用操作、客户投诉等。 7、培训服务 针对客户培训涵盖产品服务的使用、集成实施、

					维护技能、安全知识等各个方面。
2	统一政务服务网网站及移动端特色内容建设		6	1、按照项目服务规定完成相应项目打包部署工作，检查项目可用情况，项目文件禁止随意拷贝、复制到移动介质中。 2、检查并掌握应用服务进程运行情况、进程连接数、服务的正常启停。 3、检查并掌握应用服务参数配置更新前是否备份，日常日志是否按时检查。 4、检查并掌握应用服务器运行 CPU 利用率、内存使用情况、硬盘存储使用情况、网络连接情况、操作系统版本等相关指标项。 5、检查并掌握各应用系统数据库实例、监听运行状态，数据库是否能正常连接，数据库进程数，会话锁状态、死锁等异常状态情况。 6、检查生产应用系统数据库的变更、故障处理以及日常故障维护记录是否完整及抓取日志信息工作。 7、检查生产应用系统数据库参数配置文件备份，数据库数据备份清理，数据库归档日志清理脚本运行情况，数据库其他日志备份与清理。 8、按照要求规范项目运维相关内容，及时调整完善项目风险项。 9、掌握并检查项目服务器防火墙状态、开放端口情况、文档服务器限制	1、按照省级对接标准完成哈尔滨门户网站建设上线； 2、按照标准与移动端的栏目持续上新运营建设工作； 3、建设宣传哈尔滨门户特色门户栏目上线运营； 4、建设宣传哈尔滨移动端特色门户栏目上线运营。

			情况。 10、严格按照运维工单要求，完成所有对互联网暴露开放服务器重点监管，保证互联网服务器内无敏感、涉密、项目、数据等文件暴露。 11、项目服务器中禁止存在跳板机及临时性中转服务器，文件、数据等项目相关文件禁止随意迁出当前服务器。 12、备份文件、项目文件留存应当保证运维工作完成后的备份清理工作，严格执行及备及还及清理。 13、检查并发现服务器中的常见病毒，如挖矿等，及时上报，并按应急预案要求将当前服务器断网隔离。	
3	一体化政务服务及创新应用建设	10	1、按照项目服务规定完成相应项目打包部署工作，检查项目可用情况，项目文件禁止随意拷贝、复制到移动介质中。 2、检查并掌握应用服务进程运行情况、进程连接数、服务的正常启停。 3、检查并掌握应用服务参数配置更新前是否备份，日常日志是否按时检查。 4、检查并掌握应用服务器运行 CPU 利用率、内存使用情况、硬盘存储使用情况、网络连接情况、操作系统版本等相关指标项。 5、检查并掌握各应用系统数据库实例、监听运行状态，数据库是否能正	一、创新应用 1、按照系统建设要求与部门调研，将调研结果实施至系统，对外提供服务； 2、完成创新应用相关系统培训、售后讲解服务工作； 3、针对用户提出的线上咨询进行解答； 4、根据民生大小事的业务需求，开发互联网+民生系统，以互联网+思维，重构民生大小事处理的

			常连接，数据库进程数，会话锁状态、死锁等异常状态情况。 6、检查生产应用系统数据库的变更、故障处理以及日常故障维护记录是否完整及抓取日志信息工作。 7、检查生产应用系统数据库参数配置文件备份，数据库数据备份清理，数据库归档日志清理脚本运行情况，数据库其他日志备份与清理。 8、按照要求规范项目运维相关内容，及时调整完善项目风险项。 9、掌握并检查项目服务器防火墙状态、开放端口情况、文档服务器限制情况。 10、严格按照运维工单要求，完成所有对互联网暴露开放服务器重点监管，保证互联网服务器内无敏感、涉密、项目、数据等文件暴露。 11、项目服务器中禁止存在跳板机及临时性中转服务器，文件、数据等项目相关文件禁止随意迁出当前服务器。 12、备份文件、项目文件留存应当保证运维工作完成后的备份清理工作，严格执行及备及还及清理。 13、检查并发现服务器中的常见病毒，如挖矿等，及时上报，并按应急预案要求将当前服务器断网隔离。	理念与思路，改革传统受理渠道单一、事件层层分转，完成我市民生系统运营调研实施工作； 5、开通整合便民服务频道，整合或新建用电、供水、排水、燃气、有线电视、供热、通信服务、公证服务、法律援助、信用服务 10 个方面的便民服务子系统，整合多方多项便民服务，做到一站式为民便民服务； 6、对接公租房办理系统，通过接口形式接入公租房自建系统，通过政务服务网将受理数据传送至公租房办理系统，办件结果回传至政务服务网的功能； 7、调研运营智能 OCR 表格提取识别在全市范围使用的高频应用事项与附件配置实施； 8、维护全市服务端盖章印模管理、发放管理、使用统计等； 9、调研分析全市汇聚电子证照情况，实施维护建

				设我市证易办运营服务； 10 调研运营全市事项申报过程中，实现个人一个身份证、企业一个营业执照即可在线上、线下办理相关事项； 11、调研分析全市汇聚电子证照情况，实施维护建设我市证易办运营服务，通过电子亮证，实现无证也可线上、线下办理相关事项； 12、调研运营我市涉及容缺办理服务事项与材料情况，升级审批办理系统，开发容缺受理、审批及事后补齐材料等功能，实现容缺办； 13、调研运营我市适合无感办理服务事项，梳理无感办目录，智能填单、自动适配材料，做到无感即办； 14、调研运营我市适合延时办线上线下服务事项，在线下大厅设置延时办窗口，通过全市预约系统，预约延时办，为工作繁忙无法在正常工作时

				间内到达大厅的申办人员服务； 15、调研运营我市可以通过远程验服务清单，开发远程验收系统，通过远程视频会商、在线填报材料等方式，实现建设项目、工程等的远程验； 16、运营完成二手房联动过户业务升级； 17、营运完成户政业务上网工作； 18、运营建设上线我市支付宝小程序与E冰城升级服务； 19 调研运营我市企业开办与注销服务新模式，完成相关业务建设运营； 20、调研分析全市汇聚电子公文结果文件情况，实施维护建设我市文易批运营服务； 二、受理中心 1、完成受理中心相关服务事项配置、对外服务能力； 2、完成受理中心巡检功能应用； 3、完成受理中心相关系

				统培训、售后讲解服务工作； 4、完成与省级受理中心平台对接，与业务调研实施运营工作。 三、办理中心 1、完成与部门间对外服务能力； 2、完成办理中心巡检功能应用； 3、完成办理中心相关系统培训、售后讲解服务工作； 4、与省级相关业务系统完成对接数据交换工作。 四、事项子库 1、完成事项中心相关服务事项配置、对外服务能力； 2、完成事项中心相关系统培训、售后讲解服务工作； 3、完成与省事项中心的对接及应用工作。 五、事项精细化梳理 多次开展市本级、区（县）、乡镇（街道）、社区（村屯）精细化事项梳理工作，将梳理结果录

				入事项库。并对创新应用中涉及事项方面内容进行优化、完善、编辑、入库。梳理内容包括：政务服务事项精细化梳理、民生事项梳理、创新业务梳理等。 六、办件子库 1、定期完成办件子库统计工作及统计表格及相关文档； 2、根据办件子库全量数据结果对比分析完成相关报表模块对接实施工作； 七、一件事一次办 1、按照省建市用一件事清单，地市需要按照省级一件事清单，完成一件事事项条线对接与能力上架。 2、按照地市需要建设一件事清单，按照省级一件事标准完成地市一件事接入能力配置实施办事指南、政策法规、一张表单等。需要按照省里能力接口标准，完成一件事能开上架与收件接口和结

				果反馈相关能力开发。 3、按照地市特有一件事，地市需要完成特有一件事集成对接。完成与省级统一赋码接口对接，省级一件事结果接口回传。 4、按照省一件事技术标准建设哈尔滨自有一件事系统中对接纳入，应用于哈尔滨大厅、窗口一件事服务能力。 5、哈尔滨市现有“一件事一次办”138 个，对照省级下发的“黑龙江市地级一件事建议清单”（40 个），共有 18 个”一件事一次办”与省级建议清单一致并已完成建设，本次建设中 18 项已建内容与省级平台进行免费对接，其他市级 120 项需到省级平台维护、对接。
4	智慧政务大厅管理系统	6	1、按照项目服务规定完成相应项目打包部署工作，检查项目可用情况，项目文件禁止随意拷贝、复制到移动介质中。 2、检查并掌握应用服务进程运行情况、进程连接数、服务的正常启停。 3、检查并掌握应用服务参数配置更新	1、对智慧大厅涉及所有使用者进行业务培训与技术支持； 2、维护智慧大厅各级大厅信息窗口人员信息。设备信息、预约叫号信息等相关实施运营工作；

			前是否备份，日常日志是否按时检查。 4、检查并掌握应用服务器运行 CPU 利用率、内存使用情况、硬盘存储使用情况、网络连接情况、操作系统版本等相关指标项。 5、检查并掌握各应用系统数据库实例、监听运行状态，数据库是否能正常连接，数据库进程数，会话锁状态、死锁等异常状态情况。 6、检查生产应用系统数据库的变更、故障处理以及日常故障维护记录是否完整及抓取日志信息工作。 7、检查生产应用系统数据库参数配置文件备份，数据库数据备份清理，数据库归档日志清理脚本运行情况，数据库其他日志备份与清理。 8、按照要求规范项目运维相关内容，及时调整完善项目风险项。 9、掌握并检查项目服务器防火墙状态、开放端口情况、文档服务器限制情况。 10、严格按照运维工单要求，完成所有对互联网暴露开放服务器重点监管，保证互联网服务器内无敏感、涉密、项目、数据等文件暴露。 11、项目服务器中禁止存在跳板机及临时性中转服务器，文件、数据等项目相关文件禁止随意迁出当前服务器。	3、对智慧大厅硬件设备及第三方控件使用及业务培训； 4、完成各级智慧大厅自我创新过程中的业务运营工作； 5、运营调研全市各大厅统一智能排队叫号系统对接； 6、运营调研全市各大厅建设帮办待办服务系统，建设运营我市现上线下全程帮办服务窗口； 7、调研运营我市与省级大厅统一赋码专区，建设一码通办服务系统； 8、运营推广我市四级联办服务专区，打通各区县各层级事项联办模式； 9、运营调研我市窗口呼叫终端使用，建设统一窗口呼叫终端系统； 10、运营维护大厅后台管理系统，主要实现对整个综合管理系统的功能模块、权限、角色、事项、日志、工作流、进行新增、修改、删除、查询等功能； 11、运营对接我市各级大

			12、备份文件、项目文件留存应当保证运维工作完成后的备份清理工作，严格执行及备及还及清理。 13、检查并发现服务器中的常见病毒，如挖矿等，及时上报，并按应急预案要求将当前服务器断网隔离。	厅与市级智慧大厅对接能力，完成相关数据采集与标准统一； 12 运营制定我市智慧大厅标准预约、叫号、取号、大厅收件、流转接口服务，完成全市各级大厅对接运营； 13、运营完成我市智慧大厅与省级智慧大厅同标准数据上报对接、设备硬件参数对接等； 14、运营完成我市政务服务自助终端业务升级，调研实施自助终端高频服务应用上线运营； 15、运营完成我市建设企业一站式服务专区； 16、运营完成我市建设人才服务专区； 17、运营完成我市建设咨询服务专区； 18、运营完成我市建设大厅智能导引服务； 19、运营完成我市建设大厅宣传屏； 20、运营完成我市四级联办专区； 21、运营完成我市建设一

				码通办服务专区； 22、运营完成我市设立远程视频咨询帮办专区；
5	网格化管理平台	10	1.根据系统培训需求，准备相应培训文档、用户手册。组织不同角色、不同区县进行多次系统功能培训。 2.制定项目日常运维相关制度，常态化支撑制度的有效落实，进行系统日常例行检查、状态监控。 3.提供项目日常运维工作文档统一留存和管理，对系统的运维全套项目文档，如《系统使用手册》、《运维方案》等，进行创建、版本、权限、安全、等全方位管理。 4.根据业务需要创建账号、分配权限、组织机构调整、工作流调整等系统配置工作。 5.驻场市级或县区指挥中心，收集需求并解答用户提出的各种问题。 6.按周、月统计网格化系统运行数据，按用户格式要求输出各类数据报表。 7.根据项目建设情况，编制项目汇报方案、演示 PPT，配合各级指挥中心进行系统演示和汇报宣讲。 8.提供项目各业务系统全部数据库备份、数据的管理服务，对重要系统数据、文件、应用程序按天进行备份，按天巡检核查备份结果，处理异常备份任务，确保备份数据高可用。	无。

				9.提供与项目相关的业务和技术咨询。出现无法解决的疑难技术问题，立即派有关领域的技术专家去现场解决。 10.根据收集的各区县定制化业务需求进行系统升级完善，如区县定制工作流、区县中心展示大屏、区县网格一张图等功能完善类开发工作。 11.根据用户提供的人口、楼栋、房屋EXCEl 数据,整理导入实有人口、楼栋、房屋本地库。	
6	数字政府运营指挥中心建设	数字政府运营大屏展示专题	1	在服务期内提供政府服务专题和（网格、电子印章等应用）六最品牌专题相关基础软件、支撑软件、应用软件、数据资源的服务响应、日常巡检、故障处理、数据维护服务。	服务期内需时刻确保指标呈现的准确性、及时性，高标准严要求做好日常运营工作。对政务服务专题和六最品牌专题，要求提供事项类指标准确性核查服务、服务办理类指标准确性核查服务、服务评价类指标准确性核查服务、专题指标准确性核查原因分析服务、专题指标准确性核查协调处理服务、专题应用运营服务报告输出服务、专题接待视察、汇报技术支撑服务。
		城市运行	1	基础软件、支撑软件、应用软件、数据资源、配套设备的服务响应、日常	无。

		监测系统		巡检、故障处理、数据维护、设备维护	
7	一体化运维服务平台建设	运维服务平台	0	针对一体化运维服务平台，在售后服务期内，结合客户平台现网情况，提供定期协助运维服务。协助运维服务包括主动预防服务、版本演进服务、运维管理服务、基础运维服务。主动预防包含重大故障复盘、运行分析、隐患排查、看网讲网；版本演进服务包含基础云服务版本升级、高阶云服务版本升级；运维管理服务包含问题管理、风险管理、资源和容量管理服务；基础运维服务包含变更实施、紧急恢复、问题处理、日常巡检等服务。	无。
		政务云运维平台	0	基础软件、支撑软件、应用软件、数据资源的服务响应、日常巡检、故障处理、数据维护	无。
8	一体化安全运营（管理）中心建设	安全运营中心	4	1、对安全运营中心巡检：每月一次，产出巡检报告。 2、安全运营中心策略调优：每月一次，重要时期按需。 3、平台配置运维：平台配置每周备份，每周检查平台服务正常运行以及端口正常开放，每月检查信息系统进行运行状态提供分析报告。每月检查安全运营平台账号和口令管理。	1、资产管理服务：使用安全运营中心每月导出平台报告。 2、互联网暴露面检测服务：项目开始时提供《互联网暴露面服务报告》，每季度提供增量报告。 3、威胁情报服务：根据安全运营中心内容实时评估、实时通报。一年不少于 50 份。

					4、协助加固服务：根据整体评估测试结果产出《安全加固方案》。 5、网站安全防护服务：每月输出《网站安全防护服务报告》，提供服务查询方式。 6、重要时期安全保障：前期梳理工作得出《安全梳理与整改细则》，在重保实时提供《重要时期保障日报》，以及提供重要保障结束后提供总结报告。
		政务外网安全监测平台	2	1、依托政务外网安全监测平台及专业安全工程师，对政务网及相关云资源和基础资源进行保障工作，其中包括安全检测、安全值守、安全监测、安全加固、应急演练、安全培训，以资产为核心了解当前资产受攻击面，为整体防护举措全面覆盖提供支撑； 2、依托政务外网安全监测平台及专业安全工程师，进行常态化的自检、巡检、整改等工作，协助采购人迎接监管单位检查、漏洞扫描、渗透测试、安全加固、基线检查等工作，通过安全检查和渗透等自检手段对发现的漏洞协助修补和加固。	1、演练前备战工作 准备工作、安全检测、安全加固、应急演练、安全培训，以资产为核心了解当前资产受攻击面，为整体防护举措全面覆盖提供支撑；排查网络空间存在威胁以及对应威胁对抗能力等级；对已知威胁进行封堵，对客观因素无法直接封堵的，采用加强监控，缓解措施的方法进行处置，由人工持续跟进。 2、演练迎战工作

					可针对演练期间出现的新漏洞、新威胁进行综合性分析，包括传播手段、技术原理、危害程度、演变趋势等，结合不同场景进行威胁评估，形成综合性分析报告。 针对影响网站及系统运行的重大隐患进行实时监控，监控内容包括网页篡改、挂马、暗链、域名劫持、后门、关键字等；对目标网站进行全天候的安全监测，若发现异常及时通报并处置。 演练期间提供现场值守，通过政务外网安全监测平台实时捕获的流量测威胁进行检测、发现、定位、响应、溯源。 演练期间提供应急响应，针对演练中可能发生的木马事件、感染式病毒事件、蠕虫事件、后门事件、网络攻击事件、网络扫描事件、网站挂马事件、网页篡改事件、拒绝服务攻击事件、网络钓鱼事件、信息泄露事件等威胁事

					件进行紧急安全措施，恢复业务系统到正常服务状态。 针对威胁事件进行专项分析，根据事件响应与处置以及安全设备监测结果进行取证分析；对涉及样本进行动静态分析、溯源分析、事件威胁评估；根据事件处置的建议与现有安全防护体系，给出事件处置与体系优化建议。每周输出《攻防演练周报》 3、演练后总结工作 将演练期间的工作内容、成果、问题进行总结与分析，输出《攻防演练总结报告》。
		业务应用安全	1	基础软件、支撑软件、应用软件、数据资源的服务响应、日常巡检、故障处理、数据维护。	无。
		密码安全建设	1	现场服务：根据系统现状派运维服务工程师到用户现场，提供及时服务； 服务包括：巡检、维修、故障排查、系统审计、重大活动保障、节假日值班、应急、技术培训等服务； 巡检服务：定期或不定期提供软件、硬件、系统、网络、安全等巡检服务，	日常业务受理、应急任务处置、保障软硬件正常运行、保障操作流程规范，提供对接接口，配合应用系统进行改造适配测试。

				提供详尽的巡检分析报告和建议，为后期的改进、优化等提供决策依据； 设备维修/保修：针对保修范围内的设备提供，免费上门、原厂商保修服务； 升级服务：产品将在发布新版本的补丁时，第一时间为用户发送升级包或上门提供升级服务； 重大活动、事件协助：举行重大活动或发生重大系统事件时，根据事件的紧迫性，派有经验的技术工程师赶赴现场协助用户处理，重大事件包括但不限于重大灾难、重大活动、重大安全事故协助服务。	
		服务体系建设	0	同安全运营中心。	同安全运营中心。

三、其他要求

1.中标单位须负责本项目与黑龙江省数字政府项目的对接工作，包括政务数据共享交换平台、主题库专题库、统一身份认证、统一电子印章、统一电子证照、统一政务服务网网站建设、统一政务服务移动端建设、事项管理中心（市级事项子库）、受理中心、办理中心、办件中心（市级办件子库）、统一智慧政务服务大厅管理平台建设、运营指挥中心建设（大屏）、网格化管理平台建设、一体化运维服务平台建设、一体化安全运营中心建设、政务外网安全监测平台、多云纳管平台等系统，接口规范参照省数字政府建设要求执行，相关技术文档可在黑龙江省营商环境建设监督局网站获取。

2.中标单位须负责本项目与市本级和九区九县政服务服大厅对

接，对接内容详见“项目需求详细要求”章节的“智慧政务大厅管理系统”内容。

3.中标单位须按照《网络安全法》《数据安全法》《网络安全审查办法》《关键信息基础设施安全保护条例》《个人信息保护法》等要求，落实网络安全相关工作。

4.培训：

（1）中标单位须面向哈尔滨市大数据中心、市直各业务部门、区（县）有关部门、使用市数字政府项目平台能力的单位及其相关支撑方进行培训；

（2）中标单位须针对领导层、普通用户层、系统管理员和应用级管理员、技术人员分级分层培训；

（3）培训内容包括数字政府发展趋势、数字政府建设思考及经验分享、哈尔滨市数字政府一期工程总体情况、哈尔滨市数字政府一期工程各系统培训；

（4）中标单位须组织通用维护培训，包括系统整体培训、业务系统培训、政务事项办理培训、系统运营运维培训等；

（5）培训方式包括但不限于理论授课、操作演示、实操测评、参观学习和其他必须的形式，确保参培人员能全面了解和掌握系统的基本理论、技术特性、操作规范。

5.中标单位须配合采购人组织举行数据开放高端论坛和数据开放应用创新大赛。

6.中标单位须按采购人要求制作宣传展示本项目建设应用效果的视频宣传片、多媒体课件、展示图片等内容。

7.中标单位须在项目建设实施过程中配合采购人建立本项目运行管理工作机制，并研究制定本项目各组成系统相关规章制度、技术

标准、工作规范、操作指南等文档材料，随本项目各组成系统验收同时交付。

8.项目验收时中标单位须向采购人移交本项目各组成系统全部账号、密码等管理信息，并在上述信息发生变更时及时通知采购人。

9.本项目须组织现场踏勘，现场踏勘地点：哈尔滨市党政机关大楼东配楼 5 楼电教室内（黑龙江省哈尔滨市松北区世纪大道 1 号）。具体现场踏勘时间以招标文件约定为准。

10.本项目中政务服务相关升级利旧内容，其升级改造部分由各系统用户单位提供必要的技术资料。

11.投标人须响应招标文件要求，并基于建设内容要求、自主可控要求、售后服务要求等，提供项目总体方案及各子系统建设方案。

四、项目需求详细要求

（一）数据资源中心建设

1．政务数据资源中心建设

具体技术（参数）要求
政务数据资源中心建设 建设大数据基础支撑平台、数据汇聚、数据治理功能，数据“一本账”展示、“一站式”申请、“一平台”调度等能力于一体的全市政务数据资源中心，实现全市政府公共数据资源的集中存储和统一管理。统筹全市政务数据资源综合管理，与国家、省级政务数据服务门户对接，承接上级数据平台数据回流。 一、大数据基础支撑平台 （一）系统架构 为持续稳定支撑数据资源中心的大数据处理需求，大数据基础平台系统架构方面应该具备以下能力： 1、 具备基于 Apache 开源社区版本演进，不使用私有架构和组件替代开源组件（如私有文件系统等），并具备跟随社区发展进行版本升级。

2、 具备大于等于 60 个，第三方主流生态工具对接。

（二）数据存储

根据政务数据发展的节奏，本期建设的大数据基础支撑平台存储必须满足未来两到三年的大数据发展要求，大数据平台应具备 PB 级别的海量数据存储能力，数据存储方面应具备以下能力：

1、 具备分级存储，具备集群中同一节点上配备不同类型的磁盘如 SSD、SAS、SATA 等，具备指定文件存放在指定类型磁盘上。

2、 具备 HDFS 组件上节点均衡调度和单节点内的磁盘均衡调度，避免小磁盘或小容量节点总是最先写满。

3、 在大规模集群场景下，HDFS 具备联邦部署（多对 NameNode）。

4、 在大规模集群场景下，HDFS 具备 DataNode 分组，保证集群性能不受影响。

5、 在大规模集群场景下，具备存储降压能力，降低元数据库的访问压力。

（三）数据分析

为支撑政务数据分析需求，大数据平台应提供分布式计算、流式计算、内存计算、交互式分析多种数据计算引擎，针对不同的场景和数据类型采用不同的计算模型，对数据进行大规模批量处理或者准实时处理，数据分析方面应具备以下能力：

1、 大数据平台单集群具备大于等于 2400 个运行作业。

2、 具备分布式交互查询引擎，具备海量数据实现高性能的交互式查询。

3、 具备同一套 Flink SQL 定义批量计算作业、流式计算作业。

4、 具备批流一体引擎，可执行批处理作业和流处理作业。

5、 具备在流上执行类 SQL 任务，SQL 能力至少包括：过滤、转换、基于窗口的计算能力、提供窗口数据的统计能力、关联能力、流数据的拆分与合并。

6、 具备与多种外部数据源集成，至少包括：Kafka、HDFS、HBase 或 JDBC/RDBMS 服务，便于实现涉及多种数据源的业务。

7、 提供可视化 Flink SQL 作业提交和任务管理能力。

（四）数据查询

政务数据经过分析引擎处理之后的结果数据，需要支撑大屏实时展示、BI报表、问题搜索、政务窗口业务受理等各种不同类型的数据查询场景，其中数据查询组件应具备以下能力：

1、 具备检索组件 HBase，用于主键查询（Key-Value）检索，查询条件简单，主要通过主键进行查询。

2、 具备检索组件 ElasticSearch，具备全文检索。

3、 具备内存数据库组件 Redis，利用其高速 key/value 存储查询能力，用于流处理结果数据的高速缓存。

4、 具备实时 OLAP 集市组件 ClickHouse，提供高并发、毫秒级 OLAP 分析能力。

5、具备 HBase 组件的二级索引，具备为列值添加索引，提供使用原生的 Hbase 接口的高性能基于列过滤查询的能力。

6、具备 HBase 客户端双读，具备同时读取主备集群数据。

3、 具备 SparkSQL，JDBC Server 具备多租户并行执行，租户任务提交到不同的队列执行，租户间资源隔离。

4、 具备慢 SQL 监控、告警、一键停止。

5、 具备可视化的数据迁移操作，具备限速、定时任务、一键均衡。

6、 具备 LB 的高可靠，server 单点故障不影响业务。

7、 具备 ClickHouse 组件可视化元数据、业务数据备份恢复能力。

8、 具备一主一从模式的 Redis 集群，系统自动计算节点上可安装的 Redis 实例个数并分配主从关系。

9、 具备 Redis 集群的性能监控功能，可以通过直观的曲线图方式，了解当前 Redis 集群、实例的 TPS 吞吐量情况。

10、 具备 Redis 集群提供了多种告警，例如集群下线告警、持久化失败告警、槽位分布不均告警、主备倒换事件、集群高可靠性受损告警等。

（五）资源管理

大数据平台汇聚了海量的数据，针对这些数据的会提交海量的计算处理任务，大数据平台需要合理的分配和调度存储、计算资源，以确保多种应用和作业可以在集群上持续平稳的运行，在资源管理方面应具备以下能力：

1、 具备合理的分配和调度存储、计算资源，以确保多种应用和作业可以在集群上平稳运行。

2、 具备多租户管理能力，将大数据集群的资源隔离成一个个资源集合，彼此互不干扰。

3、 具备队列层级，管理员可针对实例为队列同时配置绝对值或百分比的资源策略计划。

4、 具备 YARN 集群中的节点可根据容量或业务类型不同，进行分组以使队列更有效地利用资源。

5、 具备基于租户的资源预留策略，部分租户可能在某些时间中运行关键任务，租户所需的资源应保证可用。

6、 具备基于时间的服务资源动态调整，来动态自动调整各服务在不同时间段可用系统资源。

7、 具备通过资源预留策略的机制，在这些租户队列运行的任务可立即获取到预留资源。

8、 具备队列内用户间共享资源的配置能力。每个租户中可能存在不同权重的用户，高权重用户可能需要更多共享资源。

9、 具备将计算资源划分为不同的资源池，租户可在不同的资源池配置不同的租户资源。

10、 具备服务资源静态隔离，即具备对系统中不同服务的资源使用上限进行配置，保证各服务的资源使用不会超过配置上限。

11、 具备在同一集群内同一组件部署多个服务，服务之间资源相互物理隔离。

（六）平台组成

大数据平台组件众多，不同的组件对于硬件需求各不一样，为支撑大数据平台的各组件持续稳定的运行，大数据平台组成部分应满足以下要求

1、 具备多种常见国产操作系统（欧拉 OS、中标麒麟、银河麒麟、统信 UOS 等）。

2、 具备全组件 IPv6 协议。

3、 具备 X86、ARM 单集群内混合部署。

4、 具备滚动升级能力，业务不中断。具备一次升级少量节点、循环滚动，直至集群所有节点完成升级。

5、 具备自动健康检查与巡检，可实现一键式系统运行、健康度巡检和审计，保障系统的正常运行，降低系统运维成本。

6、 具备需要对集群内节点的服务使用端口情况加以控制，并提供各服务和组件使用的端口说明。

7、 具备大数据平台系统级安全加固，具备 Kerberos 认证，具备认证鉴权，具备表和列加密以及数据加密，具备全系统的审计能力。

8、 具备 Flink/Redis 功能。

9、 具备数据湖/HBase 功能。

10、 具备 ElasticSearch/Kafka/Clickhouse 功能。

（七）平台可靠性

大数据平台承载政务数据的重要业务，为保证政务业务的持续稳定的运行，平台需要从集群、节点、数据等各个层面均要考虑整体的可靠性，平台可靠性方面应具备：

1、 具备界面化管控集群中各个组件的配置，并且修改配置后，具备滚动重启组件生效，对业务无影响。

2、 具备数据的快速备份和恢复，可以将元数据存储到其他服务器，具备多种备份目的地。

3、 具备组件进程故障后具备自动重启恢复，无需手动干预。

4、 具备单集群跨 AZ 部署，单 AZ 故障，数据不丢失，业务无影响。

5、 具备运维管理平台系统在内的所有业务组件的管理节点均实现双机 HA，业务无单点故障。

6、 具备主备集群容灾，且至少具备 HDFS、Hive、Elasticsearch 等组件。

7、 具备管理平面与业务平面的网络隔离，防止业务平面的高负载对集群管理通道造成冲击。

8、 具备对节点亚健康状态的侦测，在紧急状况下，部署认证服务的关键节点自动重启节点以恢复业务。

9、 具备界面化定义用户、用户组、角色；权限管理具备库、表级别的访问权限控制。

10、 具备通过对节点硬件（特别是硬盘）、操作系统、进程的监控，及时发现相关部件的异常状况。

11、 具备标准加密算法 AES、国密算法 SM4，并具备自定义加密算法。

12、 具备发生文件损坏的问题，平台对数据写入的全路径进行了优化，确保系统异常掉电后，业务仍能可靠地启动。

13、 具备对节点亚健康状态的侦测，在紧急状况下，部署认证服务的关键节点自动重启节点以恢复业务。

（八）平台运维

为保证大数据平台的稳定运行，需要提供便捷的集群运维能力，从告警、补丁、运维支撑等方面考虑平台的运维能力，相关能力需要具备：

1、 具备图形化集群健康巡检工具，能够检查集群相关节点、服务的健康状态，可提前发现集群中潜在的问题，并生成健康检查报告。

2、 具备大数据集群服务可以实时监控大数据集群，通过告警和事件可以识别系统健康状态。

3、 具备自定义配置监控与告警阈值用于关注各指标的健康情况。当监控数据达到告警阈值，系统将会触发一条告警信息。

4、 具备补丁操作，需要及时发布大数据平台组件的补丁，以及时解决组件的问题。

5、 具备补丁安装一键式操作，通过滚动安装，补丁升级不会停止业务，保障集群长期可用。

6、 具备高可靠、安全、容错、易用的集群部署和管理能力，具备大规模集群的安装/升级/补丁、配置管理、监控管理、告警管理、用户管理、租户管理等。

7、 具备组网规划工具进行安装前的规划，指定基本设置、节点拓扑，磁盘规划等基本规划信息。集群具备按照规划内容一键启动安装。

8、 具备对已有大数据平台添加新的服务，具备删除大数据平台中的服务。

9、 具备大数据平台参数动态生效，实时修改实时生效，无需重启组件，减少业务影响。

二、数据汇聚平台

（一）数据源管理

1、具备同构/异构数等多种数据源源之间批量数据传输能力，具备多种同构、异构数据源之间的数据迁移，具备多种同构、异构数据源之间的数据单向、双向迁移。

2、具备通过 URL 连接信息、账号、密码等信息来新增数据源。

3、具备删除无效的数据源。

4、具备根据相关信息来搜索数据源。

5、具备查看数据源详情，信息包括名称、连接 URL、账号、地址、描述等信息。

6、具备在新建数据源过程中测试连接数据源。

7、数据源具备连接源端数据库、文件服务器和消息队列。

8、在数据源建立过程中，具备测试连接是否正常，防止配置的连接信息（URL、账号、密码等）错误，避免在任务执行过程中出现此类错误。

（二）数据集成

1、具备针对关系型数据库的数据接入。

2、具备操作界面配置整库迁移，具备整库迁移表的筛选。

3、具备整体迁移关系数据库和数据仓库。

4、具备关系型数据库、HBase、MongoDB、ElasticSearch 整库迁移。

5、具备文件增量迁移和使用 Where 条件配合时间变量函数实现增量数据迁移。

6、具备文件增量迁移和数据库增量迁移。

7、具备半结构化数据接入。

8、具备非结构化数据接入。

9、单一租户可创建多套集成平台实例，一个控制台可对多个实例进行统一管理。实现信息共享，打破平台、云、网络、地域边界，实现业务数字化全联接协同。

10、集成平台将数据、服务、消息、设备等集成技术融合，统一管理，唯一的租户、子账户及访问权限，完成数字资产的融合集成。

11、具备 IPv4/IPv6 双栈。

12、具备多实例间的级联能力，具备平滑扩容能力，扩容期间业务不中断。

13、具备集群化部署与跨 AZ 部署，确保服务高可用性，提供单实例的跨 AZ 高可用能力。

14、具备数据库到 API 的转换发布能力，降低应用开发的用数难度，支撑应用快速创新。

（三）批量数据集成

1、具备异构数据库之间整库迁移。

2、具备周期任务策略，具备与数据开发调度集成，具备时间宏能力进行作业参数的替换能力。

3、具备分、小时、天、周、月级别周期任务策略，具备时间宏替换。

4、集成平台具备跨网穿越网闸或防火墙访问不同云及网络的数据源，数据汇聚的同时，不破坏企业的安全边界。

5、具备文件系统，关系数据库，数据仓库，NoSQL，大数据云服务，对象存储等数据源。

6、具备自定义及自动映射两种方式关联数据源字段与目标数据源字段。

7、具备对创建的数据集成任务进行启动、停止、修改等管理操作。

8、具备任务调度：按照时间（实时、定时），数据量（增量、全量）等来调度任务。

9、具备用户自定义开发连接器，满足用户私有协议对接诉求。

10、具备用户自定义需要集成的数据库表及数据库字段。

11、具备对汇聚的数据同步到其他数据处理系统，通过数据采集系统创建数据采集接入的数据集成任务，完成数据的采集接入。

12、具备代理，解决数据源因安全或者组网限制，无法暴露在公网场景。（四）增量数据集成

1、具备基于数据库日志的增量数据同步能力。

2、具备对汇聚的数据同步到其他数据处理系统，通过数据采集系统创建数

据采集接入的数据集成任务，完成数据的采集接入。

3、具备页面向导式配置迁移任务，具备源字段到目的字段的字段映射配置，具备作业失败重试配置以及是否定时执行等配置。

4、具备整库表搬迁，适用于将本地数据中心同步迁移到云上的数据库服务或大数据服务中。

5、具备批量数据迁移在迁移过程中对字段进行转换，具备字段转换方式：脱敏、去前后空格、字符串反转、字符串替换、去换行、表达式转换。

6、具备脏数据归档，将迁移过程中处理失败的、被清洗过滤掉的、不符合字段转换或者不符合清洗规则的数据单独归档到脏数据日志中。

7、具备迁移任务的整体并发度设置，不同配置的批量数据接入集群，具备的作业并发数也不同。

8、具备不改变用户表结构即可进行增量同步。

9、具备实时、定时，增量、全量，灵活调度，客户可以根据自己的场景配置。

（五）流式数据采集

1、满足数据实时集成的需求，包括：日志、消息、点击流等流式数据采集。

2、具备高可靠消息总线引擎消息集成。

3、具备关系数据库中实时变化的数据通过 CDC 工具捕获和解析，转换成消息发送到 Kafka 消息队列，由 Flink 接收处理写入 Hudi。

4、具备基于消息队列的设备数据实时上报到 Kafka，然后由 Flink 接收处理写入 Hudi。

5、具备事务消息功能，保障核心业务和多个下游业务的执行结果完全一致。

6、具备任意时间秒级定时消息集成采集。

7、具备消息持久化，多副本存储机制。可选择副本间消息同步、异步复制，数据同步或异步落盘等多种方式。

（六）应用数据采集

1、具备调用数据源的 API 接口获取数据并将数据写入目的端大数据中心。

2、具备 API 数据源管理，包括数据源的额创建、修改和删除功能。

3、具备集成任务创建，配置任务名称、集成模式、目标应用、源应用信息。

4、具备集成任务管理，可以对任务进行查询，展示任务名称、集成模式、运行状态、创建时间、开始调度时间等。具备对任务的启动、停止、编辑、计划制定、任务日志查看、删除。

5、具备定时调度 API 数据源集成任务，具备按照分、时、日、周、月的单位进行定时调度。

6、具备数据的增量、全量同步，通过配置开始时间段、结束时间段增量采集数据。

7、具备读数据插件，支撑数据集成任务快速配置读取数据的数据源，具备不同类型数据源读取的数据实现元数据转换。

8、具备写数据插件，支撑数据集成任务快速配置待写入的目标数据源，具备分片写入数据。

9、具备任务监控，对创建的数据集成任务的运行情况进行监控，并对异常的任务进行处理，保证业务正常运行理。

10、具备通过自定义和自动映射两种方式关联 API 数据源字段与目标数据源字段。

11、具备自定义连接器，具备根据业务需求开发相应的数据源插件，实现对该数据源的读写。

（七）数据集成作业监控

1、具备全量同步数据量增长缓慢的非核心数据。

2、具备增量同步有时间戳以及增删改标识字段。

3、具备基于数据库的所有变化写入到日志做实时同步。

4、具备数据迁移过程中进行脏数据处理，包括字段级转换、字段扩大处理、数据条数一致性检查等处理

5、具备在数据采集过程中，进行数据获取进度管理，监控数据获取状态，设计数据补救措施。

三、数据治理平台

（一）数据架构模块

1、具备流程设计和管理：新建、导入、导出、删除等操作。

2、具备信息架构管理，统一入口进行主题库建设，管理数据资产目录（业

务分层）、数据标准、数据模型等。

3、具备业务分层管理，实现对业务分层的管理查询，默认具备主题域分组、主题域、业务对象三层架构管理，具备自定义业务分层。

4、具备基于事实表的星型模型与雪花模型建设，具备多级维表管理。

5、具备自定义数据标准模板，通过自定义数据标准模板，具备不同行业的数据标准需求。具备自定义数据标准模板，满足各个行业的数据标准需求。

6、具备向数据目录模块同步所有元数据信息，包括业务元数据、技术元数据、管理元数据。

7、具备维度建模，具备维度表、事实表、汇总表模型设计，具备多级维表、维表层次管理。

8、具备数据架构数仓、Hive、SPARK 等数据连接类型。

9、具备设计即代码，技术指标设计完成后，自动生成数据开发作业脚本。

10、具备各类数据模型的导入导出功能，包括业务分层、码表、关系建模等。

11、具备基于维度建模的统一指标建设，包括自定义业务指标、技术指标，消除歧义，统一计算公式、统一指标口径。

12、具备模型物化，关系建模的业务表以及维度建模的事实表、维度表、汇总表都具备发布后直接在数仓中创建并同步。

13、具备针对原子指标、衍生指标、业务指标、事实表、维度表等进行审核后发布。

14、具备查看待审核申请和已审核对象。

15、在数据源管理、元数据管理、数据质量管理、数据标准管理、数据模型管理、数据共享服务、数据资产报告、数据安全管理、兼容性、安全性等方面均需满足数据管理平台基础能力评测要求。

（二）元数据模块

1、提供元数据采集、元数据综合管理、元数据分析、元数据全文检索，形成整个数据资产地图，展示、管理全局系统资产。

2、具备元数据综合管理，具备从技术元数据、业务元数据、管理元数据三个维度管理。

3、具备管理元数据范围：元数据存储管理信息、元数据管理流程信息。

4、具备元数据分析，包含图形化展示元数据对象表、以及过程的始端依赖关系，实现清晰的元数据血缘关系追溯。

5、具备元数据快速查询能力，通过元数据检索快速定位元数据，查阅元数据基本信息、任务信息、数据服务信息等。

6、具备创建自定义策略的采集任务，采集数据源中的技术元数据。具备自定义业务元模型、批量导入业务元数据、关联业务和技术元数据、全链路的血缘管理和应用。

7、具备通过数据地图的多级多类的资产目录，形成全面、完整的数据资产体系，梳理盘点数据资产，掌握数据资产现状。

（三）数据开发与集成模块

1、具备数据开发作业具备流处理和批处理混合编排。

2、具备丰富调度机制：时间周期调度，基于消息通道的事件调度，具备设置作业间的依赖关系。

3、具备通过图形化所见即所得的 ETL 编辑器实现 ETL 能力，具备数据抽取、清洗、转换、加载，用户可以避免写大部分 SQL、Python、Java 代码。

4、具备丰富作业运维手段：重新执行作业某批次任务，给作业补数据，对运行中作业暂停部分节点。

5、具备多种大数据服务引擎编排，包括 Hadoop 大数据平台、数据仓库。

6、作业结果具备邮件、短信通知。

7、具备局部参数和全局参数。

（四）数据资产模块

1、具备丰富的数据连接，包括数据库、数据仓库、大数据云服务数据源连接。

2、具备数据源元数据采集和存储；具备配置采集策略，选择需要采集的数据库、数据表、时间范围；具备采集任务调度策略，具备周、天、小时、分钟定时调度或手动调度等。

3、具备元数据更新，具备数据表 Schema 更新以及数据表删除等同步策略。

4、具备任务监控，具备采集任务监控，按状态、时间、名称搜索过滤，具备采集任务停止、取消、重跑、查看日志等操作。

5、具备创建多级数据目录，具备数据资产多维度查询。

6、具备查看数据资产详情，如表的 schema、表大小、创建时间、创建人、标签、关联关系。

7、具备标签定义和管理，具备给数据资产打标签。具备标签管理，标签搜索，标签可以通过搜索添加，对于不存在的标签具备实时添加，具备批量操作。

8、具备数据开发过程元数据采集和管理，与数据表自动关联呈现，自动解析数据血缘，具备跨作业数据血缘关联构建和呈现，数据开发全过程元数据采集，自动解析数据血缘，具备跨作业数据血缘关联构建和呈现。

9、具备业务分层和数据模型作为业务资产管理和呈现。

10、具备资产概览，具备数据表大小、来源、数量等维度统计数据资产概况。

（五）数据质量模块

1、数据质量包括准确性、唯一性、一致性、及时性等方面的内容，具备从组织管理、流程、技术等多角度多层面进行管理。

2、具备稽核规则配置、稽核任务管理、问题处理、质量分析等一体化管理能力。

3、具备对数据质量的全程监控。在各数据质量检测点上，可灵活配置数据质量检查规则，并提供常见问题的处理方法。

4、具备质量统计功能，包括展现质量报警和质量规则统计信息，以及近期报警、最近 7 天报警统计、最近 7 天规则统计、当日报警分类统计、报警分类趋势。

5、具备数据治理规则目录管理功能，按照目录管理和运维质量规则、运行任务等。

6、具备业务指标监控功能，具备创建自定义业务指标、规则和场景三层架构监控数据质量。

7、具备规则管理功能，具备基本数据质量监控规则。具备规则运行功能，具备多引擎、全库全表及条件扫描数据源，通知报警及向数据资产打标签功能。

8、具备质量规则通过数据开发作业的开发功能进行关联调度，自动生成质量监控结果。

9、具备创建对账作业，对作业或数据运行结果或质量进行自动和周期性检

查。

10、具备提供基于技术和业务维度的质量报告，具备查看评分历史趋势变化。

（六）数据服务模块

1、具备在线开发、调试、发布数据服务 API，通过配置、脚本实现 API 的开发和在线调试。

2、具备数据 API 开发，通过编写 SQL 脚本的方式，将数据库提供的数据服务转换为 REST API 的能力。

3、具备 API 生命周期管理，对 API 进行注册、授权、导入导出、分组、域名、环境变量、发布、修改、下线、删除等进行统一管理。

4、具备流量控制，对调用 API 的次数进行限制，具备秒、分钟、小时、天级别的设置。具备对 API、应用、用户、源 IP 的流量控制。

5、具备 API 级联，对需级联实例的 API 配置级联方式，代理到被级联实例的 API 网关某个 API，并且建立专属的认证通道，避免与被级联 API 认证冲突。

6、具备安全访问控制，对开放的 API 进行访问认证和安全管控，提供 APP 认证、自定义认证等多种认证能力，提供 IP 黑白名单访问控制。

7、具备策略路由，对请求路径和参数进行识别，并转发到合适的后台服务，具备根据不同的 Header、Query 来定制 API 接口的后端。

8、具备 API 监控分析，通过 API 调用分析获取访问 API 的请求次数、出错统计、数据流量和调用时延等指标内容。

9、具备 API 编排，通过编写 JS 脚本完成服务的编排封装，将多个原子 API 编排成场景化 API。

10、具备 API 协议和数据格式转换，包括 REST 转 SOAP， JSON 转 XML。

11、具备通过数据服务来实现动态脱敏。

2．人口、法人库应用升级

具体技术（参数）要求
人口、法人库应用升级 现有人口、法人库能力如下：已将公安局、民政局、计生委、公积金管理中心、人社局、房产局、残联纳入数据源单位，数据涵盖人口基本信息、收入信息、

资产信息、家庭关系信息、单位信息、状态信息等类别信息，目前提供 17 类基础信息持续维护更新和 30 项数据核查服务。

本期升级人口扩展数据库、法人扩展数据库，形成信息共享和校核机制，实现一数一源、多源核对、权威发布。支撑政府跨部门间业务协同联动，提高政府部门工作效率和监管能力，提升城市管理水平与公共服务能力。

（一）利旧要求

需提供人口法人扩展库建设对原有人口法人共享应用系统的利旧和升级方案。

功能要求

（二）本次平台建设主要建设内容需包括：优化数据共享系统、优化现有数据资源、优化数据核查服务、优化数据存储系统、优化数据采集系统、增加基础数据类别、探索数据向基层回流、新增系统数据范围、新增数据分析系统、新增数据服务支撑系统、新增综合展示系统、新增资源服务系统。

1、优化数据共享系统

需满足优化哈尔滨人口和法人信息共享系统，使其成为各数据源单位开展“人口”和“法人”信息资源交换的主要渠道，有效支撑资源共享和跨部门业务协同；围绕“采集、归集、治理、应用、安全、运营”的公共数据全生命周期，完善人口和法人数据交换共享标准，建立以公民身份号码、姓名为标识人口信息库和以统一信用代码、法人名称为标识的法人信息库，实现数据的标准化管理，保障数据的完整性、一致性、规范性，为后续的数据管理提供标准依据。

2、优化现有数据资源

需满足依据哈尔滨数据共享平台资源目录清单中的机动车基本信息、死亡医学证明、社会团体法人登记证书、企业基本信息、个人公积金缴存信息、商品房合同签订信息、纳税人基本信息等替代系统原有更新停滞的数据。

3、优化数据核查服务

需满足利用多源数据并结合数据核查模型，为各委办局核查工作提供支撑。具备各级用户根据不同信息种类、不同检索频度的查询，提升核查数据承载量，满足大批量数据核查的需求，从而增强数据核查服务能力；需满足完善数据核查授权机制，按照不同权限对核查申请、审批过程留痕。满足各委办局核查业务需

求的同时，做到核查流程清晰、核查数据可追溯；需满足具备多格式返回核查结果，为数据主题应用提供数据服务，满足各类业务和行业发展对公共信息交换需求。

4、优化数据存储系统

需满足将“人口”和“法人”信息按照静态和动态数据进行划分，分别采取不同存储方式，为信息持续汇聚提供支持。

5、优化数据采集系统

需提供通过统一的资源采集模块，对数据进行资源采集，便于数据统一化管理，最终实现以人口、法人静态数据为基础，阶段性汇聚动态数据，逐步形成哈尔滨人口、法人基础数据。采集时，应依托黑龙江省数据共享平台和哈尔滨市数据共享平台数据资源，结合全市核酸检测系统人口台账信息按需持续采集人口和法人相关数据。

6、增加基础数据类别

需满足增加工程建设项目招投标交易公告信息、矿业权出让交易公告信息、国有产权公告交易信息、土地使用权交易公告信息、组织机构信息、不动产信息证明等，满足“人口”和“法人”数据横向核查需求。

7、探索数据向基层回流

需满足依托该系统，按照组织架构与业务权限，建立社区库、行业库、专题库，社区可授权调取市、区（市）政务数据平台数据，解决基层应用数据难题。

8、新增系统数据范围

需满足新增工程建设项目招投标交易公告信息、矿业权出让交易公告信息、国有产权交易公告信息、土地使用权交易公告信息、组织机构信息、不动产证明信息等。满足“人口”和“法人”数据横向核查需求。

9、新增数据分析系统

需提供数据分析系统功能，主要是通过大数据技术对已有资源进行分析，将多部门数据进行比对通过数据挖掘、数据分析，构建完善的人口和法人数据模型，为上层应用提供数据支撑，为领导决策提供科学依据。比如利用人口和法人数据对税收清缴、养老金清缴、重度残疾人居家托养补贴、个人所得税专项扣除、经济活跃度、货物购销链、企业经济关系、产业链情况、企业（复工复产）生产情

况等场景进行分析预测；对低保待遇资格、低保低困低收入补助资格、保障房资格、供暖费资格、交通补助资格、高考加分资格、学区房户口资格进行审查。

10、新增数据服务支撑系统

需提供数据服务支撑系统，通过数据前置服务，为数据需求方提供目标数据。采用开放、稳定、可持续发展的软硬件技术，为各业务应用提供统一的用户会话、业务服务、计算处理、数据管理等应用支撑服务，并采用“标准先行”建设思路建设应用支撑标准体系，可以承载后续项目中应用系统的开发和运行，对接已有系统，提高信息系统的适应能力和处理能力，满足用户中长期业务与信息化的发展需要。

11、新增综合展示系统

需提供综合展示系统，综合展示系统负责将数据平台中抽取的数据展示到大屏上，展示页面数据由各应用系统提供。包括数据同步情况展示、核查业务综合展示、委办局核查业务综合统计展示、热点核查业务排行、数据治理情况展示等。

12、新增资源服务系统

需提供资源服务系统，资源服务系统主要是拓展数据服务对象，做到数据资源可横向服务于政府各级部门，为领导决策及业务拓展提供数据支撑，纵向服务于老百姓，为便民服务提供数据支持，并结合热点数据分析技术主动推送便民信息，提高老百姓的办事效率。

（三）信息资源规划和数据库建设要求

1、信息资源规划

需提供人口、法人扩展库建设的信息资源规划内容。

2、应用服务资源库

需以人口法人数据中心建设为主线，逐步形成数据统一标准规范。通过数据整合，形成人口数据共享机制。整合各方信息资源形成各类企业、政府部门与人口法人系统之间的信息交换与共享机制。另一方对人口法人数据进行整合与分析，为监管部门、政府管理部门决策提供支持依据。

（四）应用支撑平台和应用系统建设要求

1、基础支撑平台

本项目需满足应用支撑平台的建设采用开放、稳定、可持续发展的软硬件技

术，为各业务应用提供统一的用户会话、业务服务、计算处理、数据管理等应用支撑服务，并采用“标准先行”建设思路建设应用支撑标准体系，可以承载后续项目中应用系统的开发和运行，对接已有系统，提高信息系统的适应能力和处理能力，满足用户中长期业务与信息化的发展需要。

功能需包括可视化编辑器、自定义主题配置、可视化图表辑器、图标数据源管理、自定义组件管理、可视化模板管理、智能搜索、微服务治理组件。

2、数据共享服务升级

需满足人口法人数据共享服务利用云计算技术整合政务信息资源，促进信息共享利用，推动政府对“自然人”和“法人”的精细化管理。解决政府部门间条款矛盾突出、信息共享等问题，打破信息“孤岛”和“壁垒”。包括共享策略升级、共享标准升级、共享分类升级。

3、业务管理平台

需提供包括机构管理、用户管理、角色管理、权限管理、通知管理、规则管理、流程管理、审批管理、状态管理、结果查询、模型升级、公众服务功能。

4、业务分析系统

需提供核查业务智能分析、科技企业数据分析、房租赁补贴发放分析、公共租赁住房资格申请与审核分析、养老金清缴分析、重度残疾人居家托养补贴复核、税收清缴、学区房户口资格复核、企业（复工复产）生产情况、公众服务分析功能。

5、工作门户系统

需提供工作门户功能，通过对单点登录、目录检索、信息发布、交流反馈等功能的整合，将各种核查应用、数据资源集成到一个信息管理平台之上，并以统一的用户界面提供给用户，并建立单一入口的完整信息通道，安全可控地释放存储在内部和外部的各种信息数据。

3．主题库专题库建设

具体技术（参数）要求
主题库专题库建设 建设政务服务主题库、市场监管主题库、社会发展专题库、12345 热线专题

库、民生保障专题库，统一纳入一体化政务数据资源体系管理，实现多个部门或多个应用系统间的“共建共用”。对各类业务资源主题专题数据库实行规范管理。

主题库和专题库的建库需要经过一系列的操作流程。首先将数据从共享、开放的前置库采集到原始库，然后对原始库中的原始数据进行质量检测和标准化处理，处理过程中将有问题的数据存储到问题库，并且形成数据质量报告，同时将问题数据反馈给相应的委办局，进行数据修订；有效数据存储到中间库，为后续流程提供标准数据支撑。根据建模需要，抽取中间库标准化数据，进行融合治理，形成主题库和专题库。

（一）市场监管主题库

市场监管主题库建设：提供市场监管库建库方案，将来自市场监管、药品监管、知识产权、住建、烟草专卖等部门市场监管相关数据如：监管事项、监管对象、执法人员、监管行为、风险预警、信用监管等数据进行汇聚、治理、关联整合、分析计算，形成结构相对稳定、维度相对齐全、度量相对丰富、质量相对较高的市场监管主题数据库。

可根据业务情况建立如下指标分析模型：

企业活跃度分析，跃度是当前大数据时代在经济领域被广泛应用的专业术语，是用来分析研判和评估衡量各种经济活动的量化指标体系。

企业成长性分析，收集、整理区域政策、市场、资源、管理和企业等有关数据资料，建立企业成长性综合评价台账。分别评价影响企业成长性的管理成长性、经营成长性状况，汇总得出企业成长性综合评价结果。

企业风险度分析，收集、整理区域政策、市场、资源、管理和企业等有关数据资料，建立企业风险度综合评价台账。分别评价影响企业风险度的管理风险度、经营风险度状况，汇总得出企业风险度综合评价结果。

企业质态分析，收集、整理区域政策、市场、资源、管理和企业等有关数据资料，建立企业质态综合评价台账。分别评价影响企业质态的管理活跃度、成长性、风险度质态状况，汇总得出企业质态综合评价结果。

（二）政务服务主题库

政务服务主题建设：提供政务服务库建库方案，利用信息化手段推进政府行政管理效能提升，涵盖公民、企业及社会组织、其他政府部门机构等，建设政务

服务主体库资源，包括基础信息和扩展信息，通过规范核心表和扩展表，合理并多角度构建政务服务库模型。归集事项信息、办件信息、服务渠道信息、人员信息、企业信息、自助终端信息、服务人员信息、区域办件信息、大厅部门入驻信息、线上服务信息、线下服务信息、办事指南信息等。

（三）社会发展专题库

社会发展专题库建设：提供社会发展专题库方案，结合项目实践以及数据资源普查结果，对社会发展专题库中的各个子专题进行统筹规划，构建相对完整、规范的数据资源分类体系、模型体系，关注数据质量问题。参考应用支撑需要和项目实践，从规范性、完整性、准确性、一致性、时效性、可访问性等维度对社会发展原始数据进行持续的质量稽核工作，将发现的数据质量问题反馈给数据提供部门进行整改；采用技术手段，对部分问题数据进行清洗转换，使其变成满足数据质量要求的数据。

可根据业务情况建立如下资源信息表：营商监测、时长感知、创新激励、核查督查、统一身份认证、统一电子印章、统一电子证照等。

（四）12345 热线专题库

12345 热线专题库建设：提供 12345 热线专题库建库方案，根据 12345 热线情况，基于数据底座、数据共享交换平台能力建设，结合市级建设要求，通过需求调研、数据归集、数据建模、数据治理等步骤，对涉及相关等部门的业务、数据、指标进行调研，确认 12345 热线专题库需支撑的指标体系并进行相应数据的归集。同时根据已确认的指标体系进行相关库表模型的设计，在 12345 信息模型基础上，使用数据治理平台对已归集的数据进行清洗、过滤、融合等处理步骤，将数据发布至相应的库表模型。

可根据业务情况建立如下资源信息表：12345 热线信息表、工单信息表、热线任务信息表、督办信息表、回访信息表、知识基本信息表、只是引用信息表、平台评分信息表、主题信息表等。

（五）民生保障专题库

民生保障专题库建设：提供民生保障专题库建库方案，通过接入市民出行、社会保障、医疗健康、教育培训、住房保障、民政福利、文体旅游、社会治理等各方面的民生服务数据，进行数据融合分析，发现和洞察服务流程中的疏漏和用

户体验需求，以有效的利用民生服务数据资源，挖掘民生事业发展需要改善的方向与重点，促进各类设施资源的合理配置与利用，促进社会保障体系建设，促进富民安康幸福的民生发展体系的建立，提升市民获得感与参与度、提升政务服务质量，为公共服务资源配置、民生保障提供有力的决策支持。

可根据实际情况建立如下业务信息表：人员信息、企业信息、收入信息、资产信息、教育文化医疗机构信息、死亡信息、社会保障、民生幸福评价指标体系。

（六）主题库专题库采集与治理

采集与治理服务：依托政务数据共享交换平台、政务数据资源中心提供主题库专题库采集与治理服务，包括“数采、数治、数用”三个环节，通过集约化统筹实施数据资源编目、汇聚、治理，形成强大的数据中枢与能力赋能中心，为各委办局业务领域的应用提供灵活可靠的赋能与支撑。

1、数据对接集成服务

提供数据抽取、数据转换、数据校验、数据加载等全流程；以任务调度流程为中枢，采用主动抽取模式，实现政务数据的高效采集。

2、数据质量服务

数据集成汇聚后，对政府数据进行有序标准化的规划设计，梳理政府所掌握的数据资产以及一些工具化或定制化的服务，管理解决数据流转过程中每个环节产生问题的过程。

3、数据加工处理服务

在数据质量处理完成后，对每个治理对象进行分析，在明确对象之后，需要编制处理的方案，模型的构建，编写相关的脚本并做相应的配置。

4、数据融合校验处理

提供数据校验服务，将落地数据调用权威部门实时接口，对落地数据进行修正补充，提高数据准确度及完整性。

5、数据建模服务

提供数据模型建立服务，数据模型是数据治理的重点内容，是对数据治理过程中的数据进行业务化的过程，通过结合数据标准、数据开发，提供统一指标管理、数据规划、自定义主题数据模型、可视化数据建模等服务。

6、主专题库建设支撑服务

提供主专题库建设方案编制服务，方案包括技术框架、数据架构、库表设计、实施路径、实施方案等内容。建设方案编制范围包含市场监管主题库、社会发展专题库、政务服务主题库、12345 热线专题库、民生保障专题库。

7、数据应用开发服务

基于已建的主题库和专题库，融合数据资源、挖掘数据价值，为各业务部门提供数据应用服务支撑，包括数据接口开发服务、数据分析服务、数据比对服务等。

（七）主题库专题库建设系统对接要求

建设过程中需要对接包括但不限于如下各委办局必要的系统进行数据对接，待对接委办局如下：

市人社局，市网信办，市工信局，市场监督管理局，市自规局，市残联，市税务局，乡村振兴局，市信访局，公共资源交易中心，市交通局，市司法局，供水集团，排水集团，城投集团，哈尔滨住房公积金，教育局，住建局，市统计局，市财政局。

可待对接系统如下：人社云综合服务平台，哈尔滨就业地图，哈尔滨市领导包联企业数字管理平台，特种设备统计年报系统，全国认证行政监管系统，全国 12315 平台，行政审批管理系统，行业稽查管理系统，热线及统一投诉处理系统，哈尔滨市网络预约出租汽车行业监管平台，公证综合业务管理系统，智能停车平台，哈尔滨住房公积金计算机管理信息系统，义务教育招生报名系统，哈尔滨市招生考试信息化管理平台，云平台，市智慧管网系统，新建商品房网签备案系统，物业系统，哈尔滨市工程建设项目审批管理系统，全省预算管理一体化系统。

4．数据安全

具体技术（参数）要求
数据安全建设 按照统一安全技术规范，提高数据安全处置能力，形成数据安全管理闭环，筑牢数据安全防线。建设市级全流程数据安全管理和数据安全态势感知平台，具备挖掘感知各类威胁事件能力，实现高危操作及时阻断，变被动防御为主动防御，提高风险防范能力。

一、 功能要求

1、数据安全架构

数据安全架构以重要业务和数据为对象，以数据采集、数据加工、外部数据调用数据安全管理为重点，以安全大数据智能分析为抓手，构建基于云计算、大数据，覆盖“管理、技术、运行”的立体化保障体系。实现数据安全合规，落实数据安全技术要求。

2、湖内数据安全

湖内数据安全为数据湖提供数据生命周期内统一的数据使用保护能力，通过敏感数据识别、分级分类、隐私保护、资源权限控制、数据加密传输、加密存储、数据风险识别以及合规审计等措施，具备建立安全预警机制，增强整体安全防护能力，让数据可用不可得和安全合规。

（1）数据密级

系统具备数据分级分类，具备数据资产的快速检索，包括关键字检索、按名称和描述检索、按所有属性检索等。

（2）数据分类

系统具备分类管理，具备业务分类定义和管理，具备给数据资产标识分类。

（3）数据脱敏

数据脱敏包含静态脱敏和动态脱敏，具备按工作空间、数据源类型、数据库、数据表等选择任务执行范围，匹配对应的执行规则策略；使用静态脱敏经常使用测试环境中；动态脱敏经常使用在接口环境中。

（4）数据水印

数据水印应满足以下使用场景：

具备规范数据外发流程：实现对内部人员数据外发进行有效流程化管理，非授权用户在数据外发前需审批，审批通过后采取数据水印技术生成可外发数据文件即可。

具备数据版权保护：通过在关系数据库中嵌入代表所有权的水印信息，可以将数据库与其拥有者联系起来，从而实现数据的版权保护。

具备对泄露数据进行快速溯源：通过对泄露数据文件解封，根据数据文件的完整度和水印信息痕迹来检测水印是否存在，快速识别水印标记信息（数据源地

址、分发单位、负责人、分发时间等），从而对安全事件精准定位追责。

（5）数据安全管控策略

结合行业监管标准规范的安全防护要求，要求汇总出基于数据安全级别、数据安全防护要求、数据安全管理维度的数据分级管控和防护策略。

数据安全管控策略。具备不同安全级别的管控策略：在数据安全级别、数据安全管控策略两方面进行策略建设。

具备不同应用场景的管控策略：根据用户访问数据（敏感数据）场景，在业务访问场景、开发测试场景、系统运维场景、开放共享场景等场景实施数据安全管控策略，包括：分类分级、数据加密、备份归档、防泄漏、数据脱敏、访问控制、数据销毁和输入输出控制等。数据安全管控技术策略包括单位数据分类分级保护具备策略、数据分类分级管理办法、数据分类分级安全基线、数据管控技术应用策略。

3、数据安全监测

具备提供数据异常威胁分析、数据溯源等安全功能。通过集中化数据安全监测管理，实现数据分布、流转、访问过程中的态势呈现和风险识别，保障数据资产安全。

（1）应用监测

具备解析应用数据审计日志，基于知识库识别会话数据内容中的涉敏字段，对应用、API、访问行为进行涉敏标记和统计分析。

具备对应用的登录账号进行解析，具备人工干预解析模版。

具备以图表方式展示所有应用访问敏感数据量的时间趋势，并根据时间、数据标签等进行筛选。

具备按访问敏感数据量对全局应用、全局应用接口、全局应用账号进行排名，并根据时间、数据标签等进行筛选；同时具备下钻查看详情。

具备展示某个应用/应用接口/应用账号的详情，包括敏感数据标签、敏感数据标签的占比、敏感数据量的时间分布、应用账号访问敏感数据排行、来源 IP 访问敏感数据量排行、访问审计日志，并根据时间、时间标签等进行筛选。

具备全局的应用审计日志列表展示，展示字段包括访问时间、账号、来源 ip、url、接口名称、应用名称、敏感数据量、数据标签；同时具备查看日志详

情，详情中包括接口的返回的数据样例。

（2）数据异常威胁分析

数据异常威胁分析结果具备展示传输敏感数据过程中存在的脆弱性漏洞，通过对网络流量中传输数据内容进行识别分析可发现安全风险，如：敏感数据明文传输、密码未加密、密码弱加密等。

敏感数据明文传输分析具备对一段时间内传输中识别的敏感数据或文件与业务系统、策略、URL、场景等信息进行关联分析，对命中策略的风险进行集中管理和告警。

密码未加密具备对一段时间内传输中识别的密码信息与业务系统、策略、URL、场景等信息进行关联分析，对命中策略的风险进行集中管理和告警。

密码弱加密具备对一段时间内传输中识别的密码信息进行解密，并将解密后的密码信息与业务系统、策略、URL、场景等信息进行关联分析，对命中策略的风险进行集中管理和告警。

4、数据风险分析

数据风险分析组件采用大数据技术架构，基于 Hadoop、SPARK、ES 等技术完成海量数据的存储、处理、分析和检索，平台可依据数据量的增加平滑扩展通过对网络流量探针日志、DLP 套件日志、数据运行环境加固系统日志等进行关联分析，全方位感知数据流动过程中面临的风险。

（1）数据风险分析

数据风险分析组件具备场景的风险统计和风险分析，场景代表某种业务风险的集合，由具有同一属性的风险分类及其对应的权重构成，如账号风险、应用访问风险、数据库访问风险、用户异常行为风险、数据违规行为等。管理员可以根据不同的场景进行风险总体监控、事件风险分析和用户风险分析，对于重点可疑用户，可以从多方位查看系统对该用户的风险画像描述。

（2）数据风险预警

数据风险分析组件具备对可疑的数据操作行为进行预警。组件内置多种常见异常类型的分析模型，便于快速制定异常分析规则。

（3）数据溯源

安全事件溯源应具备可视化数据安全事件溯源的能力，提供主体溯源和线索

溯源等溯源场景。

5、数据安全处置

安全处置中心提供数据威胁策略、安全事件工单管理功能。数据威胁策略，基于对攻击行为和数据的深刻理解，提高各类事件处置的准确性和快速性；安全事件工单管理通过对应急事件的处置，实现紧急事件快速处理和展示能力。

（1）工单派发

针对业务告警形成安全事件工单，对所有安全事件工单进行展示，与工单系统对接，对安全事件工单进行下发（邮件、短信）给相关责任人，提醒相关责任人去处理相应的安全事件。

（2）预警通知

预警通告的管理界面，在此功能模块可查看系统发出的所有告警通知，并具备在线编辑告警、审核告警、删除告警等功能。

告警操作流程：告警触发时为待提交状态，由运维人员查验提交后，变更为审核状态。安全员对告警进行审核通过后状态变更为正式预警，安全员对告警进行发布，告警状态变更为已发布，同时会通过邮件或短信等方式发出通知。

（3）告警规则管理

告警规则的配置管理模块，可以通过客户端配置告警规则，启动或禁用某一个或多个规则。通过配置告警的告警策略、触发条件、告警输出模块来配置规则，以便出发告警。告警输出模式具备多种方式，包括邮件、脚本、短信等方式。

6、数据安全事件全过程管理

基于数据安全态势感知平台提供的风险告警与事件处置数据，自动生成告警-事件 -处置明细表，按分类分级、响应时长等不同维度生成统计图表，结合数据处理活动进行合理评价。

7、数据安全运营

（1）建立数据安全自评价机制

数据安全管理系统和数据安全态势感知平台自身需要充分考量安全形势、合规要求、业务需要等变化，对组织的数据安全工作开展情况进行审核与监督，结合相关行业法律法规和监管部门的考核要求，数据安全成熟度或者场景风险等，进行技术性比对评估或佐证。并根据评估结果提供可落地的安全整改建议，从而

协助组织及时发现安全薄弱环节，指导组织针对性的进行安全能力建设。

（2）数据安全应急响应服务

应急响应服务应以经验丰富的应急响应专家为支撑，依托于云端大数据平台，形成全面的应急响应服务体系，在发生安全事件时，快速定位问题根源，以保障业务的安全运行和生产。

应急响应服务应以现场应急和远程应急两种方式对客户现场突发安全事件进行处置分析。应急响应服务主要分为六个阶段，分别为：准备阶段、检测阶段、抑制阶段、根除阶段、恢复阶段和总结阶段。

8、数据安全整体防护

数据安全防护应对数据资源中心业务数据的被动和主动防御功能，面向应用提供数据资源访问与接入管控、数据防泄漏、数据运行环境、数据库审计、数据库公司防护等方面安全建设，确保重要数据在存储、传输中的安全性。

（1）数据防泄漏

网络数据防泄漏：在网络出口处，发现并监控网络流量中的敏感文件传输。可通过镜像流量旁路接入、正向代理或透明代理方式，提供对网络流量审计的能力，将关键文档外传至文库、邮箱、网盘等行为实施有效监控。具备 HTTP、HTTPS、SMTP、POP3、FTP、SMB、IMAP 等常用网络协议，能够对基于 http 协议的网站、应用程序和即时消息等的 http/https 传输进行实时阻断。

终端数据防泄漏：终端数据防泄漏能力应用在组织内各计算机终端，用于发现、识别、监控终端中的敏感数据，对组织数据资产分布、敏感数据的违规存储进行展现，同时对敏感数据的违规使用、扩散等敏感行为进行策略响应控制。

（2）数据运行环境加固

安全加固系统应具备资产梳理、暴露面梳理、风险发现、威胁监测、病毒查杀、等保合规基线、系统加固、溯源分析等全面的安全能力，在服务器端形成事中控制、事后溯源的业务服务器一体化防护体系。全面覆盖服务器资产梳理、暴露面梳理、漏洞检测、病毒查杀、勒索病毒防护、等保合规、服务器微隔离、日常运维等。

（3）数据库审计

数据库审计应针对数据库和业务系统的重要性以及面临的风险，提供风险预

知，异常行为审计告警，操作行为审计，查询结果及报表展示等，实现事前预防，事中监控，事后追溯。

（4）持续评估与实施

需定期开展数据安全态势感知平台及子系统的系统脆弱性评估工作，通过人工测试、系统扫描、威胁情报等多种手段发现系统缺陷及安全漏洞，并针对发现的系统问题进行漏洞修复、整改与升级，提升系统可用性、可靠性和健壮性。

二、 建设内容

数据安全建设内容以重要业务和数据为对象，以数据采集、数据流转、外部数据调用、数据安全管理为重点，以安全大数据智能分析为抓手，构建基于云计算、大数据，覆盖“管理、技术、运行”的立体化保障体系。

(一) 数据安全态势感知

数据安全态势感知平台具备数据安全的发现能力、防护能力、检测能力、响应能力，实现覆盖数据全生命周期的安全管控，全面满足合规管理要求，有效防护数据安全风险。具体参数如下：

硬件规格：不低于标准 2U 机架设备，设备应采用鲲鹏、龙芯、飞腾、海光等自主可控硬件平台，CPU≥44 核,内存≥256G，硬盘≥1T SSD，硬盘≥48T SAS，网络接口：≥2 个 SFP+万兆光口、≥4 个 SFP 千兆光口，冗余电源。5 台。

1. 具备海量数据采集器与快速检索能力，具备平滑扩展。

2. 具备分布式部署，单一模块具备集群状态监测。

3. 具备对接数据采集器，可新增网络数据流转监测、数据库审计、数据安全态势感知探针等采集器，具备设置设备属性。

4. 网络数据采集器具备 HTTP、HTTPS 和 Oracle、SQL-Server、DB2、MySQL、Informix、Sybase、Postgresql、Cache、MongDB、国产数据库等协议的数据日志解析和采集。

5. 具备数据日志以 Syslog、SNMPTrap、文本、数据库、HTTP 等格式导入第三方日志，灵活满足日志格式兼容需求。

6. 具备用户自定义、配置解析规则、过滤规则、富化规则等。

7. 具备展示日志来源，具备根据时间筛选，查询内容包括：数据源日志接入数量、接入日志等内容。

8. 具备与 API 分析系统进行对接，提升数据安全分析和展示多面性和完整度。

9. 具备完成对数据库系统扫描采集，具备定期扫描任务。

10. 具备被动方式进行数据资产发现和扫描，降低对生产数据库的侵入影响。

11. 具备扫描结果查看。

12. 具备对数据库/实例进行自动采集解析，发现并提取数据库/实例信息、表信息、字段信息、表记录总条数等元数据信息，并识别其中的数据资产，生成数据资产目录，具备查看数据样例。

13. 具备兼容结构化、非结构化数据载体，进行数据采集和解析，至少包含 ostgreSQL、Mysql、oracle、Gbase8a、Gbase8t、XDM、sqlserver、Elasticsearch、Hbase、Hive、MongoDB、Kudu 等。

14. 具备定义并维护应用、数据库等资产信息，包括名称、所属部门等信息。

15. 具备数据资产对象管理，可实现字段级数据资产定义与维护，数据资产存储内容包括元数据信息、数据分类分级信息及数据标签信息。

16. 具备手动维护字段敏感数据标签。

17. 具备大屏可视化展示数据资产态势，包括新增数据类型、数据源分布、数据类型分布等信息。

18. 具备数据安全告警的统一、集中展示，实时获取、展示数据安全告警总体情况。

19. 具备告警信息钻取，具备根据不同的时间期限进行展示；

20. 具备展示和过滤字段等具备灵活设定。

21. 具备根据告警，研判是否为风险或事件，具备自动研判和人工研判。

22. 具备系统内置至少 5 种分析策略，用户可自定义每种内置策略的参数，如敏感数据量阈值、IP 范围、城市范围、时间范围、敏感数据级别等。

23. 具备自定义分析策略，可选择多个日志源，设置检测策略、归并策略。

24. 具备内置风险分析场景，对流量、日志进行实时统计和分析。内置

规则包括：账号共用拉取敏感数据、恶意操作造成数据破坏、非工作时间拉取敏感数据、非办公地点拉取敏感数据、数据违规外发、运维绕行拉取敏感数据等。

25. 具备基于监测分析规则进行威胁告警，具备用户自定义告警列表的展示字段，包括名称、类型、基本信息等。

26. 具备基于数据资产的安全级别自动设置告警等级。

27. 具备根据告警的类型、等级等配置告警归并规则，增强告警信息的可读性。

28. 具备根据数据威胁影响范围、危害程度、数据资产安全等级、法律法规要求等要素定义数据安全事件等级，灵活扩展要素。

29. 具备数据安全事件查询与展示，展示内容包括事件统一编号、事件名称、事件等级、事件描述、处置建议等。

30. 具备基于告警信息自动生成数据安全事件，具备手动将告警确认转为事件。

31. 具备从安全事件或告警入口，溯源展示事件详情和原始日志信息，包括发生时间、源 IP、风险等级等信息。

32. 具备根据数据安全事件信息，选择匹配的处置方案进行处置策略下发，具备编辑处置描述和设置同步选项，具备对无关事件进行忽略。

33. 具备处置方案库的管理与维护，具备新建，编辑和删除等操作。

34. 具备查看和搜索处置记录。

35. 具备在数据安全事件详情中，展示涉及的敏感数据、应用、数据库等信息。

36. 具备查看事件的原始日志，并进行进一步检索分析。

37. 具备对检索结果进行源 IP、目的 IP、数据标签等多维度的条件集中度分析和筛选展示。

38. 具备溯源结果的统计分析及可视化呈现，用户可自定义统计维度、要素。

39. 具备数据安全事件或告警进行可视化追踪溯源，可根据事件或告警的主客体等要素，按照数据流转过程生成安全溯源链。

40. 具备基于资产安全分级结果生成统一的数据资产识别策略、安全管

控策略，具备集中管理和配置维护资产安全策略库，具备新增、编辑、启停用等操作。

41. 具备安全策略库具备配置资产授权和防护建议，包括访问控制、脱敏、水印等管控策略定义。

42. 系统内置数据安全评估模型，至少包含组织架构、制度保障、分类分级、数据风险、权限管理、安全审计等评价要素。

43. 具备根据不同的评价要素中的指标项组合自定义评估模型，具备自定义分数范围，各评价要素报告方式支持编辑，提供文本、表格、选项、文件上传等反馈方式。

44. 具备根据数据资产安全评估模型生成安全评估报告；具备根据评估过程中产生的各种指标和最终结论，针对相应的薄弱环节提出安全整改建议。

45. 具备自由设置时间范围生成数据资产安全评估报告;具备 PDF、Word、HTML 三种格式的报表生成与下载。

46. 具备报表模板管理，可自定义报表内容，具备灵活编辑和布局调整以形成整体报表，包括选择展示数据内容、图表类型等，系统预置 5 种以上报表模板。

47. 具备 PDF、XLSX、图片等格式的报表生成与下载。

48. 具备设置报表定期运行，按日、周、月、季等周期自动生成输出报表。

49. 具备提供运行时应用自我保护功能（RASP）。可提供 SQL 注入防护能力、XSS 防护能力且可自定义防护规则。

50. 具备通过插件的方式，工作于 IIS、Apache、Nginx 等 web 中间件内部，通过判断流量特征和 WAF 规则引擎，对访问流量进行监控或防护，阻断 SQL 注入、XSS、漏洞利用等 Web 攻击。

51. 具备防端口扫描功能，且可设置单个 IP 请求时间范围、最大扫描端口数量、IP 锁定事件等信息。所投产品需具备微蜜罐功能，且可设置返回文本信息以及监听端口。

52. 具备对 Agent 进行统一管理，包括：Agent 降级，Agent 暂停，Agent 异常重启，Agent 安装的版本、可升级的版本占比情况进行统计，并可对 Agent

版本进行更新和同步，Agent 性能保护。

53. 具备五元组的主机防火墙，具备以 IP/端口/协议/方向/域名/进程服务等条件实现对服务器的经典访问控制。

54. 具备设置端口的暴露控制规则，包括但不限于：禁止/允许外网暴露、禁止/允许内网暴露等策略，并具备例外端口的添加。

55. 具备对服务器的进程外连控制进行规则设置，包括但不限于：禁止/允许进程外连外网、禁止/允许进程外连内网，并具备进程白名单和例外进程的设置。

56. 具备对主机进行一键隔离、一键禁止暴露外网、一键禁止暴露内网等快速应急操作。

57. 具备对服务器进程、端口的网络连接情况进行学习，通过学习生成白名单实现对非白名单内的 IP 流量进行监控阻断。

58. 具备文件监控与防护的能力，可有效检测并阻断攻击者对文件权限随意篡改，并具备对目录及文件权限控制(读、写、执行等)的能力。

59. 具备对操作系统加固能力，针对修改系统可执行文件/引导文件/系统服务/注册表、创建 autorun.inf/lpk.dll/usp10.dll 等高风险文件、添加系统用户/加载非法驱动/劫持系统引导启动/窃取系统内存密码等高危操作进行加固拦截。加固具备对进程、文件加白，具备开监控模式。

60. 具备阻止攻击者利用 powershell 远程连接下载恶意程序的能力，可检测并阻断攻击者利用 powershell 访问互联网行为。

61. 具备阻止非授权用户利用 psexec 工具执行命令的能力，可检测并阻断攻击者利用 psexec 工具执行命令行为，防止获取服务器超级管理员权限。

62. 具备阻止攻击者通过制作函数/脚本反射注入 dll，获取操作系统控制权的能力，可检测并阻断攻击者反射注入 dll 恶意行为。

63. 平台软件支持适配 X86、ARM（鲲鹏、飞腾等）架构服务器。

64. 具备用户的统一管理，具备角色定义与系统自身操作权限设置，具备灵活细致的权限设置。

65. 具备双因子认证功能以及账号设置等功能。

66. 具备对系统自身所有操作生成日志信息，具备对操作日志的查询检

索，具备备份系统日志，系统日志保存期限不少于 180 天。

67. 具备对用户登录进行统一认证和鉴权，具备登录失败处理功能，具体参数可以由管理员设置。

68. 具备时钟同步功能，保障系统时间与威胁发现时间的准确性。

69. 具备系统备份与还原功能。

70. 具备通过界面对系统升级包以及系统补丁包进行升级。

71. 具备对管理员等操作进行安全审计。

（二） 数据安全态势感知探针

数据安全态势感知探针具备政务数据资源中心流量中的数据情况进行识别、解析、检测、分析，并且将其检测和分析的结果上传数据安全态势感知平台作为元数据进行关联分析。具体参数如下:

1. 硬件规格不低于标准 2U 机架，设备应采用鲲鹏、龙芯、飞腾、海光等自主可控硬件平台，处理能力≥5Gbps；CPU≥16 核；内存≥64G；硬盘≥4TB SATA；网卡接口≥2 个千兆电口；双电源，1 台。

2. 具备旁路部署模式。

3. 具备与数据安全态势感知平台安全对接，上传相关数据安全检测数据，实现数据安全分析。

4. 采集过滤条件具备但不限于源地址、目的地址、服务、流量采样比、时间、例外应用等。

5. 具备空载荷过滤，具备对采集的流量的上下行载荷长度设置。

6. 具备离线采集，可通过手动 Pcap 导入或 FTP 等协议批量上传导入等方式对离线流量进行采集。

7. 具备文件传输方向为上传、下载、双向。

8. 具备流量上下行载荷以及 web 访问请求体长度的自定义配置。

9. 具备 IPV4 及 IPV6 流量的采集与处理。

10. 具备流量十六进制及文本形式的载荷格式。

11. 具备 VXLAN、GRE 、VLAN 、MPLS 的流量接入与解析，日志中可提现响应标识信息。

12. 具备 Oracle、MySQL、MSSQL、PostgreSQL、MongoDB、DB2、国产数

据库等数据库行为的解析。

13. 具备 WebMail、SMTP、POP3、IMAP 邮件行为解析。

14. 具备 HTTP、SSL 等基础协议的解析。

15. 具备如 ftp、smb、oracle、mysql、mssql、postgresql、ssh、pop3、smtp 的登录动作解析。

16. 具备对多种应用的文件进行还原。

17. 具备同连接及跨连接的大文件拼装还原，还原文件最大不得低于 200M。

18. 具备多种文件类型的筛选，可执行文件还原格式包含：bin、exe、bat、dll、sys、com、ax、acm、drv 等；压缩文件还原格式包含：rar、zip、gz、7z、tar 等；文档类型的还原格式包含：doc、docx、xls、txt、pptx、pdf、rtf、ppt 等。

19. 具备基于敏感数据采集策略对采集数据范围、敏感数据检测范围进行配置，具备 4000 条敏感数据采集策略，且策略具备优先级匹配。

20. 具备通过内容深度分析技术可实现针对结构化数据/非结构化数据/半结构化数据的检测分析，如文件类型检测、文件内容提取及分析、压缩文件内容提取及分析、JSON/XML 内容提取及分析等，可结合用户业务数据特点进行深度内容分析，判断当前文件内容是否包含敏感信息（法律法规政策规定和或者自定义配置的相关敏感数据），并产生敏感信息文件告警，为数据安全的进一步处理提供依据。

21. 具备半结构化数据检测分析，包含 FROM、XML、JSON、MIME 等。

22. 具备结构化数据检测分析，包含 PostgreSQL、MySQL、MSSQL、Redis、人大金仓、瀚高、南大通用、优炫等数据库等。

23. 具备非结构化数据检测分析，包含 doc、docx、xls、xlsx、ppt、pptx、pdf、rtf、cebx、ceb、odt、ofd、odp、wps、et、dps、zip、gz、tar、rar、7z、bz2、xz、html 等。

24. 具备 SMTP、POP3、IMAP 邮件协议中正文及附件的内容提取及检测。

25. 具备个人敏感信息规则，包含身份证号、军官证号、护照号、港澳通行证号、银行卡号、银行卡类型、开户行、驾驶证档案编号等，具备种类不得

低于 28 种。

26. 具备个人信息规则，包含出生日期、年龄、电话号码、电子邮件地址、职业资格证书编号、毕业证书编号、学位证书编号、IMEI、SIM 卡号、经纬度、不动产单元号、产权号等，具备种类不得低于 70 种。

27. 具备重要数据规则，包含金融信息（不动产权证号、银行账户、出口贸易编号、汇率、业务流水号、交易币种、交易金额、收款人类型、客户类型、客户名称、客户代码、产品名称、产权人名称、银行代码、金融许可证号）、汽车信息（车架号、车牌号、发动机型号）等，具备种类不得低于 50 种。

28. 具备自定义敏感数据检测规则，定义规则内容包括但不限于类型、子类型、敏感程度、匹配条件等字段，规则类型需具备正则和关键字两种方式。

29. 具备敏感数据原始文件样本留存，留存单个文件大小最大不低于 50M 。

30. 具备记录 Web 访问日志，审计维度包括但不限于源 IP、目的 IP、源端口、目的端口、Web-Method、Web-URL、Web-Host、日志记录时间。

31. 具备记录文件传输日志，审计维度包括但不限于源 IP、目的 IP、源端口、目的端口、文件传输方向、文件名称、MIME 类型、文件类型、文件大小(B)、Web-URI、Web 文件传输方向、日志记录时间。

32. 具备记录登录动作，审计维度包括但不限于源 IP、目的 IP、源端口、目的端口、登录用户、登录结果、登录数据库类型。

33. 具备记录数据库操作日志，审计维度包括但不限于源 IP、目的 IP、源端口、目的端口、登录用户、数据库版本、数据库名称、数据库类型 、SQL 语句、SQL 执行结果。

34. 具备记录 Ssl 加密日志解析，审计维度包括但不限于源 IP、目的 IP、源端口、目的端口、SSL 版本、SSL 会话 ID 、SSL 服务器 、SSL 颁发者。

35. 具备以流转途径维度查看数据流转情况，展现内容包括应用名称、访问用户数、行业类型、数据标签、访问总条数、去重后条数、访问数据量、首次访问时间、最新访问时间等。

36. 具备以数据维度查看数据流转情况，展现内容包括数据标签、关联用户数、敏感程度、访问总条数、去重后条数、访问数据量、首次访问时间、最

新访问时间等。

37. 具备以 web 应用、数据库、其他应用等不同应用类型分别展现数据流转的风险，展现内容包括应用名称、风险名称、风险等级，首次发现时间，最新发现时间等。

38. 具备以受害者维度展现数据窃取风险，展现内容包括受害者、风险名称、风险等级，首次发现时间，最新发现时间等。

39. 具备以访问者维度展现可疑访问风险，展现内容包括访问者、风险名称、风险等级、流量上行字节数、流量下行字节数等。

（三） 数据防泄漏

数据防泄漏系统具备深度内容识别技术，对网络传输中的流量（HTTP/S、FTP、SMTP）进行检测和针对终端电脑（Windows、macOS）进行数据安全管控，发现、识别、监控终端中的敏感数据，依据预先定义的策略，识别敏感数据，执行特定动作，实施特定响应。具体参数如下：

1. 硬件规格：不低于标准 2U 机架设备，设备应采用鲲鹏、龙芯、飞腾、海光等自主可控硬件平台，CPU≥32 核，内存≥32G，硬盘≥4T SAS，网络接口：≥2 个千兆电口，冗余电源，1 台。

2. 具备内置 OCR 能力，离线情况下，也能够对常见的 png、jpg、jpeg、bmp 图片中的文字进行识别。

3. 具备图章识别能力，能够发现常见的文档、图片中是否携带有图章，并可以根据图章中的文字识别图章类型。

4. 具备关键字、正则表达式等常规内容识别技术，检查目标文档中是否包含指定内容。能够对识别结果进行数量统计、忽略重复内容。能够识别诸如关键词混淆、乱序，简繁体混合，大小写混合等故意逃避行为。能够通过上下文语义识别出“主机密钥”并不包含关键字“机密”等场景。

5. 具备准确识别出身份证号、银行卡号、磁道信息、军官证等有明确标准定义的数据，并能够对这些数据进行宽泛或精确的校验，具备自定义校验内容，而非通过正则表达式进行简单的判断识别。同时能够对识别出的数据进行统计和去重处理。系统内置不少于 700 种以上的数据识别模型，并且能够快速进行数据识别模型更新。

6. 具备对收集的样本文件进行训练，形成敏感数据识别模型，根据识别模型来判断其他数据是否属于敏感数据。

7. 具备通过指纹识别技术检查目标数据中是否包含有指定的内容，并能够计算出包含内容的数量。指纹可以通过手动和在线两种方式进行提取，提取过程可以周期性自动开始、暂停和停止。在线提取下，可以通过 FTP、FTPS、SFTP、Samba、NFS 协议对文件服务器上的文档提取指纹，也可以通过 S3 接口对对象存储设备中的数据进行指纹提取，或通过数据库接口对数据库中数据提取指纹，具备的数据库类型不少于 18 种。

7. 具备文档自动聚类技术，通过机器学习的方式对杂乱无序的文档进行分类，并具备通过设置分类参数如特征值个数、相似度、分类数量等方式影响分类结果。通过能够将分类后的结果应用到内容识别中，对其他未参与分类的文档、数据进行类别判断。

8. 具备识别各种文档类型，对于修改后缀、删除后缀等文档仍然可以准确识别出文档真实类型。能够识别出 office、pdf 文档，已经常见压缩包是否被加密。同时，系统内置不少于 600 种文档类型，对于不在内置范围的文档可以通过自定义文档特征进行识别。

9. 具备多种识别技术联合识别的能力，能够将多种技术的识别结果进行组合计算，至少要具备与、或、非计算方式。

10. 具备指定要识别的位置，比如邮件可以指定识别邮件头、主题、正文、附件、收件人、发件人。能够识别出文件中的页眉、页脚、内容、作者、修改时间、自定义属性等内容。

11. 具备对于 word、ppt 等嵌套文件和 zip、rar 等常见压缩文件能够判断文件嵌套或压缩的深度，深度至少识别出 100 层。同时，也可以将每个被嵌套的文件进行单独的内容识别，判断要识别的内容是否都在一个被嵌套文件中，还是分散在多个嵌套文件中。

12. 具备按 excel 文件中的每个 sheet 页进行内容识别，能够限定比如身份证号码、手机号码需要同时出现在同个 sheet 页中。

13. 能够根据被识别文档中包含的敏感数据数量自动标定被识别文档的严重等级。

14. 具备自动采集并监控终端新增的应用信息。并对各种应用配置运行和访问权限，禁止运行高危应用、外置应用程序给系统带来风险，对存在泄漏风险和未知应用的访问敏感文件行为进行审计、阻断、审批、备注等管控措施。

15. 具备对终端外设的数据传输行为进行管控，阻止敏感文件拷贝、保存、另存到外接设备。同时提供在线审批、备注放行等方式，在完成审批或说明原因后可以实现敏感数据的拷贝。对于内部安全U盘或指定U盘，系统具备手动输入、在线申请等方式导入到系统中后可以正常使用。

16. 具备监控 IM 软件的外发消息，如 QQ、TIM、微信、企业微信、钉钉的外发消息，对包含敏感内容的外发消息进行拦截、告警、审计。

17. 具备监控 GIT、SVN 等工具的使用，能够定义 GIT、SVN 工具能够上传文件的地址，阻止文件上传到非法的GIT、SVN服务器上。

18. 具备监控到用户的打印或虚拟打印行为，能够根据不同用户设置不同的打印权限，能够对打印的敏感文件进行审计、拦截、提供流程申请、要求说明原因、添加水印等保护，水印内容、样式、字体、颜色可以自定义，具备文字、图片、二维码、溯源水印。

19. 具备对终端接入的网络进行监控，对接入非预定义的合法网络时，系统会产生审计记录、或阻止通过该网络发送任何流量。终端在接入合法的网络后，能够对指定应用的外发流量进行监控或例外，被监控的流量中如果包含敏感内容时能够进行审计、告警、阻断。同时具备按IP地址进行例外。

20. 具备监控终端屏幕，对打开敏感文件窗口自动添加文字、图片、二维码水印，水印内容、样式、字体、颜色、位置可以自定义，水印会随着窗口移动和隐藏。系统也能够直接在屏幕上添加文字、图片、二维码或隐写水印。同时，系统能够阻止用户对敏感文件的截屏、录屏行为，具备系统自带的截屏、录屏软件和第三方的截屏、录屏软件。

21. 具备监控到对敏感文件内容的拷贝行为，可以限制将敏感文件内容复制到指定的应用程序，从而产生泄漏风险。

22. 具备提供安全区（仅 windows 系统），包含用户本地上存储的敏感文件，安全区中文件在程序未正常启动情况下，将不可见、不可用，可以根据不同用户建立不同的安全区，实现用户间重要文件的隔离。

23. 具备提供离线文档保护功能，对需要外发的文件进行加密，并设置读写权限、编辑权限、打印权限和有限期等，外部人员在访问该文档时会自动添加窗口水印。

24. 具备对终端上保存的文件进行内容扫描和变化监控，及时发现终端上保存的敏感文件。

25. 具备对用户的终端风险行为进行详细的记录、邮件通知、syslog 输出、截屏和原始数据留存。

26. 具备静默安装、一键安装、推送安装。程序安装后具备显性和隐性两种运行模式。在显性模式下，可以自定义产品名称。

27. 具备内外网自动切换，当终端离开办公环境后，可以自动连接到公网的统一管理平台。

28. 具备软件停用功能，管理员可以直接停用指定终端的防护功能，用户也可以根据需要通过流程提前申请停用时间。

29. 具备主动登录、域。登录获取或指定用户方式实现与用户的绑定，绑定后用户可以自行调整所在部门。

30. 具备远程升级指定终端，升级过程可以后台自动升级，或由用户自己安排升级时间。

31. 终端插件支持 Windows 7/8/10/11 版本，支持 Windows Server 2008R2 及之后版本，支持 macOS 10.11-12.1 版本，支持 M1 芯片。支持 Ubuntu 18.04/20.04 版本。

32. 终端插件具备自主可控环境部署能力，支持银河麒麟 V10、中标麒麟 V7、UOS V20 版本。支持 x86、ARM、MIPS 芯片。

33. 管理端支持银河麒麟 V10，支持 x86、ARM 芯片。

34. 具备对网络中的 HTTP、HTTPS、SMTP、SMTPS、POP3、POP3S、IMAP、IMAPS、FTP、FTPS、NFS、Samba 等协议进行监控，并能够完整地进行恢复流量中传输的内容。

35. 具备对 BBS 论坛、网盘、文库、webmail、云笔记、SNS 社交等各种 web 应用进行监控，能够对上传的超大文件进行完整地恢复和扫描，并对包含敏感数据的传输行为进行防护。

36. 具备对邮件的收发行为，以及邮件客户端与邮件服务器的邮件同步行为进行监控，能够实时发现包含敏感数据的邮件传输过程进行防护防护。

37. 具备通过代理方式，提供 web 访问、邮件收发、文件传输服务，并对传输的过程进行控制，具备源地址白名单和目的地址白名单。

38. 具备对内部的 web 系统、邮件系统提供代理服务，对发送到 web 系统、邮件系统和从 web 系统、邮件系统下载的数据、文件进行识别和防护。

39. 系统具备域同步、手动创建、模板导入方式导入组织架构和用户信息。对于域同步方式，具备手动同步和周期同步。

40. 系统具备自定义系统角色，不同角色有不同的权限组合。系统具备多种分级管理模式，比如可以按策略、按组织架构，或按策略所属部门进行分级管理，分级管理员只能查看权限范围内的数据、配置。

41. 系统具备自定义管理员，可以对管理员可以管理指定设备的数据，同时也可以设置用户登录时间、地址、会话连接时长、密码有效期和密码复杂度等配置。

42. 具备系统自定义审批流程，并对不同的审批流程增加说明，用户可以根据所在部门、业务要求选择不同的流程进行审批操作。审批流程可以自定义多种审批模式，具备指定审批人员、部门审批、逐级审批、是否会签。

43. 系统内置多种识别规则，具备自定义防护策略，并对每个策略指定优先级、有效期，对策略产生的泄漏事件定义保留期限，一条策略可以同时应用到终端防泄漏、网络防泄漏、邮件防泄漏产品，并可以对不同产品定义不同的防护措施。

44. 具备对接外部专用的 OCR 服务，通过专用的 OCR 设备进行图片文字的精确提取和识别。

45. 对于在线训练的识别模型，在使用过程中能够收集产生误报的文件，并将误报文件自动加入到训练模型的反向样本中进行再次训练，以提升模型的识别准确度。

46. 具备事件列表中能够详细地展示泄漏事件信息，至少包含事件 ID、发送者、用户、部门、违规策略、泄漏时间、泄露方式、处置方式、事件状态、邮件主题、邮件正文、邮件附件列表、敏感文件列表、条件名称、敏感内容快照、

敏感数据所在位置、匹配度、留存位置等详细信息，能够对事件进行多维度查询和统计，生成不同的分析报告。

47. 管理员具备对指定的泄漏事件进行审核、标注，也可以进行导出、变更严重等级、归档、删除、发送邮件通知、添加备注等操作。

48. 系统具备通过 syslog 方式，将系统的泄漏事件、系统日志、采集日志、登录日志等上报到第三方平台，上报字段、周期具备自定义。

5．政务数据共享交换平台建设

具体技术（参数）要求
政务数据共享交换平台建设 现有政务数据共享交换平台能力如下：（1）政务数据共享交换系统。在政务外网建设具有 20 个前置交换节点的政务服务数据交换平台，实现政务服务数据交换，提供了数据交换、数据转换与清洗、数据比对、数据质量管理等功能。（2）政务数据共享交换系统应用。数据共享应用软件部署在电子政务外网平台，实现全市数据共享。具体内容包括：政务服务资源共享服务门户、政务服务资源目录管理系统、数据资源管理系统、主题服务系统、审批认证服务系统、大数据分析系统等。 本期升级需形成我市数据共享交换的核心枢纽和主通道，并以此为市级主平台，构建“1+N”的全市数据共享交换平台体系，实现与国家、省数据共享交换平台的对接，为跨层级、跨地域、跨系统、跨部门、跨业务的数据资源共享交换提供支撑服务。 （一）数据共享应用平台升级。 1、级联接口对接全省 开发与省数据共享交换平台的数据接口，实现市级与省数据共享平台数据资源的全面共享互认。要求对接的数据项符合国家标准，功能至少包括查询与核查。 （1）接口对接 通过政务服务能力开放平台与省级数据共享应用平台对接，与机构查询接口、目录分类注册接口、目录分类变更接口对接、目录注册接口、应用系统注册接口、库表资源注册等接口对接。实现查询接口信息，获取对应接口的名称、标

识等信息，并留存数据到本地。

1）接口调用解析

对接口进行调用解析，实现接口的联通。

2）解析信息处理

对解析信息进行处理，实现数据交互。

（2）上行库表对接

1）数据申请情况上报

统计本级数据申请情况数据写入申请情况上报表中，汇总到省级数据共享交换平台。

2）接口调用情况上报

统计各接口调用情况并写入调用情况表中，汇总到省级数据共享交换平台。

3）数据交换量统计上报

统计本级数据交换量并写入交换量统计表中，汇总到省级数据共享交换平台。

（3）下行库表对接

接收省级下发的库表信息，包含：目录分类信息、资源目录信息、资源目录信息项、资源信息、数据资源申请信息、审核过程信息、消息通知信息、堵点信息。

（4）级联对接系统

1）机构信息

展示机构信息，包含机构单位名称、组织机构代码、统一社会信息代码等信息，通过调用省级机构信息信息接口可实时获取所需的机构信息。

2）目录分类信息

展示省级下发和本级向省级注册的目录分类信息，通过分类名称可进行模糊搜索，具备向省级注册本级的目录分类、目录分类修改、目录撤销等功能。

3）资源目录信息

展示省级下发和向省级注册的资源目录信息，具备向省级注册本级的资源目录信息、资源目录修改、资源目录撤销等功能。

目录信息内包含各种资源信息的上报，包含数据源信息、文件资源信息、接

口资源信息、库表资源信息等。

4）应用系统信息

展示已向省级注册的应用系统信息，包含应用系统名称、机构唯一标识、外部访问 IP、外部访问地址等信息，具备调用省级接口向省级注册应用系统信息、变更应用系统信息等。

5）资源申请

资源申请中展示的是省内所有未申请的资源信息，可再此进行资源申请、资源代理授权申请等操作。

6）我的申请

我的申请内展示所有提交的申请信息，省级未进行审核操作的申请信息，可再此处进行撤销操作。

7）我的审核

查看本级资源的申请信息，可对申请进行审批。

8）我的共享目录

我的共享目录内展示本级自建的目录信息，且被其他地市申请使用，在此列表内可以进行资源回收。

9）通知回执

查看省级下发的通知信息，并在此发送阅读回执。

10）数据申请情况

展示本级数据申请情况，包含资源名称、申请数量等。

11）数据调用情况

查看各资源目录的总体调用数据，包含目录名称、调用次数等信息。

12）数据交换量

展示资源目录数据交换量信息，包含目录名称、交换数据量等信息。

2、接口异常监管

开发与省数据共享交换平台交换接口异常监管功能。市数据共享平台调取省数据共享交换平台接口时，增加对突发异常接口、请求响应超时的接口实时报警提示，清晰的展示调用接口异常的接口位置，以便于监管人员快速、智能监管接口。

（1）监管任务管理

接口连通情况的计划任务，可新增监管任务，调整监管任务，停用监管任务，删除监管任务。

包含任务名称、调用频次、调用时间、调用路径方法等信息。

（2）异常接口信息

展示最新一次监管任务执行后标记异常的接口信息，可查看异常信息内容。

（3）最新接口信息

展示最新一次监管任务执行后的接口调用信息。

（4）通知人员管理

监管异常的接口信息，会发送给预设定人员，包含人员的名称、职务、电话等信息，可增加预设定人员、调整人员信息、删除人员信息等。

（5）监管信息统计

统计各接口连通率，以及当天连通情况。

（6）短信通知

向监管人员发送异常接口信息通知，便于掌握当前接口连通情况，并能够及时调整或联系省级数据共享平台。

3、数据资源阈值管理

开发数据资源阈值管理功能，自定义调取接口次数报警规则，通过自定义调取接口上报监控数据后，可对监控信息设置报警规则。当调取数据阈值达到报警条件时，触发相应报警通知方式。

（1）阀值管理

数据资源阀值是针对各应用的每一个资源申请单独做阀值管理，阀值内容自定义可调。

（2）报警人员设定

超限接口信息会发送给预设定人员，包含人员的名称、职务、电话等信息，可增加预设定人员、调整人员信息、删除人员信息等。

（3）报警短信通知

向接警人员发送接口超限信息通知，可动态掌握当前接口流量。

（4）调用拦截器

对外提供的接口服务增加超限拦截器，当次数超过预警阀值后，自动拦截访问内容。

（5）阀值初始化

各应用的申请接口依据历史访问量，初始化峰值、平均值、最小值等数据，通过计算规则初始化阀值数据。

（二）数据共享交换平台升级.

1、政务数据服务门户升级

升级现有共享服务政务外网门户，应提供目录管理、供需对接、资源管理、数据共享、数据开放、统计分析、异议处理功能，其中目录管理、供需对接、资源管理、数据共享、数据开放、统计分析通过整合集成方式进行建设，异议处理应提供异议申请、异议审核、异议回复、异议确认、我的异议功能。

2、政务数据目录梳理与注册

全面梳理我市政务信息共享资源，完善哈尔滨市政务信息共享资源清单，在现有资源目录管理系统提供的资源目录产生、维护、发布、查询功能基础上，将梳理的政务数据目录进行分类注册到目录管理系统中,实现全市政务数据目录统一管理。应提供目录梳理及编制、政务数据目录实施。

3、政务数据交换系统升级

升级现有政务服务数据交换系统，实现国家、黑龙江省级垂管系统、哈尔滨市级各部门数据交换全覆盖，支撑我市跨部门、跨区域、跨层级、跨网络政务信息交换共享交换。围绕各类应用，满足部门间的信息汇聚和传递、在线实时信息的交换、部门间业务协同等需要。

（1）前置数据采集

市政务数据共享交换平台现有 20 台前置机，为了实现全覆盖市级部门的目标，需要扩充达到 48 个节点。应提供策略配置管理、任务生成管理、任务执行管理、数据处理框架、数据处理算法管理功能。

（2）数据交换管理

在交换数据逐渐增多的情况下，应在中心端新增 1 套数据交换管理软件，与现有数据交换管理软件进行集群部署，以提升数据处理效率，满足日常管理需求。数据交换管理是部署在平台中心交换服务器上的应用系统，作为交换平台的中心

管理模块，提供图形化的配置工具，实现对整个信息交换过程的流程配置、部署、执行和整个交换平台运行进行监控、管理。应提供网状交换、交换节点管理、数据源管理、映射模型管理、交换任务管理、交换主题管理、交换接口管理、调度管理、参数管理、日志管理、用户管理、监控管理功能。

4、政务原始数据处理系统

政务原始数据处理系统提供原始数据汇聚处理，通过元数据管理、数据标准管理、数据转换与清洗、数据比对管理、数据质量管理等功能，提升原始数据的数据质量，建立标准数据库，为数据共享、基础库、主题库数据加工提供标准化数据支撑。

（1）数据标准管理

数据标准管理应提供业务术语管理、值域代码管理、值域规则管理、数据元管理、数据模型管理、业务指标管理、数据标准管理功能。

（2）元数据管理

元数据管理应提供元数据采集、元模型管理功能、资产库管理、版本管理、关联分析、血缘/影响分析、全景图、数据剖析、业务术语管理功能。

（3）数据模型管理

数据模型管理应提供物理模型、实体关系图、导出建表语句功能。

（4）数据转换与清洗

在交换数据逐渐增多的情况下，应新增 1 套数据转换清洗软件，与现有数据转换清洗进行集群部署，以提升数据处理效率，满足用户日常管理需求。数据转换与清洗应提供异构数据源整合、图形化映射工具、数据抽取、数据转换、数据清洗、数据加载、转换清洗规则模型管理、转换清洗流程管理、分布式并行运行；多线程并行抽取、加载；调度规则管理功能。

（5）数据比对管理

在交换数据逐渐增多的情况下，应新增 1 套数据比对软件，与现有数据比对软件进行集群部署，以提升数据处理效率，满足用户日常管理需求。数据比对管理应提供比对内容定义、比对任务管理、数据比对执行、比对异常处理、比对管理监控、比对配置管理功能。

（6）数据质量管理

在交换数据逐渐增多的情况下，应新增 1 套数据质量管理软件，与现有数据质量管理软件进行集群部署，以提升数据处理效率，满足用户日常管理需求。数据质量管理应提供规则配置管理、检查任务执行、质量事件管理、数据质量监控、数据质量评估功能。

（7）问题数据管理

问题数据管理应提供问题数据质量统览、问题数据分类统计、问题数据处理进展、问题数据分类查询和问题数据协作管理功能，其中问题数据协作管理应提供问题数据在线反馈、问题数据在线处理和问题数据在线查询功能。

5、供需对接系统

供需对接系统统一全市数据供需双方共享渠道，实现政务数据供需对接，及时响应市级各政务部门数据共享需求。

（1）供需管理

供需管理应提供需求单发起、供给确认、目录关联、数据确认功能。

（2）审核管理

审核管理应提供需求单审核、需求汇总、责任单接收确认审核、供给确认审核、目录关联审核功能。

（3）中心审批管理

中心审批管理应提供供需单/责任单审批、目录关联审批、供需分支重分配、供需分支重分配审批功能。

（4）责任归集管理

责任归集管理应提供责任单发起、责任单确认接收、整体数据确认功能。

（5）负面清单管理

负面清单管理应提供负面清单维护、负面清单审批功能。

（6）我的任务

我的任务应提供我的需求、我的责任、代办任务、我的消息功能。

6、国家、省垂管系统对接管理

（1）国家垂管系统对接管理

配合省政务数据共享交换平台分批推进国家部委垂管系统对接。通过汇总市各部门对国家垂管系统数据的需求，向省数据交换平台集中申请数据，通过市前

置机接收省数据交换平台返还的国家垂管系统数据。应提供国家垂管系统目录管理、国家垂管系统资源管理、国家垂管系统资源服务、国家垂管系统数据对接功能。

（2）省级垂管系统对接管理

应提供省级垂管系统目录管理、省级垂管系统资源管理、省级垂管系统资源服务、省级垂管系统数据对接功能。

（3）省数据共享交换平台对接

按需实现与黑龙江省数据共享交换平台全面、多渠道对接，包含目录信息、数据资源等核心功能的对接，以确保实现平台与省数据共享交换平台的“网络通、数据通、应用通”的目标。应提供省数据共享交换平台目录管理、省数据共享交换平台资源管理、省数据共享交换平台资源服务、省数据共享交换平台数据对接功能。

7、政务数据资源管理系统升级

对现有数据资源管理系统升级，提供国家、黑龙江省、哈尔滨市各类政务数据资源注册、变更、维护等统一管理，实现市级各部门共享数据集中管理。应提供配置管理、资源注册、资源维护、资源审核、资源发布功能。

8、政务数据共享系统

数据共享系统提供政务数据资源共享发布、订阅、审核等管理，实现国家、黑龙江省、哈尔滨市各类政务数据资源共享资源统一管理，满足市级各部门数据共享需要。应提供共享资源发布、共享资源订阅、共享资源审批功能。

9、传输节点

传输节点主要实现信息传输基础能力，进行跨局址智能路由，具备实时交易、消息、文件、库表等类型的信息传输。实现安全管控、动态网络控制、实时交易控制、文件传输控制、消息转发控制、容灾高可用控制等功能。

10、数据交换节点

建设各地市数据交换节点，实现接口、库表、文件、消息四类交易的请求鉴权、请求路由、网络代理和安全控制，功能包括实时接口交易网关、数据库代理、文件代理、消息代理等模块，各级业务系统按需就近接入，即可触达全网络资源。

11、全局管理系统联调

完成地市传输节点、数据交换节点建设后，完成其与省级全局管理系统业务与功能接入联调，实现一点管理，多点触达的能力。

12、政务数据管控系统升级

（1）API 接口管理

API 接口管理应提供网关节点、API 管理、规则配置、网关流控、网关挡板、黑白名单、网关测试、灰度发布、服务鉴权、服务监控、日志审计功能。

（2）运行环境监控

运行环境监控针对操作系统、中间件、数据库等不同类型的应用环境，提供资源纳管、监控、策略告警和通知等功能。

（3）应用性能监控

应用性能监控平台应提供应用全堆栈全景监控、应用代码级定位分析、用户体验追踪及在线状态管理、运行缓慢业务流程分析定位、应用性能风险根源问题分析定位等功能。

（4）数据共享交换监控

数据共享交换监控应提供数据交换情况监控、数据处理监控、数据共享监控、资源来源分析、资源发布情况、资源使用情况、资源利用率分析及预警、资源应用情况分析功能。

（5）通知预警

通知预警应提供审核超时预警、数据上报预警、数据更新预警、资源发布通知、平台使用通知功能。

（6）应用支撑平台

应用支撑平台应提供数据可视化软件、应用运行环境监控软件、业务自动化巡检平台。

6．统一身份认证升级改造

具体技术（参数）要求
统一身份认证升级改造 现有统一身份认证能力如下：系统集企业法人、自然人在 PC 端的身份管理、身份认证、授权管理、应用资源访问控制，构建多信息资源的应用整合、集中管

理和安全防护的安全基础服务平台。实现哈尔滨市一体化政务服务平台各业务模块的统一身份认证，对接政务服务系统、e 冰城 APP、政府电子公文系统、哈尔滨市网约车登记系统等 30 余个系统。

本期统一身份认证需与省级数字政府对接，以省政务服务平台为基础，实现自然人、法人、公务人员的统一注册、统一登录和实名认证。

对统一身份认证系统进行升级对接改造，不影响现有系统正常运行，割接时间需保证在 48 小时之内，将原有统一认证系统按照《黑龙江省统一身份认证技术规范》和《黑龙江省统一身份认证接口要求》进行升级对接改造，进一步提高身份认证的安全性、响应效率和更多场景应用，更好地服务于广大群众和企业。

1. 集成省级政务服务平台的统一身份认证登录接口。提供统一身份认证系统自然人和法人的注册、登录、信任传递、登出等功能与省级政务服务平台统一身份认证系统对接服务。

2. 改造用户注册接口。实现自然人、法人和公务人员的统一注册、统一登录和实名认证，确保用户注册、登录过程的安全性和可靠性。

3. 升级改造不影响原统一认证业务应用，已实现互联互通的政务服务网、工商拓扑、工程建设审批系统等无需二次集成。

4. 提供统一身份认证系统对接鉴权升级改造服务，识别接入系统申请，提供接入权限定义，对身份信息的创建、变更、冻结、删除等生命周期进行管理记录，增强系统接入集成安全性。

5. 提供基于已发放的政务 UKEY 证书登陆认证服务、提供基于企业云章登陆认证服务，提升统一身份认证系统整体安全能力。

6. 本次升级改造需满足 GM/T 0034《基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》要求。具备访问控制功能、自身安全功能、日志功能。

7．电子证照升级改造

具体技术（参数）要求
电子证照升级改造 现有电子证照能力如下：哈尔滨市电子证照，提供制证、发证、集中收集、管理和共享等服务，简化公众办事过程中的证照材料提交。

本期升级改造电子证照系统，优化电子证照制证、用证服务，优化电子证照制发证体系，将制发电子证照作为业务办理的必要环节，实现事项办理系统与电子证照库无缝融合，加强电子证照信息互认共享，推动电子证照在政务服务领域的应用。

电子证照升级改造。

（一）电子证照数据模型构建

需提供整体的哈尔滨市电子证照库数据建设，包括上报库、回流库、基础库三大库。针对每类库需要进行相应的电子证照相关的数据模型设计与构建，包括概念模型、逻辑模型、物理模型。内容包括信息资源分类规划（证照目录信息、证照类型信息、证照基础信息）、上报库、回流库、基础库。

（二）电子证照数据采集汇聚

需具备电子证照数据采集，主要是针对上报库的数据采集以及回流库的数据采集。内容包括电子证照数据调研、电子证照数据采集、上报库、回流库。

（三）电子证照数据治理入库

需具备电子证照数据治理建设，建立一套统一规范的电子证照数据治理体系，依托数据治理相关工具，基于完善的数据归集、数据清洗转换入库、数据校核比对、数据质量控制、数据资产管理、数据分析机制，完成上报库、回流库采集数据以及基础库的提取、转换和加载，并根据数据标准化、专项分析需要，进行电子证照数据的整合加工处理，形成标准规范的上报库、回流库、基础库等，实现电子证照库整体的建库过程。内容包括电子证照库元数据管理、电子证照库数据标准管理、电子证照数据质量校核、电子证照库数据清洗转换入库。

（七）电子证照数据资源编目

需具备电子证照库信息数据资源编目和资源挂接。具备用户对数据资源目录信息进行方便、准确的检索。

系统需要建立电子证照数据资源结构体系，分类分级细化管理，对入库的所有电子证照经济数据资源按照数据标准的统一规则进行分类、登记、维护。提供数据资源分类管理与维护、数据资源信息管理与维护等运维服务。包括电子证照数据资源分类管理、电子证照数据资源分类维护与审核、电子证照数据资源信息管理、电子证照数据资源维护与审核。

（八）电子证照综合查询

系统需要提供电子证照综合查询功能，具备基于电子证照编码、电子证照类型、证照签发部门等多个查询条件，进行电子证照相关信息的综合查看查阅功能。内容包括电子证照特定查询、电子证照版面展示、电子证照档案显示、关联信息显示、人员证照关联查询、法人证照关联查询。

（九）电子证照统计分析

需具备基于电子证照库中证照的多维度信息，提供统计分析和可视化展示服务，具备通过同比、环比趋势分析和关系网络等分析方式，辅助电子证照管理、研判、辅助决策。内容包括证照目录统计分析、证照调用统计分析、证照综合图标分析、证照关联办理业务分析、证照预警监控。

（十）电子证照汇聚治理查询统计分析

根据电子证照库采集汇集的全部数据资源，提供对电子证照采集上报情况、回流情况、治理情况的全貌，并监控数据资源的总体情况，提供可视化的展示。内容包括采集上报情况分析、省上回流情况分析、基础数据资源分析、数据库资源全景分析。

（十一）系统管理

系统需要实现系统支撑功能的管理，内容包括组织机构管理、用户管理、角色管理、权限管理、日志管理。

（十二）与外部系统对接

需要与省统一身份认证系统对接、与省电子证照系统对接、与市数据共享系统对接、与市数据资源中心对接。

8．电子印章升级及场景应用

具体技术（参数）要求
电子印章升级及场景应用 现有电子印章能力如下：包含电子印章制作系统、电子印章状态发布系统和电子印章应用系统，实现了电子印章的生成、管理、签章、验签等功能。 本期拓展统一电子印章应用，按照国家电子印章和电子签名标准规范，为各级政务部门提供制章、用章、验章等服务，加强电子印章一体化应用，为电子印

章在电子证照、电子文书、电子公文等业务中的应用提供支撑，建设全市企业电子印章平台，建立企业电子印章制作、发放、使用服务体系，逐步在政务服务、电子政务、电子商务、电子金融等领域扩展应用。

升级改造服务要求与哈尔滨市一体化政务服务平台、哈尔滨市政府电子公文系统、国垂省垂专网、本地连接专网等业务系统实现完全兼容互通。项目升级后，应完全兼容前期已经开发的政务服务类及电子公文类各项应用业务，实施过程中不中断业务运行，过程中产生的所有对接费用由供应商自行承担。

(一) 电子印章业务服务升级改造

对原有政府电子印章扩容升级，新增企业电子印章及个人电子印章业务服务部分，包括印章的申请、核验、审核、签发、应用统计等功能。

1. 政府应用授权信息获取：

(1) 用户登录信息获取：获取用户登录相关信息。

(2) 授权请求信息获取：获取授权请求信息。

(3) 授权处理信息获取：获取授权处理信息。

(4) 访问授权资源：对授权资源进行访问。

2. 政府印章吊销原因：

(1) 印章状态查询：具备查询印章的当前状态，包括是否被吊销。

(2) 吊销原因展示：具备查询已被吊销的印章，系统可显示该印章被吊销的原因。

(3) 吊销操作记录：系统会自动记录每一次印章的吊销操作，并且可以在后台进行查看和管理。

3. 政府印章吊销状态获取：

(1) 印章状态查询：具备获取并同步印章吊销状态码，对印章吊销状态进行查询。

(2) 吊销申请提交：填写印章吊销的相关信息并提交申请，等待审核。

(3) 吊销结果反馈：审核员可以在审核完成后反馈吊销结果，告知吊销是否成功。

4. 政府印章信息获取：能够获取原有政府单位印章名称、印章编号、有效起始时间、有效结束时间、印章状态。

5. 政府印章无效状态生效时间获取：

(1) 印章无效状态判定：系统根据印章的状态和其他相关信息，判断印章是否处于无效状态。

(2) 印章无效状态生效时间获取：具备获取并同步印章无效状态生效时间。

(3) 异常情况处理：如果输入的信息不合法或者系统发生异常，需要给出提示并进行相应的处理。

6. 印章更新提醒：

(1) 更新时间计算：系统根据印章最后一次更新时间和预设的更新周期，计算出下一次更新时间。

(2) 提醒信息发送：在印章到期一个月之前提供印章更新提醒。

7. 企业信息核验：通过资源共享交换平台进行企业身份核验，实现法人单位真实性核验。

8. 企业电子印章申请：

(1) 印章申请：对于持有法人数字证书的企业，可直接提交电子印章制作申请。

(2) 印章生成及下载：平台审核身份成功后生成电子印章。电子印章数据使用密码设备加密后安全存储。

(3) 印章管理：管理员在制作完成后，将电子印章部署到系统中，并进行相关管理操作。

9. 企业证书签发：

(1) 企业身份验证：验证申请证书的企业的身份信息，确保申请者合法且有权获得证书。

(2) 证书签发：系统具备对单位用户签发第三方数字证书，数字证书可作为单位用户真实身份保证单位用户在网络中的身份真实有效。

(3) 证书管理：记录证书的使用情况和更新时间，方便后续管理和维护。

10. 企业电子印章激活：

(1) 获取印章信息：具备印章信息获取。

(2) 印章验证：系统会对电子印章进行验证，确保其合法性和真实性。

11. 企业电子印章冻结：

(1) 单个印章冻结：暂停单个电子印章的使用，但其他电子印章仍然可用。

(2) 多个印章冻结：暂停多个电子印章的使用，但其他电子印章仍然可用。

12. 企业电子印章解冻：

(1) 确认电子印章已经被冻结：验证该电子印章是否已被冻结。

(2) 完成印章解冻：解冻后可进行权限内的系统操作。

13. 企业电子印章更新：先删除原有印章，再重新申请制作新印章，实现企业电子印章更新，增加印章使用期限；

14. 个人身份核验：对接公安部公民网络身份识别系统进行实名认证。

15. 个人电子印章申请：

(1) 印章信息填写：填写相关的印章信息。

(2) 印章生成及下载：平台审核身份成功后生成电子印章。

16. 个人电子印章审核：

(1) 获取印章信息：具备印章信息获取。

(2) 审核印章：对印章信息进行审核，并根据实际情况提供反馈意见；

(3) 管理印章：对已有电子印章进行管理。

17. 个人证书签发：系统具备对个人签发第三方数字证书，数字证书可作为个人真实身份保证在网络中的身份真实有效。

18. 个人电子印章激活：

(1) 获取印章信息：具备印章信息获取。

(2) 印章验证：系统会对电子印章进行验证，确保其合法性和真实性。

(3) 印章激活：系统具备个人通过云章平台进行电子印章激活，在申请完印章后可通过系统进行激活操作，激活后的印章可正常使用。

19. 个人电子印章查看：

(1) 电子印章查找：查找需要的电子印章。

(2) 电子印章预览：对选中的电子印章进行预览。

(3) 电子印章信息获取：对电子印章信息进行获取。

20. 个人电子印章冻结：

(1) 电子印章查询：查询已绑定在自己账号下的个人电子印章信息。

(2) 电子印章选择：选择对应的印章。

(3) 电子印章冻结：对个人电子印章进行冻结，冻结后不具备系统操作。

21. 个人电子印章解冻：

(1) 确认电子印章已经被冻结：验证该电子印章是否已被冻结。

(2) 完成印章解冻：解冻后可进行权限内的系统操作。

22. 个人电子印章更新：

(1) 重新申请制作新印章：具备个人用户申请重新制作新印章，并设定电子印章样式。

(2) 增加印章使用期限：实现电子印章更新，增加印章使用期限。

23. 个人电子印章删除：

(1) 印章信息查询：查询已经申请过的电子印章信息。

(2) 印章信息获取：获取印章信息。

(3) 印章删除：将已申请的电子印章删除，印章删除后将看不到印章信息，如需使用印章，需重新进行印章申请。

24. 电子印章统计功能：具备按时间、按人员、按申办单位量、按印章量等不同维度统计政府电子印章发放及应用情况、企业电子印章、个人电子印章发放及应用情况。

(二) 电子印章应用服务升级改造

对电子印章应用服务进行升级改造，将原有应用服务进行升级，新增 API 接口、应用集成管理、可视化签署、授权签署、协同签署、云签名认证管理、密钥管理等功能。并针对印章管理提供微信小程序、APP、WEB 终端等多种接入方式。

1. 文档处理 API：提供文档处理 API 接口，通过文档对 API 接口进行填写处理。

2. 文档签章 API：提供文档签章 API 接口，业务系统调取签章 API 接口，完成签章。

3. 文档验章 API：提供文档验章 API 接口，业务系统调取签章 API 接口，

完成签章文档真实性验证。

4. 应用集成服务：提供应用系统接入云章服务所需应用集成服务，完成云签章的接入。

5. 应用开通服务：提供应用系统接入云章服务所需应用开通服务，开通服务后可随时调取签章功能签章。

6. 应用配置服务：提供应用系统接入云章服务所需应用配置服务，标准化配置，实现云章功能。

7. 可视化签章：

(1) 可视化预览：实现可在页面预览 PDF，确保签章位置准确性。

(2) 获取认证方式：获取认证方式。

(3) 获取可视化签署地址：获取可视化签署地址。

(4) 签署文件下载：签署文件下载。

(5) 签署完成通知：签署完成通知。

8. 可视化验签：

(1) 可视化预览：实现可在页面预览 PDF。

(2) 验证签章真实性：实现可视化验签功能，确保签章真实性。

(3) 签署信息查询：签署信息查询。

9. 查看授权：可以通过授权人姓名、身份证号等信息来查询该授权人所完成的所有印章记录。

10. 增加授权：系统具备对印章使用人的增加，可通过系统将印章授权给多个人使用；

11. 冻结授权：

(1) 显示已授权印章列表：系统具备在可视化页面上显示所有已授权的印章列表。

(2) 查看印章详情：系统具备在可视化页面上查看某个特定印章的详细信息，包括印章类型、授权人、授权时间等。

(3) 冻结印章：系统具备在可视化页面上对任何一个已授权的印章进行冻结，一旦冻结，被授权人将无法使用该印章。

12. 解冻授权：

(1) 显示已冻结印章列表：系统具备在可视化页面上显示所有已冻结的印章列表。

(2) 查看印章详情：系统具备在可视化页面上查看某个特定印章的详细信息，包括印章类型、授权人、授权时间等。

(3) 解冻印章：系统具备通过可视化页面对已经冻结的印章进行解冻。

13. 取消授权：系统具备通过可视化页面对已经授权的印章进行取消授权操作，取消授权后相关人员无印章使用权限。

14. 协同授权签名：

(1) 授权签名设置：设置授权签名的各类参数和规则，包括签名算法、签名域、签名时限等。

(2) 协同授权签名：通过密钥协同运算方式进行授权签名，实现多方合作签名，保证签名结果的完整性和安全性。

(3) 签名验证：验证签名的有效性和真实性，避免篡改和伪造。

15. 二维码推送：

(1) 二维码生成：系统具备生成待认证/签名任务的二维码，并将其展示。

(2) 扫码识别：系统具备在移动端设备上扫描二维码，并将待认证/签名任务信息获取到本地。

16. 时间戳服务配置：系统具备通过 web 页面以可视化的方式对时间服务进行配置管理，可通过页面配置时间戳服务地址，满足时间戳服务的调用，具备新增、修改、删除等操作。

17. 协同签名统计分析：

(1) 用户量统计分析：系统具备对注册用户数量进行统计分析。

(2) 证书签发量统计分析：系统具备对签发的数字证书数量进行统计分析。

(3) 签名量统计分析：系统具备对签名数量进行统计分析。

18. 协同签名日志审计：

(1) 日志记录：系统可以自动记录所有用户的签名行为，并将其存储到系统日志中。该功能用于跟踪签名活动和进行审计。

(2) 日志统计：系统能够根据所记录的日志数据，自动生成有关签名数

量、证书数量、用户数量等方面的统计信息，以帮助管理人员了解系统运营情况。

(3) 审计和检查：系统具备对每天所记录的信息进行审计和检查，通过日志，管理人员可以了解系统的系统签名数量、证书数量、用户数量的情况。

19. 根证书管理：配置管理云签名认证网关所信任的根证书（根证书是未被签名的公钥证书或自签名的证书）；

20. CRL 管理：

(1) 管理 CRL 下载地址：允许管理员配置和管理根证书对应的 CRL 下载地址。

(2) 列出可疑证书：列出被认为不能再使用的证书的序列号。

(3) 监控证书状态：允许管理员监视信任列表中证书的状态，并在证书到期或被吊销时收到通知，以便及时做出反应并保证证书的有效性。用户管理：配合云签名服务完成单位用户和个人用户人员的全生命周期管理，从生成到删除。

21. 证书管理：配合云签名服务完成单位用户和个人用户证书的全生命周期管理，从生成到销毁。

22. Hash 计算：具备对数据进行 hash 计算，将任意长度的二进制值映射为较短的固定长度的二进制值。

23. 文档格式具备管理：

(1) 具备 pdf 格式文档签章：具备 pdf 格式的文档签章，保证文档的完整性和真实性。

(2) 具备 ofd 格式文档签章：具备 ofd 格式的文档签章，保证文档的完整性和真实性。

(3) 多种文件格式支持：具备在一个平台上对多种不同类型的文件进行数字签名，包括 pdf、ofd 以及其他常见的文档格式。

24. 文档预处理：

(1) 文档检查：检查待签章文档是否符合签名要求，例如文档格式、大小、页数等。

(2) 文档解析：对待签章文档进行解析，提取文档内容，生成文档 hash 值，以确保文档的完整性和一致性。

(3) 文档预览：对待签章文档进行预览，以便在签署前查看文档内容，确认其正确性和完整性。

25. 文档合章：配合外部配备的签名模块对文档预处理 hash 值签名后，得到的签名结果和印章信息进行合章，完成文档签章。

26. 文档坐标签章：

(1) 设定坐标值：具备在文档中指定要放置电子印章的位置。

(2) 定位电子印章：根据设定的坐标值，在文档中精确定位电子印章的位置。

(3) 在设定位置完成文档签章：在指定位置签署选定的电子印章。

27. 文档关键字签章：

(1) 设定关键字：具备根据关键字在文档中指定要放置电子印章的位置。

(2) 定位电子印章：根据设定的关键字，在文档中精确定位电子印章的位置。

(3) 在设定位置完成文档签章：在指定位置签署选定的电子印章。

28. 文档骑缝章：通过选定骑缝位置，具备左右骑缝章，具备奇偶页骑缝章设置。

29. 文档添加水印：具备对待签章文档，通过自定义方式添加水印，确保文件不被调用。

30. 批量文档签章：为了适应大量签章业务场景，具备批量文档签章，批量签章时，具备不同文档不同章。

31. 文档验章：具备验证文档已签章文档签章有效性。

32. 文档上传下载：具备对待签文档的上传下载，同时具备已签文档的上传下载，能够基于文档 ID 号完成文档签章。

33. 产生挑战随机数：具备产生随机数，使用该随机数可作为登录认证的挑战随机数，确保登录真实性。

34. 验证签名：

(1) 验证签名有效性：对签名结果进行验证，确保签名结果是由合法的签署者签署，并且签名结果未被篡改。

(2) 验证签章信息完整性：确认签名中包含的签章信息是否与原始文件

一致。

(3) 显示验证结果：展示签名验证的结果。如果签名验证成功，则显示验证结果为“有效”，否则显示验证结果为“无效”。

35. 验证证书：具备对标准格式 X.509 证书有效性进行验证。

36. 证书解析：

(1) 获取证书基本信息：获取证书的基本属性信息，例如：序列号、颁发者、有效期、公钥等。

(2) 证书解析：具备解析标准格式 X.509 证书内容，获取证书属性信息。

(3) 检查证书合法性：检查证书是否合法，包括证书链验证、crl 检查、ocsp 验证等。

37. P1 签名转 P7 签名：具备 P1 格式签名值转换成 P7 格式签名值，可做到无损转换。

38. 文件签章：为政务事项办理提供业务支撑，可以对接入的电子政务系统提供文件签章服务。在文件签章页面，能够完成上传 PDF 文件签章、已签署文件下载、已签署文件查看文件删除、已签署文件验签等操作。

39. 文件验签：为政务事项办理提供业务支撑，可以对接入的电子政务系统提供文件验签服务。

40. APP 接入： 在业务 APP 中进行云章管理和使用的入口，与业务 APP 对接，嵌入到业务 APP 中实现基于业务 APP 用户体系的用户注册、印章申领、印章管理、印章授权、扫码授权签章等功能。

41. 微信小程序：实现以微信小程序的形式提供云章管理和使用的入口，实现在微信端的用户注册、印章申领、印章授权、扫码授权签章等功能。

42. 签约模板文件管理：对于签约模板文件进行管理，该模板用于生成电子协议版式文件。实现版式文件的生成、修改、删除等生命周期管理，可生成动态模版；

43. 签约授权管理：对于签约授权进行管理,具备菜单授权管理、数据授权管理；

44. 签约文件管理：对于签约文件进行管理，具备合同文件查询、预览、下载、撤销等管理；

45. 签约统计管理：对于签约统计进行管理，具备用印台账管理、证书查询；

46. 签约审计管理：对于签约审计进行管理，具备系统日志管理、业务日志管理、系统运行日志管理；

47. 签约证书管理：对于签约证书进行管理，具备根证书管理、法人单位证书管理、个人证书管理、CRL 列表管理；

48. 签约机构管理：对于签约机构进行管理，具备组织机构管理、法人单位管理、部门管理，具备树形分层；

49. 签约用户管理：对于签约用户进行管理，具备管理员管理、签章操作员管理；

50. 签约印章管理：对于签约印章进行管理，具备印章的生命周期管理，主要包括印章创建、修改、查询、删除、启停等，具备印章图片上传、根据印章模板自动生成；

51. 电子协议发起：具备从第三方业务系统（通过服务接口）发起协议，也具备协议发起方直接在统一电子印章服务平台上直接上传和发起协议。发起协议时定义协议名称等必要的基础信息，选择一个或多个协议签约方，完成协议发起；

52. 电子协议签章：协议签约方使用数字证书对电子协议进行签章。签章时，可以选择事先配置好的电子印章（如公章、合同章、人名章等），统一电子印章服务平台具备手动盖章、批量盖章、骑缝章等多种盖章方式。盖章位置可以手动拖拽选择，或根据关键字自动定位和加盖。电子协议签章可以同时增加时间戳，实现对协议签约的时间认证；

53. 电子协议验证：签约完成后的电子协议，具备本地离线的 PDF 签章验证、统一电子印章服务平台上的在线验证，以及第三方验证等多种方式。在线验证可以完整验证电子协议中的每一个签章的有效性；

54. 具备数据签名及验证：非对称国密 SM2 算法的私钥对数据进行签名，使用对应的公钥对数据签名进行有效性验证，检验信息真实性，防止信息篡改；

55. 具备数据加解密:具备对称国密 SM4 算法加解密,同时具备 ECB、CBC、OFB 模式加解密；

56. 文件签名与验证：具备非对称国密 SM2 算法的私钥对文件进行签名，使用对应加密的公钥对文件签名进行验证，确保其真实性。

（三） 电子印章运营服务

1. 电子印章运营管理升级改造：为运营管理人员提供渠道管理功能，提供运行监控、运维管理服务及动态展示等服务，面向政务管理人员提供可视化数据展现，提供精准研判依据的同时，利用信息化技术切实有效的保障平台安全、可靠、稳定的运行。

2. 电子印章运营可视化升级改造：提供大屏展示功能。具备一站式数据可视化展示平台，能够以图表的形式展示整个平台的注册用户总数、注册单位总数、激活印章总数、签章验章总量、印章增长趋势、签章验章增长趋势等数据，协助客户更加直观和方便的了解运营管理的数据统计情况。

3. 政府单位电子印章运营服务：提供为期 3 年的政府电子印章运营服务，签发单位数字证书 2500 套，标识单位用户网络身份，提供电子印章的申请、制作、使用、变更等生命周期管理服务，具备对公文、证照、电子票据等各类电子文档提供电子印章服务。能够对历史签发的电子印章数字证书进行更新。

4. 企业电子印章运营服务：提供为期 3 年的企业电子印章运营服务，每年签发企业数字证书 4 万套，累计 12 万套，每套包含企业公章、财务章、发票章、合同章、法定代表人章五枚印章发放和签署服务。能够对过期的企业电子印章数字证书进行更新。

5. 个人电子印章运营服务：提供为期 3 年的个人电子印章运营服务，3 年累计不超过 100 万次，提供个人电子名章服务，实现网上办事电子签章应用。

6. 人员驻场服务：提供为期 3 年的 5*8 小时驻场服务，驻场人员 4 人，服务内容包括但不限于安全巡检、日常运维、运行分析、数据管理和维护等。

（四） 电子印章公共基础设施升级改造

对电子印章公共基础设施进行升级改造，将原有基础设施进行升级，新增云服务器密码机 2 台和时间戳服务器 2 台，完成加解密运算及加盖时间戳，保障安全性、合法性。

1. 云服务器密码机（2 台）

云服务器密码机需要满足以下功能：

(1) 基于虚拟化技术，具备单台宿主机创建虚拟密码机≥96 个，具备虚拟密码机的创建/启动/停止/删除；

(2) 具备对称算法：SM1、SM4,具备 ECB，CBC 模式。具备非对称算法：SM2，具备杂凑算法：SM3；

(3) 采用安全隔离技术，具备对每个虚拟密码机使用的密钥在存储和使用上进行安全隔离；

(4) 具备虚拟密码机漂移，虚拟密码机漂移速度可达毫秒级；

(5) 具备虚拟密码机的迁移，具备将正在运行中的或停止运行的虚拟密码机机从当前宿主机迁移至另一台宿主机上；

(6) 具备资源动态分配，利用负载均衡技术实现虚拟密码机对密码资源占用的动态分配，管理系统可以根据实际情况动态增加或释放密码运算资源；

(7) 具备镜像加密保护，对虚拟密码机内操作系统、与用户相关的配置、密钥及敏感信息等整个镜像进行加密和完整性保护；

(8) 具备租户权限管理，具备云服务器密码机宿主机和虚拟密码机设备管理配置，具备对多台虚拟密码机的集群管理；

(9) 采用由国家密码局审批的双 WNG-9 随机数发生器产生的真随机数，单个虚拟密码机具备生成≥1024 位 ECC 密钥对。具备私钥权限码功能，保证不同应用系统的密钥使用安全；

(10) 具备系统管理员、审计管理员、安全管理员三权分立。分别赋予不同的操作权限。具备采用数字签名技术，实现对登录用户的强身份认证。

(11) 具备 JCE、PKCS#11、SDF 等多种标准密码应用接口，满足传统应用迁入虚拟化及云环境后对密码服务的需求；

(12) 具备日志审计功能，日志信息包含系统日志、错误日志和操作日志等，对日志信息进行签名及完整性校验，确保关键日志信息防篡改，日志信息可查看及导出，日志保存 6 个月以上；

(13) 具备采用 B/S 管理方式对设备进行管理，提供设备管理统计数据及监控管理功能;

(14) 具备虚拟密码机之间网络双活，具备白名单功能；

(15) 具备多方协同签名、多方协同解密，密钥分散等功能；

(16) 设备高度≤2U；

(17) 网络接口≥2*1000M；

(18) 电源指标：冗余电源；

(19) 云服务器密码机符合 GM/T 0018-2012 《密码设备应用接口规范》、GM/T 0028-2014《密码模块安全技术要求》第二级要求。

2. 时间戳服务器（2 台）

时间戳服务器需要满足以下功能：

(1) 具备 HTTP 协议的时间戳签发和验证；

(2) 内置权威时间源模块，信号源 4G/5G、北斗，符合国家授时中心的时间精度标准，并且经国家授时中心的权威鉴定测试，时间误差＜2 毫秒；

(3) 具备算法： SM2、SM3 等国产密码算法；

(4) 时间同步：具备 NPT、SNTP 时间同步协议；

(5) 授时精度：0.5-3ms(毫秒)；

(6) 守时精度：〈1ms（72 小时），内置恒温晶振；

(7) 对外可提供高稳定、高性能的服务，具备热备负载功能；

(8) 提供 C、COM 、Java 等主流开发 API；

(9) 设备高度≤2U；

(10) 网络接口≥2*1000M；

(11) 电源指标：冗余电源；

(12) 内置恒温晶振：日老化率≤ 5E-10，秒稳定度≥ 2E-11，日平均准确度≥ 1E-12；

(13) 性能参数：时间戳签发速率（SM2） ≥8000 次/秒，验证效率（SM2）≥3000 次/秒。

(14) 时间戳服务器符合 GM/T 0018-2012《密码设备应用接口规范》、GM/T 0028-2014《密码模块安全技术要求》第二级要求，具备 RFC8200、8201 等标准协议，具有良好的一致性和互通性。

(五) 电子印章接入服务升级改造

对电子印章接入服务进行升级改造，接入统一身份认证系统、黑龙江省电子印章平台、电子营业执照系统、政府电子公文系统等业务系统，对接银行及其他

省市电子印章系统，同时与司法鉴定机构、公证处、公安电子印模库对接，保证电子印章合法合规并提供司法保障。

1. 统一身份认证系统接入服务：接入哈尔滨市 PC 端及移动端统一身份认证系统，实现企业及个人用户通过手机扫码的方式登陆统一身份认证系统。

2. 电子营业执照接入服务：具备与电子营业执照系统对接。

3. 公安电子印模库接入服务：具备与公安电子印模库对接，对接公安电子印模库，获取印模编号、印模图片等数据。

4. 司法鉴定机构接入服务：客户应用电子签名发生纠纷时，根据客户的鉴定需求申请电子签名电子数据鉴定，司法鉴定中心利用专业的司法鉴定工具、采用特定的鉴定方法对纠纷涉及的电子签名数据进行分析、鉴别，得出电子签名数据是否被篡改以及电子签名行为真实性认定等鉴定意见，并出具具有法律效力的司法鉴定意见书。

5. 第三方数据保全接入服务：实现在采集完成后立即固化和加密，在事后出现纠纷时，可提供对应的司法服务。

6. 公证处接入服务：提交委托协议及相关材料至公证处，具备同步电子印章数据到公证处进行电子数据存证。

7. 银行接入服务：实现与银行业务系统对接，实现企业远程开户，助力“企业开办直通车”的电子印章应用。

8. 其他省市电子印章系统接入服务：具备与北京、深圳等其他省市电子印章接入，实现电子印章的跨域互认。

9. 接入黑龙江省电子印章平台服务：具备对接黑龙江省统一电子印章系统，按照《黑龙江省统一电子印章接口要求》，对哈尔滨市统一电子印章服务平台进行用章、验章、获取印章接口升级。

10. 业务系统接入服务：提供电子印章系统与我市行政审批系统、国家水利部出水许可证证照系统、哈尔滨不动产电子证照应用系统、全国中小型企业融资信用服务示范平台系统、哈尔滨市网约车登记系统、哈尔滨市城乡居民医疗保障服务大厅系统、哈尔滨市职工及单位医疗保障服务大厅系统、哈尔滨市企业开办直通车系统、哈尔滨市企业注销直通车系统等系统的接入服务，实现事项审批、办结、证照生成等环节的电子印章服务。

（二）统一政务服务网网站及移动端特色内容建设

具体技术（参数）要求
统一政务服务网网站及移动端特色内容建设 现有政务服务网网站及移动端能力如下：提供政务服务事项网上办理、事项查看、便民应用、大数据展示等数据指标与应用服务，2021 年按照国家政务服务网统一门户要求与省政务一体化门户对接，完成哈尔滨政务服务网向省级一体化过渡阶段，已对接哈尔滨全部政务服务事项、特色门户应用服务、高频查询专区、统一身份认证等栏目。哈尔滨移动端与政务服务网同步建设投入使用，移动端包括特色专区与高频服务，2021 年按照全国一体化移动端要求，将哈尔滨移动端特色应用 20 余项目进行上报对接。 本期按照《关于确认第一批黑龙江省数字政府建设项目中涉及市级（含县级）项目的通知》，哈尔滨市根据自身情况，从特色专区清单、简单高频应用清单、复杂高频应用清单中选取应用，进行建设，并同时在政务服务网、移动端安卓版、移动端 iOS 版、微信小程序版、支付宝小程序版五端上线。 哈尔滨政务服务网主要依托省平台支撑底座、能力支撑系统、后端支撑系统、服务功能、服务界面。其中支撑底座主要包括工作台服务、工作协同服务、消息推送服务、文本检测、元数据表单管理服务、任务调度中心服务、工具箱服务、日志管理服务等。能力支撑系统主要包括：事项同步系统、事项管理系统、资源库建设支撑、政民互动系统、智能检索系统、智能推荐系统、应用代理组件、统一消息组件、综合查询系统等。后端支撑系统主要包括：多语言版系统、内容管理系统、无障碍系统、专题专区建设支撑、统一预约支持、门户网站建设后端支撑系统、手机版网站建设支撑、网站适老化改造建设支撑。 1、政务服务网网站 系统需基于省级政务服务网网站建设哈尔滨专区。 （1）栏目标准适配改造 现有PC门户专区栏目服务需按省数字政府PC端应用接入视觉设计要求标准设计对接完成接入调试。包括页面布局、内容发布、链接接入、页面视觉风格等。 页面布局、页面视觉风格要有固定标准并且做到视觉统一。

针对内容信息要有内容校验功能，对涉密或敏感信息进行相应处理。

（2）接口开发改造

需具备门户相关接口接入，要对接口自行进行封装，接口开发要求符合基于 http 的 RestFul 设计风格，请求方式具备 get 或 post。

提供接口需有入驻能力，并且接口需传输加密和白名单等安全性保证，对输出数据进行数据脱敏，脱敏范围应不少于 50%，常见用户隐私信息脱敏规则如下。

中文姓名脱敏 李** 保留第一位，后面以*替换；

公民身份号码脱敏 **********5762 保留后 4 位；

固定电话脱敏 ****1234 保留后 4 位；

手机号码脱敏 1******34 保留第一位，后面保留 2 位；

地址脱敏 北京市海淀区**** 保留前 6 位；

电子邮箱脱敏 g**@163.com ***@后面的部分；

银行卡号脱敏 622260**********1234 保留前 6 位后 4 位；

公司开户银行联号脱敏 12******** 保留前 2 位；

时间类的处理，建议脱敏规则为：入参 yyyymmdd（没有下划线，中划线）****1234 保留后 4 位，可根据不同业务需求场景自行判断是否脱敏。

（3）应用开发标准改造

需完成门户专区相关栏目适配开发工作，按照相关省标基于省政务服务统一平台完成相应特色栏目、专区服务、接口能力开发应用。见表 2.1、表 2.2、表 2.3。

需保证流程、接口、界面风格等的统一性。

（4）应用注册

应提供各接入单位登录应用管理平台注册应用基本信息，注册时应对相关信息及内容进行相关约束，有唯一身份标识，对人员身份进行校验。

（5）市级能开接入

应提供基于省级接口能力开发平台接入标准，完成能开接口接入能力。将哈尔滨政务服务门户相关能力接口上架发布管理，同时接入省级能开平台。能力封装内容信息包括接口地址、请求方式、接口协议以及相关请求参数与返回结果示例。

（6）省事能开接口联调

市集能开需要与省级平台连通后，将提交接口至能力开放平台后，需要基于能力开放平台统一输出的接口自行调试接口，便于完成后续应用开发。

（7）用户对接与注册对接

应用开发过程中，部分应用是涉及到用户对接的，应用需对接统一身份认证系统。Web 端应用对接统一身份认证后，可以通过政务服务门户传递票据，获取用户信息。

同时按照省级统一注册汇聚接口完成我市全量用户汇聚能力。对接完成统一用户登录方式与接口对接。

与省统一申报、省新闻信息发布、省智能客服、特色目录等我市现有专区栏目、链接、接口、H5 页面等按照省级标准接入省数字政府统一门户中。

（8）通过省级能开平台获取统一申报系统能力接口，对哈尔滨门户相关特色栏目申报表单信息进性维护等。

2、移动端子站

按照数字政府移动端应用开发对接接入 API 规范标准对接黑龙江省数字政府政务服务移动端。具体要求与 PC 门户一致。

哈尔滨市按照省统一全省事要求接入现有专区栏目、链接、接口、H5 页面等按照省级标准接入省数字政府统一全省事 APP、小程序中。

建设重点建设清单目录如下。

表 2.1 特色专区清单

特色专区清单	
序号	名称
1	省内通办专区
2	智能秒办
3	全程网办
4	一件事一次办
5	多证合一
6	营商环境专区

7	在线帮办服务专区
8	企业开办注销
9	老年人专区
10	妇幼服务
11	一证查事
12	扫码亮证

表 2.2 简单应用接入清单

简单应用接入清单	
序号	应用名称
1	落户审批查询
2	社会组织信息查询
3	个人住房信息查询
4	商品房合同备案查询（商品房房屋交易信息）
5	建筑企业基本信息查询
6	施工许可证信息查询
7	失信被执行人查询
8	信用黑名单查询
9	公积金缴存记录查询
10	公积金提取记录查询
11	公积金缴存信息查询
12	有无违法犯罪记录证明开具
13	户口审批查询
14	高校毕业生落户查询
15	道路运输经营许可信息查询
16	网络预约出租汽车运输许可信息查询
17	出租汽车营运许可信息查询

18	网约车驾驶员查询

表 2.3 复杂应用接入清单

复杂应用接入清单	
序号	应用名称
1	话费缴纳
2	公共场所卫生许可证查询
3	水费缴纳
4	电费缴纳
5	燃气费缴纳
6	暖气费缴纳
7	城市低保救助申请
8	农村低保救助申请
9	失业补助金申领
10	公积金提取

（三）一体化政务服务及创新应用建设

具体技术（参数）要求
一体化政务服务及创新应用建设 现有一体化政务服务及创新应用能力如下：已建成一库一门户三平台，统一的政务服务信息资源库（一库）、互联网政务服务门户（一门户）、政务服务管理平台、业务办理平台、政务数据支撑共享平台。 本期建设以下内容： 1.打造更多政务服务创新应用。 聚焦优化一体化政务服务，打造一批具有我市特色的证易办、文易批、一证办、免证办、容缺办、无感办、延时办、远程验等创新应用，持续发力便民利企、优化营商环境、全程电子化分析，推进政务服务由“可办”向“好办”、“易办”、“愿办”转变。

2.优化一体化政务服务平台。

将哈尔滨市相关数据全部割接到省级数字政府统一申报平台、电子监察平台、好差评管理系统，实现一体化政务服务平台省建市用。升级办件子库、事项子库，完成市自建系统办件数据实时归集，完成办件数据由省向市定时回流。利旧受理中心、办理中心，与省级政务服务平台对接，互联互通。精细化梳理事项，按照“四级五十同”标准，对标全国先进水平，梳理全省政务服务事项。落实全省“办好一件事”的对接和应用工作，哈尔滨市现有“一件事一次办”，对照省级下发的“黑龙江市地级一件事建议清单”，市级需到省级平台维护、对接。

（一）创新应用

聚焦优化一体化政务服务，打造一批具有我市特色的证易办、文易批、一证办、免证办、容缺办、无感办、延时办、远程验等创新应用，持续发力便民利企、优化营商环境、全程电子化分析，推进政务服务由“可办”向“好办”、“易办”、“愿办”转变。

1、开发互联网+民生系统

需根据民生大小事的业务需求，开发互联网+民生系统，以互联网+思维，重构民生大小事处理的理念与思路，改革传统受理渠道单一、事件层层分转、处理周期漫长、群众意见较大的弊端，通过人工智能等技术的运用，对民生事项精准分类梳理、加注智能标签、网络电话多渠道获取、全流程网办，建设扁平化、全渠道、全在线、即时达、强监管的民生服务与社会治理体系，群众迫切需求直达处理人员，即诉即接即办，切实提升民生民意处理效能和人民群众的满意度。主要建设内容需包括以下几点。

（1）民生事项智慧化梳理

利用大数据，分析我市历史数据，归纳总结民生需求数据，建设我市民生事项库。将民生事项由电话接听人的自由发挥向全面分类、科学定义转变。建设实时动态更新机制，有新需求、新部门、新事项、新方法时随时自动入库。

（2）训练民生任务智能分配机器人

选择适合的神经元网络算法，利用我市民生数据，训练民生任务智能分配机器人，做到当民生诉求进入系统，开启智能分配机器人，做到即诉即达即办。

（3）民生事项人工优化系统

需具备人工配置关联事项前后置关联关系。需具备对 12345 平台事项的来电内容及办理办事进行人工加注标签，包括关键字、来电区域、来电人员、诉求、事发区域、办理路径、办理结果等。

（4）民生大小事多渠道收集系统

需开发多端民生大小事多渠道收集系统，与传统系统融合，实现民生大小事全渠道收集，推进完善民生大小事诉求的标准化、规范化与网络化。

（5）民生大小事办理系统

需具备收到办理事件的工作人员，开展办理工作，将办理结果通过工作机上报。采用工作流等系统对智能机器人和人工坐席人员无法精准分配的新兴事件，具备传统人工层层分转，直达办理部门与人员。事项处理完毕同步更新事项库与机器人算法。

（6）大数据统计分析与辅助决策系统

系统需开发大数据统计分析与辅助决策系统，全面统计民生事项数据，并归纳总结民生事项发生频次，提前预判与应对，在大屏幕上全面展示。

（7）民生事项办理好差评系统

系统需对民生事项办理结果做评价，群众可通过多渠道进行评价，对评价数据进行统计，对差评进行跟踪整改。

（8）民生事项电子监察系统

系统需引入电子监察机制，对各部门、各类事项开发监察规则设置、实时监控、预警纠错、督查督办、大数据监察等功能，进行全方位监察民生大小事项。

（9）系统对接与数据共享

系统需将互联网+民生系统与网格系统互联互通，实现业务协同；与数据资源中心对接，实现民生数据的全面共享应用。

2、建设便民服务频道

在一体化平台首页设计、开通便民服务频道，整合或新建便民服务子系统，整合多方多项便民服务，做到一站式为民便民服务。

（1）便民服务门户

优化便民服务专栏形式及内容，将常用服务事项进行高频常用展示，并提供配套支持服务入口。

（2）便民服务后台管理

新增便民服务后台管理功能，实现门户便民服务链接配置、页面设置、发布审核、服务撤销等功能。

事项梳理新增公共服务。通过事项梳理能够更多的服务公众人群。

（3）用电服务

- 电费缴费服务
- 电费查询服务
- 用电故障报修服务
- 个人二手房更名联动过户（不动产、水、电、燃气、电视）
- 居民电力客户过户
- 事项梳理新增服务
- 建设项目基建临时用电申请
- 建设项目正式用电申请

（4）供水

- 水费缴费服务
- 水费查询服务
- 停水通知
- 供水报装
- 供水报装（临时用水）
- 征收止水核定
- 供水接入（临时用水）
- 供水接入
- 中小微企业临时用水核定
- 中小微企业正式用水核定

（5）排水

- 排水报装
- 排水接入

（6）燃气

- 居民电子发票

- 居民普表燃气用户缴费服务
- 居民 IC 卡表燃气用户缴费
- 燃气工商服用户发展（工业和整体性仓储项目，政府投资公益类项目及基础设施类项目）
- 燃气居民用户发展
- 燃气工商服用户发展

（7）供暖

- 供热缴费
- 供热报停
- 在线诉求
- 卡号管理
- 电子票据

（8）有线电视

- 有线电视新建建筑物内暗埋配套工程验收
- 有线电视工程报装

（9）通信服务

- 宽带新装：移动、联通、电信等运营商
- 电话缴费：移动、联通、电信等运营商

（10）公证服务

- 公证员执业审批（一般任职）
- 公证员执业审批
- 公证机构设立
- 公证机构查询
- 公证员变更执业机构核准（跨省变更）
- 公证员变更执业机构核准（市内变更）
- 直属公证机构及负责人的年度考核
- 公证员变更执业机构核准（省内变更）

（11）法律援助

- 法律援助申请

- 对申请人不服法律援助机构作出的不符合法律援助条件的通知的异议审查
- 法律援助补贴发放
- 公证机构分立、合并或变更执业区域核准（合并）
- 公证机构分立、合并或变更执业区域核准（分立）

（12）信用服务

- 行政处罚信息信用修复

3、对接公租房办理系统

需建立对接公租房办理系统，通过接口形式接入公租房自建系统，通过政务服务网将受理数据传送至公租房办理系统，办件结果回传至政务服务网的功能，将公租房事项纳入政务服务网，为办理公租户人员提供“一网通办”。内容包括办理公租房事项梳理、办理公租房事项政务服务网展示、事项申请表维护、事项材料目录设置、事项办件数据落库、系统对接。

（1）办理公租房事项梳理

梳理办理公租房事项办事指南，办事指南要素维护到事项子库，并发布到政务服务网。

（2）办理公租房事项政务服务网展示

事项搜索功能，快速查询，进行网上申报或办事指南查看。

（3）事项申请表维护

根据梳理事项进行事项申请表单维护，满足办理事项所需信息要求。

（4）事项材料目录设置

根据梳理事项进行事项目录维护，满足办理事项所需申报材料要求。

（5）事项办件数据落库

需将公租房自建系统办理完成数据进行办件储存，用户可在政务服务网进行办件数据查询、办件材料复用等操作。

（6）系统对接

提供多端对接标准，完成与公租房办理系统对接。实现政务服务网受理信息数据推送至公租房办理系统；办件结果及状态等数据回传至政务服务网及办件中心，对办件量做统计。

4、智能 OCR 表格识别应用

内容包括扫描和导入图像、图像的调整、表格的元数据定义和提取、文档的输出和自动挂接、兼容多种系统、具备扫描仪、配备 OFD 格式转换和预览、自动数字化图像预处理技术、具备单机版和服务器功能、扩展性。

(1)扫描和导入图像

智能 OCR 提取识别软件具备直接导入已有图像文件序列，或从已有的 pdf 文件进行仿真扫描导入图像。

客户端具备手工将图像分割为不同文档，文档间图像次序调整。多文档合并，一个文档拆分功能。

(2)图像的调整

扫描或导入到工具中的图像，具备图像先后顺序、旋转方向调整。实现必要的图像处理。

(3)表格的元数据定义和提取

需通过 OCR 识别提取属性的值，定义文档的指定表格的某个区域进行 OCR 识别。每个证照都可以定义多个识别区域，表格提取模板进行保存。

(4)文档的输出和自动挂接

图像经过 OCR 识别和格式转换，可以批量上传到业务系统或者保存到本地磁盘中。

输出到业务系统时，应该根据文件属性实现自动的内容信息条目建立和著录。经过 OCR 的输出文件的格式具备包含文字信息的双层 ofd。

输出到本地磁盘时，文档属性可以存放到对应的 ofd 文件中，或者保存为一个 XML 文件。

(5)配备 OFD 格式转换和预览

系统能够直接把扫描结果以国家标准的版式 OFD 格式输出到业务系统。提供转换接口，与客户端无缝集成。

(6)自动数字化图像预处理技术

具备图像预处理能力，提高 OCR 算法的准确性。

提高处理文件速度，实现一系列自动预处理。

(7)具备单机版和服务器功能

需实现表格区域设置和画框提取。

(8)扩展性

需对机打清晰、表格内容在表格内并且对位准确的表格信息，自定义表格提取，适应各种表格内容的提取。

5、企业云章应用

服务系统指：移动端、小程序等多端应用。

内容包括应用、调取、验证、转换 PDF 板式文件、预览。

(1)应用

需在应用端对申报过程或特定环节增设企业云章加盖能力，调用企业云章实现政务服务应用上得企业云章功能。

(2)调取

通过企业云章绑定的参数，返回可用印章。

申报系统调用电子印章平台触发数据共享接口，传递给省印模系统参数；

省印模系统根据请求参数找到对用匹配的所有印模，通过数据共享交换平台返回至印章平台；

电子印章平台将返回的所有类型的章展示在申报系统；

选择需要的类型章，加盖至电子文件上。

(3)验证

申报系统具备对常用文档的签章。

申报系统调用电子印章平台签章接口参数；电子印章平台找到要签盖的印章类型；申报系统使用要签盖的印章，完成签章；将签章结果及签章后的文件返回给申报系统。

(4)转换 PDF 板式文件

需读取传入的电子文档（word 等格式），解析文档，利用 CA 数字证书及 PKI 算法，进行数字签名，将数字签名及印章图像捆绑，更新形成新的 PDF，输出已签章的 PDF 文档（或 PDF 流）。盖章保存文件，生成 PDF 版式文件，不可修改。

(5)预览

对盖章后的 PDF 文件提供在线预览功能。

6、证易办

建设证易办，内容包括证易办门户、智能搜证、智能引导、常见问题、智能问答、系统管理。

（1)证易办门户

证易办门户内容包括门户设计、主题分类、已办件列表、已办件统计分析、办证进度查询。

（2）智能搜证

提供市事项子库全库搜索功能。将检索出来的事项、证照结果分类高亮展示在搜索功能中，找到对应的事项或证照后可以选择办理或查看办事指南。

（3）智能引导

区域引导通过选择四级联选（市、区县、乡镇街道、社区村屯）快速分类定位证照事项范围。

事项类型问选，通过事项类型的不同，分类筛选。

事项专选，通过对不同事项预先设置的问题与答案，关联事项内容不同的表单字段、材料，做到申请人在选择问题后，申请表单或申请材料对应进行情形缩减，展示当前情形下的所需内容。

（4）常见问题

需提供常见问题展示栏目。

（5）智能问答

需提供智能问答导办功能。

（6）系统管理

需包括市事项子库标签管理、问题与答案库管理、页面风格管理。

7、文易批

建设文易批，内容包括文易批门户、智能搜文、智能引导、常见问题、智能问答、系统管理。

（1）文易批门户

文易批门户，包括门户设计、主题分类（个人、企业、主题等分类展示）、已办件列表、已办件统计、批文办理进度查询。

（2）智能搜文

提供市事项子库全库搜索功能，将检索出来的事项、批文结果分类高亮展示

在搜索功能中，找到对应的事项或批文后可以选择办理或查看办事指南。

（3）智能引导

区域引导通过选择四级联选（市、区县、乡镇街道、社区村屯）快速分类定位批文事项范围。

事项专选，通过对不同事项预先设置的问题与答案，关联事项内容不同的表单字段、材料，做到申请人在选择问题后，申请表单或申请材料对应进行情形缩减，展示当前情形下的所需内容。

（4）常见问题

提供常见问题展示栏目。

（5）智能问答

提供智能问答导办功能。

（6）系统管理

需包括市事项子库标签管理、问题与答案库管理、页面风格管理。

8、一证办

（1）一证办事项梳理

需对各厅局部门进行事项梳理，通过事项子库信息录入，将事项转化为政务服务网能够查询到的事项，经过各项设置后，将事项发布，实现对应事项的线上、线下申报。

（2）个人事项身份证办

- PC 申报端一证办
- APP 端一证办
- 小程序端一证办
- 自助机端一证办
- 大厅受理系统一证办

（3）企业事营业执照办

- PC 申报端一证办
- APP 端一证办
- 小程序端一证办
- 自助机端一证办

➢ 大厅受理系统一证办

（4）一证办标签

通过对事项子库的事项进行一证办标签的新增、修改、删除、筛选，通过对事项进行标记，进行一证办事项查询展示。

（5）一证办智能关联

申报表格数据、材料数据。

（6）一证办基础数据增补

对于一证办中缺少的必填数据，动态化的进行增补。

（7）一证办数据统计统计

提供一证办统计功能，并以图表形式进行可视化展示，提供表格导出能力。

9、免证办

（1）e 冰城“亮证”功能

通过证照信息梳理，分类信息，提供查询接口，使用 e 冰城 app 中亮证功能。

（2）免证办

个人或企业在互联网上申报时通过 app 扫描二维码，进行证照信息获取，上传亮证中的各类证照，实现一机在手，证照自动上传。

个人或企业到大厅办理时，通过 e 冰城 app 人脸识别验证后，出示手机中的证照，受理系统驱动高拍仪进行扫描，自动加载至系统中，实现免证可办事。

10、容缺办

升级市事项子库管理系统，对可容缺办理的事项加注标“容缺办”标签，升级互联网申报、大厅受理及审批流转系统，对可“容缺办”事项，在要件不全时可申报、可受理、可审批，并增加补全环节，在补齐材料后，核发办理结果。内容包括事项子库标注、互联网容缺申报、容缺受理、容缺审批、增补材料、容缺办件统计。

11、无感办

（1）事项子库标注

需要通过事项梳理功能来筛选无感办的事项，提供信息对事项子库中进行字段标注操作，为后续系统提供事项标注，方便在门户上的检索查看。

（2）无感申报

在政务服务门户用户登录后，需要在进行无感办事项在线事项申报时，采取材料带入方式，直接申报提交即可，无需填写任何内容。

（3）办件审批

在办理系统中，部门审批人员查看到无感办事项标识时，可以快速进行审批通过，无需进行材料核验、申请表单字段核验。

（4）无感办统计

需要在无感办统计功能上展示不同类型不同端口下的统计总览，并以图表形式进行可视化展示，同时具备提供表格导出功能。

12、预约延时办

需要在线下大厅设置延时办窗口，通过全市预约系统，提供预约流程，为工作繁忙无法在正常工作时间内到达大厅的申办人员服务。

13、远程验

需要“远程视频验场”模式，省去现场核查工作的往返时限，降低了企业审批成本，提高办事效率，同时也为特殊情况无法面对面验场下满足企业办事需求提供了有效路径。确保特殊情况下行政审批部门工作有序推进，为企业做好全程不见面的线上审批功能。

14、全市办

需要实现全市所有事项在线上、线下均可“全市办”。基于哈尔滨政务服务网网站建设“全市办”专区栏目。公示“全市办”事项清单等功能，同时要求具备全市办相关功能的便民搜索。

（1）全市办事项梳理

梳理“全市办”事项清单，形成“全市办”服务专栏，进行网上便民专区。

（2）事项子库标注

将梳理后的事项在事项子库标注，能在线下附近大厅受理服务查看全市办事项，将事项权限分配区域内政务服务大厅服务中心，提供事项登记服务。

（3）受理系统

需在大厅受理系统增加全市办栏目，为各部门、区县受理系统展示全市办栏目，具备区划综合窗口收件人员查看当前区划及其区划上级的就近办事项，能够进行就近办事项的登记收取。

（4）办理系统

需展示全市办事项标注，部门审批人员进行办件审批，审批通过后将全市办事项收取的申报材料和办件结果返回当前区划的办事大厅，由大厅进行物流邮寄。

15、企业开办直通车（升级）

需在哈尔滨企业开办系统进行优化，新增医疗（生育）保险参保登记业务和水、电、气预约报装办理环节，业务信息办理同步企业开办系统，实现在企业开办的同时进行医疗（生育）保险参保登记和水、电、气业务的预约报装办理。

（1）医疗（生育）保险参保登记

需在原有企业开办环节的基础上延伸服务，增加医疗（生育）保险参保业务。申请人在办理开业登记（设立登记注册）申请时，具备自愿选择“医疗（生育）保险参保业务”服务，用于医疗（生育）保险参保业务。

医保部门在办理业务过程中及时将办理进度信息回传给本平台，便于查询办理进度。

（2）供水

供水内容包括：业务概述、对接方式、信息采集、信息推送、信息反馈、短信通知、结果状态信息共享。

（3）供电

供电内容包括：概述、对接方式、信息采集、信息推送、信息反馈、短信通知、结果状态信息共享。

（4）供气

供气内容包括：概述、对接方式、信息采集、信息推送、信息反馈、短信通知、结果状态信息共享。

16、企业注销直通车

内容包括注销一网通办联办对接说明、业务流程、注销申请、一般注销、简易注销、电子营业执照作废声明、注销进度管理、注销联办对接、业务系统对接。

17、户籍专区

在一体化政务服务特色专区开通“户籍专区”，办理公安户政的各项业务，包括身份证、户口、迁入、迁出、证明开具、档案管理等各项功能。内容包括事

项子库标注、门户专区清单。

18、二手房联动过户升级

需要针对二手房过户手续繁、多次跑等问题，拟会同不动产、水、电、气、热等公共服务企业，联手打造个人二手房水电气热联动过户平台，由主城区升级至九区九县实现二手房过户一站式办理服务。

实现在二手房过户过程中不动产交易申请人将纸质材料拍照或扫描后在互联网上提交，各部门在互联网上核验原始资料，双方进行合同签署，缴纳相关税费，一次性办结，辅助快递邮寄，最终实现不见面过户。

内容包括实名注册、买卖双方授权、申请联办要求、填报信息、窗口办理、进度查询、联办办理范围。

19、支付宝小程序

建设哈尔滨市“e 冰城”支付宝小程序。主要包含市民中心主程序建设、市民中心分程序建设、生活号开发及运维、市民中心管理平台建设。

通过支付宝小程序建设将“市民中心”用户数纳入本地一网通办考核指标。推动更多便民服务接入“市民中心”，能够通过支付宝平台在线办理事项，能够与政务服务网同步用户登录与政务事项办理。能够对外开展新闻宣传、政策解读、政务服务推广。

基于支付宝平台开展联合运营。利用官方发布渠道、支付宝中心化流量运营能力及线下物料布设，共同宣传推广哈尔滨市“e 冰城”品牌，包括但不限于媒体新闻宣传、政务大厅线下摆展 ，不定期进行支付宝端内端外信息及服务宣传，推广，提升服务曝光度。

内容包括首页（支付宝主程序）建设、办事频道建设、支付宝生活频道开发及运维、业务管理平台建设、小程序运营、运维服务、数据备份、上线指导、使用指导、免费修复 BUG、能力支撑。

20、e 冰城升级

哈尔滨市 e 冰城是我市城市综合服务类 app，为满足我市进一步提升便民利企服务，本次进行升级 e 冰城，升级内容包含建设标准规范，项目升级与服务改造，增加运维平台建设，与省级标准对接。内容包括 APP 建设标准规范、项目升级与服务改造、运维平台建设、与省级标准对接。

（二）统一申报平台

需要完成哈尔滨市表单数据割接，包括将哈尔滨全市事项申报表单字段、版本数据割接到省数字政府统一申报平台，并保证割接历史数据内容符合省级割接标准，全量数据割接，具备历史数据查询调阅。

（三）电子监察平台

需要完成哈尔滨市电子监察平台数据割接，包括将哈尔滨全市电子监察数据全部割接到省数字政府电子监察平台，并保证割接历史数据内容符合省级割接标准，全量数据割接，具备历史数据查询调阅。

（四）好差评管理系统

需要完成哈尔滨市好差评系统数据割接，包括将哈尔滨全市办件、人员、窗口、大厅等好差评数据全部割接到省数字政府好差评管理系统，并保证割接历史数据内容符合省级割接标准，全量数据割接，具备历史数据查询调阅。

（五）办件子库

构建哈尔滨全市办件子库，通过省、市政务数据共享交换平台，对接利用省级办件中心统一质检服务能力，实现哈尔滨全市汇聚的市县自建系统的办件信息数据质检、上报。承接所属哈尔滨市的省垂、国垂系统业务办理的办件数据。基于办件子库的数据，可开展多维度、多层次办件数据分析，为政务服务效能决策提供辅助决策依据。

主要实现哈尔滨全市省垂、国垂办件数据承接服务，办件数据共享应用，办件数据综合分析，与省级办件中心对接，对哈尔滨市办件子库汇聚的市县自建系统的办件信息数据进行质检、上报。

内容包括办件数据承接、办件数据查询、办件数据共享应用、综合分析、与政务数据共享交换平台、省级办件中心、政务外网统一身份认证平台、统一工作门户等系统集成。

（六）事项子库

需升级哈尔滨市事项子库，主要实现与省事项管理中心的事项同步、事项对账，统计分析、部门自建业务系统对接，实现政务服务事项推送与应用，保障政务服务事项同源应用。同时可实现对哈尔滨本地特色事项的事项个性化要素修改。

（1）事项标准化管理

应提供事项标准化管理，包括事项数据同步、事项版本变更确认、事项要素维护管理、事项维护管理、镇街村居事项下放、事项标签化管理、事项数据统一下发接口。

1）事项数据同步：以版本迭代的方式存储同步获取下来的政务服务事项数据，记录事项历次版本的版本号、同步时间、变更内容，并在同步新版本数据后自动对相应统计分析数据进行更新。

2）事项版本变更确认：对于从黑龙江省事项库同步获取到的事项新版本，系统将其推送到对应业务主管部门账号进行变更版本确认，确认版本变更之后，系统自动将其替换为当前在用版本，并将在哈尔滨市事项管理系统中维护的内容复制到此版本中。

3）事项要素维护管理：需对哈尔滨市要素信息进行管理，需对哈尔滨市受办理基准要素进行维护，需对哈尔滨市受办理基准状态进行管理，需对哈尔滨市受办理基准内容进行质检。对于要素的管理需满足要素自动存储、要素清单草稿保存、要素清单复用、要素解释和流程图生成。事项关键要素变动需预警，主要包括：预警规则配置、预警事项范围配置、预警检测、预警情况确认、预警处置、预警处理结果核验。事项自定义要素需维护，主要包括：基于全局事项扩展、基于事项类型扩展和基于事项扩展。

4）事项维护管理：对于事项信息的维护，系统需提供政务服务事项的基本目录和实施清单/业务办理项的录入维护功能。事项信息审核需针对哈尔滨市自设政务服务事项，系统提供政务服务事项的基本目录的审核功能，和对所有实施清单/业务办理项的审核功能。事项发布需由事项的业务部门操作完成对事项的统一发布，事项发布后即可通过事项数据统一下发接口下发给下游各应用系统。事项动态管理需提供政务服务事项的基本目录和实施清单/业务办理项的动态管理功能。事项版本管理要求系统需能够自动保存各版本的信息并自动更新版本号，实现事项的全程留痕、可追溯管理。

5）镇街村居事项下放：市级业务部门需能够自主选择需下放、授权、委托的事项基本目录和目标业务部门，填写事权调整的理由、上传依据文档，发起调整申请。县级业务部门需能够在可承接事项模块中查询本业务部门可承接的上级

业务部门下放、授权、委托的事项，并可根据实际业务情况判断是否承接。需将政务服务事项拓展到镇（街）、村（居），优化政务服务事项覆盖，实现全市政务服务事项四级覆盖（市、县（区）、镇（街）、村（居））工作

6）事项标签化管理：需可通过设置模块自定义事项标签，可对事项标签进行分类，需提供标签配置及展示功能，并具备信息的筛选及导出。

7）事项数据统一下发接口：需对接哈尔滨市政务服务平台，由哈尔滨市事项管理系统统一发布政务服务事项数据。

（2）事项质量优化分析

应提供事项质量优化分析功能，包括事项质量监测、横向比对分析、问题分析与发现、制订优化措施、部门实施优化、评估优化效果。

1）事项质量检测：需提供规则的分类维护和质检规则维护。对于自定义质检内容需满足人工选择质检规则、划定质检事项范围，进行单次质检。对于全量数据质检则用于数据上报国家平台之前的数据质量全面检查。对于异常数据需提供对应的异常查看功能。需对常见词和敏感词进行归类建库，并提供词库的维护功能。在对事项进行质检的同时需提供质检结果的通知及公示。

2）横向比对分析：需实现哈尔滨市范围内市级和各区县事项优化程度的横向对比，并以表格形式展示市级和各区县事项的比对要素内容，针对优化情况差异性较大的政务服务事项，政务服务管理部门可直接编辑该事项的优化措施建议。

3）问题分析与发现：需提供给政务服务管理部门能够将发现的每一项问题将其记录到系统之中的能力，系统将问题关联到相应的政务服务事项上，政务服务管理部门发起事项优化建议流程时，系统自动将之前关联的问题带入到流程中，待相关业务部门整改完成之后，政务服务管理部门可以确认问题是否已解决。

4）制定优化措施：需能够帮助政务服务管理部门针对分析得出的政务服务事项问题和优化方向制订优化措施，在事项优化建议流程中提交事项实施部门进行确认和优化。

5）部门实施优化：哈尔滨市业务部门需要能够在在系统中收到政务服务管理部门提供的事项优化建议，并查看对应的政务服务事项信息、存在问题清单以及事项优化建议信息，系统具备导出以上信息为本地文件，便于业务部门进行线

下研讨、汇总文件资料。

6）评估优化结果：政务服务管理部门需能够借助系统对各阶段的事项优化工作评估优化效果。

（3）事项统计分析

应提供事项统计分析功能，包括事项自定义查询、服务指南和业务手册导出、事项固定模板统计、事项关键指标提升历程。

1）事项自定义查询：需提供政务服务事项自定义查询功能，实现对政务服务事项基本目录、实施清单、业务办理项的自定义条件查询和清单表格导出。

2）服务指南和业务手册导出：需提供政务服务事项的服务指南和业务手册导出功能，便于哈尔滨市政务服务管理部门以及各级业务部门快速完成服务指南、业务手册相关格式化文书的编写。

3）事项固定模板统计：需能够针对哈尔滨市事项管理工作中某些特定的统计场景，固化成为固定模板的统计。

4）事项关键指标提升历程：需记录哈尔滨市政务服务事项的版本迭代情况，对各事项关键指标的提升历程进行留痕。

（4）组织架构管理

应提供组织架构管理功能，管理组织单位信息，具备新增/删除/修改操作，允许设置组织管理员，各级管理员能管理自己的组织、用户和资源，上级管理员能管理下级的组织、用户和资源，可按照组织查看用户。

主要功能需包括部门管理、单位管理员、组织架构分级管理。

需具备管理全局组织单位信息，可添加各个下属部门到顶级部门下，作为一级子部门，系统还需要具备创建一个单位管理员角色。同时将各单位内的某些人员设置为单位管理员，这些单位管理员进入系统后，有权访问部门维护管理模块。并在该模块维护部门基础数据，要对用户、部门、角色、用户角色关系、模块和模块权限来进行管理。

（5）权限管理

应提供权限管理功能，包括准入授权管理、角色授权管理、细粒度授权管理、多级授权管理功能。

1）准入授权管理：在系统中能够创建或者维护的用户，拥有自己能够访问

的应用列表。

2）角色授权管理：需具备为不同应用配置不同的角色，并将应用角色指派给用户。

3）细粒度授权管理：对菜单、url 连接、用户添加页面、用户信息、类方法、页面中按钮来进行权限管理。

4）多级授权管理：需具备按照用户、组织、应用三个维度进行组合，进行分权、分域的管理员权限控制。

（七）受理中心对接

需按照黑龙江省数字政府建设要求及标准，哈尔滨市一体化政务服务平台受理中心与省级政务服务平台对接，互联互通。

内容包括对接省级收件中心、对接省级表单中心、对接省级流程配置中心、对接省级材料中心、对接省级事项管理中心、对接省级统一政务服务工作台、对接统一身份认证、对接智慧政务大厅排队叫号系统、对接省级好差评系统、对接省级电子监察系统、对接统一电子印证、对接省级统一短信网关、对接省级个企档案。

（八）办理中心对接

按照黑龙江省数字政府建设要求及标准，哈尔滨市一体化政务服务平台办理中心与省级政务服务平台对接，互联互通。

内容包括对接省级收件心、对接省级表单中心、对接省级流程配置中心、对接省级材料中心、对接省级事项管理中心、对接省级统一政务服务工作台、对接统一身份认证、对接省级好差评系统、对接电子证照系统、对接电子监察系统、对接统一电子印章、对接省级统一短信网关、对接省级个企档案。

（九）事项精细化梳理

开展市本级、区（县）、乡镇（街道）、社区（村屯）精细化事项梳理工作，需要将梳理结果录入事项库。并对创新应用中涉及事项方面内容进行录入。内容包括开展事项标准化梳理实施工作、事项梳理实施步骤、事项标准化梳理相关要求、事项精细化梳理内容。

（十）一件事一次办

需要按照地市需要建设一件事清单，按照省级一件事标准完成地市一件事接

入能力配置实施办事指南、政策法规、一张表单等。需要按照省里能力接口标准，完成一件事能力开发平台上架与收件接口和结果反馈相关能力开发。 按照我市自有一件事清单，系统需完成自有一件事集成对接。完成与省级统一赋码接口对接，省级一件事结果接口回传，并应用于哈尔滨大厅、窗口一件事服务能力。

（四）智慧政务大厅管理系统

具体技术（参数）要求
智慧政务大厅管理系统 现有智慧政务大厅管理系统能力如下：推进“一网”式政务服务，大厅设备包含呼叫器、手写板（评价器）、一体化高拍仪（身份证读卡器、指纹验证、双屏显示、高拍仪）等，所有业务可通过PC端、手机端、大厅端全程留痕、进度查询、短信提醒、监督监办，在预约、导办、受理、流转、审批、出件、可视化数据分析等流程，建设功能全覆盖、数据全口径对接的信息化平台，实现“数据多跑路，群众少跑腿”。 本期建设智慧政务大厅管理系统，接入市本级和九区九县政服务服大厅的排队叫号系统、高拍仪、摄像头、评价器等软硬件设备信息，根据实际情况升级改造和适配，与省级政务大厅智慧管理平台对接。持续推进政务服务智慧化大厅标准化、规范化建设，大幅提升政务服务智慧化水平，提高政务服务效能。 1、中心综合管理系统 需要建设中心综合管理系统，满足大厅日常人员、窗口、部门的管理的需求，能够进行。 （1） 日常考勤功能：需要包括员工考勤管理、请假管理。 （2） 绩效管理功能：考勤规则配置、窗口、部门、办件考核。 2、智能排队叫号系统 需要建设智能排队叫号系统，具备刷卡快速打印号票，显示办理事项、排队人数等信息，具备窗口软件叫号集成功能，具备取号机缺纸自动预警功能。 （1） 需要具备实时监管系统运行情况，自动跟踪各个服务队列并做自动调整。

（2） 需要具备群众多渠道预约、刷身份证取号；可以自行维护号票展示内容；预约数量限制功能。

（3） 需要提供窗口坐席呼叫程序，具备多种叫号渠道；提供报表查询统计功能，包括办事人服务情况、办事人流量情况、业务办理评价情况、员工工作情况；具备排队管理，对部门、业务、窗口、叫号配额进行系统管理；

3、建设在线帮办系统

需要提供帮办业务系统，实现事项办理、满意度评价的全程帮办服务。

（1） 需要提供客服人员工作台，展示常用功能，提升工作效率

（2） 需要给窗口提供帮办代办登记能力，帮忙申请方实现帮办代办信息填写。

（3） 需要具备多种帮办代办能力，包括在线沟通帮办能力，线下回访帮办能力，视频沟通导办能力。

（4） 需要提供问题收集解答汇总库，方便客服人员通过问题库进行快速查询疑难问题，并给出解答。

（5） 需要具备帮办代办满意度回访。

（6） 需要具备帮办代办各维度数据统计。

4、建设一码通办服务系统

需要建立一码通办服务事项进驻大厅服务系统，通过一码通办服务事项特质与一码通办标签进行线下大厅主题式服务。

（1） 扫码登录。需要具备用户在线下一码通办服务窗口办事，通过一码通办窗口扫码登录，替代身份证读取登录。

（2） 扫码收件。由原来线下窗口收取纸质证照和档案信息拓展为窗口人员扫码获取本人（企业）电子证照，实现实物证照免提交。

（3） 多材料扫码亮证。需实现由扫多个码向扫一个码转变，通过用户关系扫码，实现与事项多个材料绑定，从而实现一次扫码一码获取该事项所有具备减少要件亮证材料。

（4） 码上通评。需实现一码通评，扫码获取评价指标信息完成对大厅、窗口、人员、办件、办事指南等评价服务。

（5） 码上核查。通过申请人主动亮出的材料码，完成线下窗口设备扫码获

取核查材料，减少部门对纸质材料证件材料依赖性。

（6） 码上征信。需要通过一码与信用平台结合，归集企业或个人授权的各类数据，实现码上征信。

5、四级联办系统

需要通办窗口人员通过大厅服务系统，异地受理市、区（县）、乡镇（街道）、社区（村屯）联办事项，实现异地受理，办件结果回寄的服务。

需要系统增加四级联办功能模块，显示区划、部门、事项名称、办事指南、在线申报等功能按钮，完成电子材料流转，纸质材料通过 EMS 免费邮寄。

6、全市统一预约模式对接

需要实现一口预约管理，通过技术对接整合实现大厅综合窗口、专厅业务的整合统一，通过标准统一、技术统一、管理统一等方式建设一套大厅服务标准模式。

我市存在部分专窗业务系统需要通过系统对外提供的统一接入标准配合专厅设备利旧改造升级实现大厅预约、叫号、取号、收件的统一分发模式。

需要全部服务大厅接入预约叫号系统，包括市、区县政务大厅和专厅。

7、窗口服务设备升级

各大厅设立的帮办窗口，各区县大厅在设立帮办窗口需自行配备无线耳机、无线麦克、摄像头等专业服务设备。

参数需满足：

耳麦，2 套：

（1）2.4G 蓝牙双模无线头戴式耳麦；

（2）40mm 驱动单元高音强劲、低音有力；

（3）待机 40 小时以上；分为标准蓝牙、极速蓝牙模式；

（4）连接方式：蓝牙 5.2、极速蓝牙 2.4G；

（5）蓝牙协议：A2DP\AVRCP\HFP\HSP；

（6）有效距离 约 10 米左右；

（7）阻抗：32Ω；

（8）包装产品：耳机、麦克风、充电线、多功能适配器等。

摄像头，2 套：

（1）摄像头直播视频会议摄像头 1080P；最大分辨率1080p/30fps-720p/60fps；

（2）视频客户端支持多种操作系统，如：macOS10、Android 5.0 以及上更高版本，免驱；

（3）对焦类型：具备自动对焦；

（4）内置麦克风：立体声；

（5）视野：78°；

（6）平台兼容性：具备市场主流视频会议平台；

（7）USB 线长度，不低于 1.5m。

移动终端，1 台：

（1）屏幕尺寸不小于 10 英寸；

（2）分辨率不低于 2560*1600；

（3）连接方式 ：具备 WIFI、蓝牙；

（4）存储空间：内存不低于 8G；储存不低于 128G;

（5）电池容量不低于 7000mAH；

（6）摄像头：前置不低于 800W 像素，后置不低于 1300W 像素；

（7）主要功能：具备分屏；重力感应；GPS 导航；陀螺仪；AI 语音；多点触控等。

（8）操作系统：安卓或 IOS。

8、设立远程视频咨询帮办专区

需要建立远程视频咨询帮办专区收件登记功能。

9、建设企业一站式服务专区

需要设立企业一站式服务专区，含收件登记、咨询记录、跨层级审批、政策解读记录等功能。

10、建设人才服务专区

（1）打造“一体化”人才服务专区。以市民大厦为载体，市级综合窗口为依托，拓展建设人才服务专区。

（2）核管理人才政策进驻专区。按照《人才新政 30 条》依据职能组织梳理人才政策实施细则和人才类政务服务事项。

（3）提供“一站式”综合服务。按照“前台综合受理、后台分类审批、综合窗口处件”模式，将人才服务业务统一纳入人才服务专区（专窗）综合受理，实现全流程“一站式”服务。

11、建设咨询服务专区

需要在大厅设立咨询服务专区，为需办事人提供本部门复杂事项审批相关、政务政策文件解读等专业服务功能专区及咨询记录等。

12、建设大厅智能导引服务

需要通过结合我市大厅布局、扫码导引、打点定位，完成大厅智能导引服务，通过扫码后唤起的页面获取当前定位位置，播放预制宣传内容与导引服务。

13、评价系统

根据大厅需求，窗口配置桌面评价交互系统，需实现如下功能：

（1）显示窗口受理人员部门、工号、姓名、座右铭等宣传内容；

（2）申请人身份证读取功能并对接政务服务网实现身份信息自动录入，加快办理速度；

（3）申请人活体识别功能并对接政务服务网实现“活体认证、人证合一”，解决本人到场鉴别；

（4）申请材料高拍功能并对接政务服务网实现申请材料的快速拍照上传系统，加快办理速度；

（5）对受理通知书、接收告知单等单据的扫码功能，实现扫码查件，快速定位，加快办理速度；

（6）办理过程中实现需要确认的关键要件双屏推送与信息确认功能；

（7）办理后的评价功能，对接政务服务网实现国家“好差评”标准评价；

（8）评价鉴别功能，通过摄像头捕捉评价瞬间照片，鉴别是否申请人自行评价；

（9）对接叫号器实现从叫号起到评价结束的全过程录音录像，一旦出现差评办理过程视频全部上传政务服务网，跟踪差评原因。

14、短信应用系统

需要通过与运营商短信网关的对接与整合，实现手机短信的发送。短信在系统中主要应用如下：系统自动短信提醒（邮件短信）、排队叫号短信、中心短信

群发、通知申请人取件、短信满意度调查等。

15、窗口呼叫终端系统

需要放置在窗口工作人员工作台上，具备提供窗口叫号、评价发起等功能。

（1） 窗口叫号：与智能排队叫号系统对接，窗口工作人员登录窗口叫号平板后，即可获取当前窗口信息、窗口工作人员信息、排队信息，窗口工作人员可进行“呼叫”、“重呼”、“读卡”、“作废”等操作。

（2） 评价发起：每次服务完成后，窗口工作人员即可进行发起评价操作，办事群众可进行满意度评价操作。

16、物料流转系统

需要具备服务大厅内容，办件材料的流转监管。大厅受理过程中，由综合窗口接收的原件材料，需要流转至审批部门，审批部门审定后，特料需流转回综合窗口，为严格管理相关过程，避免出现申报人材料丢失等问题，需配备 PAD 等设备并开发管理系统，实现物料流转功能。

（1）待出件：需要展示当前大厅已办结但未将结果物给申请方的办件信息。

（2）已出件：需要展示从大厅已经出件的办件信息。

（3）待流转（发起物流）：需要展示已经发起物料流转的办件信息。

（4）待签收（接收物流）：需要展示已经在流转中的办件信息。

（5）待出件（窗口出件）：需要展示当前从流转到窗口的办件信息。

（6）物料流转查询：需要提供进行物料流转的办件信息查询的功能。

17、后台管理系统

系统管理主要供系统管理员使用，是系统的控制中心。主要实现对整个综合管理系统的功能模块、权限、角色、事项、日志、工作流、进行新增、修改、删除、查询等功能。

需要包括大厅管理、大厅入驻部门信息、入驻大厅人员信息、模块管理、权限管理、系统日志管理、业务配置管理、工作流配置管理、统一设备管理、统一排队管理、统一预约管理、统一信息发布管理、大厅资产管理。

18、市级智慧大厅与各区县对接

需要市级与各区县智慧大厅对接，内容包括但不限于排队取号能力对接、排队叫号能力对接、受理能力对接、窗口评价能力对接、统一预约对接、统一设备

管理对接、智能查询能力对接、大厅综合管理对接、能力对接基本功能、设备数据对接、统一身份认证接口对接、视频监控系统对接。

19、大厅对接服务能力

需要建设统一标准服务接口，完成市、区县综合政务大厅、专厅的预约、叫号、取号、收件、流转的统一服务能力，打通各级大厅服务能力。内容包括获取预约信息能力、取号成功回调能力、叫号成功回调能力、获取部门信息能力、获取事项与窗口分组信息能力、获取时段余号查询能力、收件与预约信息绑定状态回调能力。

20、与省级智慧大厅对接

需与省级智慧大厅对接，内容包括上报设备清单、上报设备在线状态、上报故障信息报送、上报排队业务信息、上报排队取号数据、上报叫号数据、上报办结数据、上报窗口基本信息、上报窗口状态、上报预约部门信息、上报预约事项、上报预约记录、上报预约取消、上报预约改约、上报预约已取号、上报预约已呼叫、上报预约已办结、上报大厅入驻部门信息、上报入驻大厅人员信息、上报考勤结果、上报绩效结果、上报月度人员考评结果、上报月度部门考评、上报评优结果、上报月度服务之星、上报月度红旗窗口、上报党员先锋岗、上报大厅资产台账、上报资产变更信息、统一身份认证接口对接。

21、政务服务自助终端业务升级

在为部分市本级与区县大厅、乡镇街道、社区村屯配备政务服务自助终端，实现政务服务 24 小时不打烊，市民可以就近进行便利的自助服务。汇聚政府、事业单位、国企等公有性质的部门单位提供的信息来源，通过整合、接入各类服务，按类型、按地域集中为公众提供查看、查询、办事、互动等服务，部署在各级行政区域的行政服务中心、街道、社区，也可以部署商场、车站、办公楼等公众密集区域，实现政务服务 24 小时不打烊，市民可以就近进行便利的自助服务。通过自助终端，在政府与社会之间、政府与公众之间，建立起交流互动、信息共享以及政务办事的渠道，改善政府的公共服务，提高政府的服务质量和行政效率。内容包括开展自助办理的业务、政务服务自助终端软件前端功能、区县自助终端适配改造。

（1）开展自助办理业务

系统需包含申请办理政务服务事项、生活缴费、行政处罚缴费、充值、查询公积金、不动产、医疗险、养老失业等保险、办件进度；打印审批公文、各类证照、信用档案、征信证明、社区街道开县的各类证明等，预约医院挂号、大厅办事预约等，大厅取号排队、考勤打卡、宣传展示，身份识别，自动审批等特色服务。 （2）政务服务自助终端软件前端功能 政务服务自助终端以智慧政务为核心，为相对人提供一站式电子政务服务，窗口工作人员日常的办事服务，一体机同样能够办理，申报者无需排队等候，可以自助处理，包括办事指南打印、预约履约、排队取号、在线申报、办件查询、补件、取件、评议、证照查看复用、材料机读扫描等服务。 系统需具备社区办事，利用大数据理念，对本机办理最多的事项进行排序，将频次最高的前若干项放在高频事项中，方便办事人员快速选择，高效办理。必须具备公积金业务、涉税业务办理，生活缴费和电子证明开具等功能。 （3）区县自助终端适配改造 系统需具备区县自助终端需按照市级自助终端新增的办理业务及前端功能进行同步适配改造，其中包括缴费、查询、打印、预约、大厅服务、特色服务等自助办理的业务。开具证明、公积金、涉税业务、生活缴费、终端后台管理等前端功能。保持区县自助终端与市级自助终端业务内容及功能一致。需实现自助机基础信息同步、自助机实时状态同步、助机硬件模块状态同步、自助机终端资源预警同步、自助终端业务办理量同步、自助机事项开发等功能。

（五）网格化管理平台

具体技术（参数）要求
网格化管理平台 建设网格化信息管理平台。建设市级基层网格信息化平台，包括网格管理、协同联动、综合评价、“一标三实”和基层党建系统，基本实现网格化管理服务网络化、信息化，集成连接千个社区的 3 万个网格，实现“一网多格、一格多能、一岗多责”。接入城管、市场监督、卫生健康、应急管理等业务，实现多网融合。梳理网格服务事项清单，向省级平台归集网格和网格员数据。

（一）支撑平台与服务

1、 业务平台

业务平台需要具备共性技术能力和统一应用组件的提炼封装和共建共享，平台需要具备实现业务融合，行业赋能，以简化集成开发为目标，构建网格化应用提供开发集成平台，需要具备加速行业应用上线。业务中台由开发设计中心、业务组件仓库、监控运维中心和基础业务服务等模块构成。

2、物联网平台

物联网平台需要具备对基础设施、市政设施、能源设施、城市运营管理设施等全场景物联设备的接入和应用，需要具备将政府数据、能源数据和社会数据进行采集汇聚，为网格化协调指挥中枢提供海量数据资源。核心功能包括设备监控、远程操控、对外接口开放服务等。系统需要具备直观详细的设备展示功能与统计分析功能，需要具备实时展示接入的各类设备位置、状态、数据信息。

3、视频融合平台

视频融合平台需要具备对网格化相关视频监控资源进行统一接入，统一调度，统一运营，核心功能包括：摄像设备的管理、视频接入网关、视频服务器管理、视频接入配置、存储管理服务、视频搜索、视频播放、平台运维等。

4、基础服务

基础服务需要具备平台级中间服务组件，包含工作流引擎、网关微服务、多媒体应用服务、消息群发服务、高性能查询检索服务、流媒体转发服务，用于支撑业务平台相关的设计与封装工作。

（二）党建引领平台

1、党群服务中心子系统

（1）党群服务中心管理

系统需要具备在哈尔滨市民政局牵头绘制的“哈尔滨市基础地理信息共享与服务系统”的网格地图上对各级党群服务中心进行标注，维护运营开放时间、实景照片、服务标签等基本信息。

（2）服务管理

系统需要提供对于党群服务中心的教育培训、谈心谈话、宣传讲解等服务进行维护更新，党员、群众可以根据需要进行预约，参与完成后进行服务评价。

（3）活动管理

党群服务中心需要提供至少两种类型的活动服务，一种是由各中心级组织的主题活动，另外一种是由社团或群众自发组织的活动。需要通过发布相关活动后根据需要进行预约，参与完成后群众、中心可进行双向评价。

（4）场地管理

系统需要提供服务场所基本信息的维护，包含场景照片、预约须知、开放时间及容纳人数等，社团或个人可在系统中查询预约。

（5）社团管理

系统需要提供各种社团基本信息的维护，包含社团名称、简介、负责人及成员，群众可搜索申请加入各社团。

（6）积分与评价

系统需要提供积分与评价功能，通过参与的各种活动或服务，需要提供双向评价。社团或群众可以通过签到、参加活动等途径获得积分，积分可在中心进行奖励兑换，以此鼓励群众参与到党群服务活动中。

2、党员党组织信息建设子系统

系统需要提供党组织建设功能，完成党组织结构框架，完善党员及党组织基本信息（如党组织名称、党组织简称及党员名称、性别、照片等可公开的信息），并且需要通过权限进行管理。

3、党员进网格子系统

系统需要提供党员与网格、社区的绑定功能，网格中党员可参与志愿者活动，并需要根据党员在网格中参与的基层工作对其进行评价考核，实现党员进网格，引领基层治理的理念。

4、党政宣传子系统

系统需要提供通过文字、图片、视频等内容对党政宣传数据进行编辑与发布，并可根据具体党政情况自定义排序进行多种方式的分享，同时需要提供评论互动、标题搜索等功能，可在移动端查看党建宣传信息。

5、志愿者活动子系统

需要具备党员和群众申请为志愿者，针对活动、群众困难、专项行动等特殊事件，志愿者可进行报名，对于特殊活动也可自动推送给志愿者、党员。志愿者

参与活动时可进行定位、记录信息，系统应具备活动情况统计和分析。

6、统计分析子系统

（1）在职党员排名

需要具备在职党员排名，根据党员参与活动情况，需要提供活动数据统计分析；可以查看所有在职党员完成志愿者服务的数量、好评数量、好评率等信息，并进行排名。

（2）志愿者服务统计

系统需要具备根据志愿者参与活动的情况，提供活动数据统计分析，对志愿者服务的整体信息包括共建单位、志愿者小组、党员进行多维度的统计。

（3）党组织数据分析

系统需要从网格的维度出发，提供网格内的党员、党组织的相应数据分析。统计党员在网格参加活动的完成情况，同时根据数据进行分析、排名等。

（三）协调指挥平台

1、事件处置子系统

（1）事件受理

系统需要具备接收由网格员上报、12345 热线登记、“e 冰城”APP、“e 冰城”微信小程序、“e 冰城”支付宝小程序、摄像头识别及领导交办的事件，需要提供通过系统内自设的工作流引擎将案件流转下去，达到网格精细化治理的目的。在系统受理中需要查看事件详情、附件信息，并且在上报时需要自动识别语音文字，根据事件上报的文字提取关键字，进行识别并给出推荐分类，实现事件与数据的汇总。

（2）任务分派

系统需要具备指挥中心受理员通过系统将事件派单到相应的专业部门，需要具备回退、向上级派转、向各级别职能部门流转的功能，直到事件能够得到妥善处置。并且系统根据事件情况需要具备人工派单，根据事件类型和严重程度需要提供自动派单。根据事件发生地址，匹配相应的网格，需要提供自动发送核实任务给网格员进行核实。对于职能部门处置完毕的事件，系统根据情况发送核查任务给网格员，由网格员去现场勘查处置。为实现自动派单功能，系统需要提供事前需设置好自动派单规则，规则需包括流转对象设置、自动派单时限，自动派单

时间类型。系统需要对事件处置过程留痕，可查看事件办理进度。12345 受理员通过平台登记事件，需具备事件流转至相应的网格并继续执行接下来的流程。需要提供与 12345 呼叫中心系统对接，需能够实现自动上报和派单。

（3）事件办理

系统需要提供派单后各相关部门对事件进行办理操作，需要提供事件处置、回退、申请结案、延期等操作。同时需要具备事件定位、办结、反馈、回退、超时提醒等功能。

（4）延期管理

某些棘手的事件，系统需要具备申请延期办理的功能。申请时须填写延办理由、延长时间等信息，需要提供领导审核功能，并确保领导审核后才可进行延期。

（5）预警管理

对于事件处理不及时的，系统需要进行预警，且此事件完成处置后变为超时件，领导端收到超时事件信息进行督办。

（6）督办管理

事项分类里需具备落实各事项处置时限，根据处置超时情况，系统需要自动派发给领导，领导可选择需督办事件派单给相应的部门去进行处置。达到监督催促的目的。

（7）地图操作

地图需要提供放大、缩小、移动、二维、图层叠加、扎点等功能，实现网格定位、事件上报功能。

2、指挥决策子系统

（1）调度指挥

系统需要具备语音、视频、图像、数据、文本消息等各种信息媒体的交互，满足指挥中心实时了解事件发生进展情况和应急处置状况传递给相关人员，通过视频指挥、多人会议完成视频连线、会议沟通等功能。

（2）视频融合

视频融合系统需具备视频监控系统接入，同时需要结合地理信息系统，在网格化管理中心的大屏幕上显示，实现对事件的全方位、全时段的可视化监控管理，从而事件作出准确判断并及时响应。

（3）消息群发

根据对网格员、部门和各下属指挥中心的权限控制，系统需要具备对个人、部门和整个下辖指挥中心进行单个或群发系统消息，需具备针对政策、处置意见、调度分析、指挥决策等信息以消息的形式进行发送和管理。

3、事件维护子系统

（1）事件上报

系统需要具备所有处在事件受理环节的事件，可以通过事件上报功能进行处理，同时系统需要提供查看事件详情、受理派发等功能。

（2）网格员上报

所有巡查上报的事件，系统需要具备在网格员上报中显示。可查看事件详情，对事件进行受理派发。

（3）视频上报

系统需要具备在视频上报列表中显示视频类上报事件。且需要提供对事件进行受理派发。

（4）核实事件

在已经派发核实，且未核实状态下，系统需要具备查看事件详情，但不可对事件进行操作，网格员核实后，可对此条事件进行处理和事件流转操作。

（5）经办事件

需要提供所有本账号发起或者经办过的事件，在经办事件中展示。经办事件只能查看不可操作。方便处理人员查看自己办理过的案子。

（6）作废事件

系统具备对有作废权限的角色，查看自己账号作废的事件。

（7）待核查事件

职能部门事件处理完成后，系统需具备在待核查事件中统计职能部门处理完成的且未核查的事件。并且需要具备核查操作。

（8）核查事件

已经核查完成的事件需要在核查事件中进行查看，同时处置结果与处置过程没有问题的事件，系统需要具备办结操作。

（9）群众上报事件

辖区下群众随手拍上报的事件，在网格员审核通过后，系统需要具备在群众上报事件中进行展示，并且需要具备根据权限显示辖区下的事件列表。

（10）问题上报事件

在网格员进行巡查的过程中，系统需要具备问题上报，并自动派发给对应的指挥中心，问题上报后，系统需要具备在问题上报模块进行统计所有网格员问题上报的事件，并根据权限显示辖区下的事件列表，同时系统需要具备事件情况进行处理和派发。

（11）自处置事件

对于网格员可以自行解决的问题，系统需要具备自处置功能，并且系统需要具备在自处置事件中进行查看。

（12）12345 上报

所有 12345 派单的事件系统均需单独进行统计和查询，并根据上报情况对事件进行核实检查或派发给职能部门进行处理。在 12345 事件上报模块需要提供展示事件的详情及操作功能。

（13）其他事件

统计除了自处置、问题上报、群众上报、视频上报、12345 上报以外，系统需要提供所有指挥中心上报的其他事件展示界面。

（14）待办事件

系统中所有关于事件处置环节中的账号均需提供待办事件功能，并通过待办事件进行查看和操作。

（15）当前超时件

对于当前节点超时的事件，系统需要提供当前超时功能模块进行展示提醒。

（16）历史超时件

对于历史超时过的事件，系统需要提供历史超时件功能模块进行展示提醒。

（17）缓办事件

对于处置过程中申请缓办的事件，系统需提供缓办事件清单，并可针对不同情况做出不同的操作。

（18）已缓办事件

系统需要针对本部门所有已经缓办事件提供已缓办清单，并且需要提供已缓

办事件解除功能。

（19）回退事件

在处置阶段，对于不属于职能部门的事件且申请了回退的事件，系统需要提供回退事件清单，指挥中心可查看回退原因，并需要对该事件进行重新派发。

（20）督办事件

系统需要对职能部门已超时的事件进行显示且展示督办清单，在督办清单的事件需提供领导督办功能。

（21）已督办事件

已被督办的且已处置的事件需要系统在已督办功能中展示。系统需提供已督办事件的列表项。

（22）核查事件

系统需要提供在核查阶段的事件列表功能，需要提供在核查事件中进行查看，指挥中心人员可根据事件情况进行核查、派发。

（23）我办结事件

系统需提供统计我办结的事件功能，并且需要提供查看事件的详情、办理的流程、各节点的处置情况及办理意见。

（24）答复授权

对于申请缓办、申请作废、申请回退、申请办结等功能，系统应提供答复授权功能，答复授权后职能部门人员可根据答复内容进行处置或其他办理。

（25）急要件

在受理过程中，如果是紧急事件，系统需要提供标记为急要件的功能，被标记为急要件事件需要在“急要事件”中查看并且可以进行办理。

（26）岗位事件

系统需提供岗位事件功能，需要具备查看岗位处理的事件信息。

（27）辖区事件

系统需提供辖区事件功能，让各级指挥中心根据账号权限显示辖区下的所有事件信息。并且需要具备查看事件办理的过程、办理人员、办理意见、特殊状况、多媒体信息等数据。

（28）部门事件

系统需根据账号权限查看本部门下的所有事件。所有部门内账号上报的、经过此部门的事件都需要在部门事件中查阅。同时需要提供查看事件办理的过程、办理人员、办理意见、特殊状况、多媒体信息等数据。

（四）专项行动平台

1、模板制作子系统

系统需要提供模板的制作功能，需要满足用户根据不同的行动，设计不同的表单，可对模板内容进行自定义的管理。需提供手动维护或 excel 模板导入，完成模板制作。

2、任务发布子系统

系统需要根据任务情况进行任务设计，设计过程中可选择已添加的模板导入，导入后需具备在此模板中增加任务信息，任务新建后可进行发布，发布对象可接收任务信息。

3、任务接收子系统

系统需要根据任务发布中设置的人员权限分配给各级人员的移动端系统。并且需要以通知的形式进行提醒。

4、任务处置子系统

系统需要根据任务发布中设置的人员权限分配给各级人员的移动端系统。并且需要以通知的形式进行提醒。

5、任务统计子系统

系统需要有任务统计功能，将专项行动处理的结果进行汇总统计出对应的统计报表。

（五）社会治理平台

1、人口管理子系统

（1）实有人口服务管理

实有人口管理子系统需提供四大类人口数据的管理：户籍人口、流动人口、留守人口和境外人口。同时实有人口应包含对信息新增、修改、删除功能，通过输入查询条件或关键字进行多维度搜索，需具备通过 Excel 模板进行批量导入/导出功能等。同时需要具备由网格管理员对数据进行更新，并且对于每户需具备显示网格员的走访记录和日志。具备家庭成员关系展示功能，需具备显示不少于

四代家庭成员关系。

（2）特殊人群服务管理

系统需具备特殊人群标签化配置，同时具备根据各管辖职责对特殊人群的数据进行配置，实现不同角色查看不同的特殊人群的信息。特殊人群标签包括刑满释放人员、社区矫正人员、精神障碍人员、吸毒人员、重点青少年、临时管控重点人等人员。

（3）人员检索

系统需要具备对人员信息进行检索包括但不限于姓名、身份证号码、性别、民族、曾用名、出生日期、籍贯、婚姻状况、政治面貌、学历、宗教信仰、职业、服务所处、联系方式（座机、手机）、住址、人户一致标识、与他人关系等信息。

（4）人房关联

系统需要提供人员与房屋关联功能，在系统内通过人员找到所在或所属房产信息，也可通过模拟仿真楼栋图，去查找某一个房产下所有人员的信息，人员包括：租户、房主等。

（5）隐私数据加密存储传输

系统应可以基于 AES 加密标准将涉及个人隐私的数据内容进行安全加密存储和传输。前端数据在提交给后台时，使用密钥进行加密操作，传输时使用加密后的数据。后端通过对应的密钥进行数据解密，进行数据操作。前端请求数据时，后端需具备首先将结果数据使用密钥进行加密，传输时使用加密后的数据。前端通过对应的密钥进行数据解密，进行数据展示。

2、房屋管理子系统

（1）实有楼栋管理

系统需要具备楼栋管理，具备通过地图扎点将小区内的楼房按栋进行管理，包括楼房信息的增、删、改、查等功能。

（2）实有房屋管理

系统需要提供实有房屋管理功能，通过对地图上已采集的楼栋基本信息的采集登记。需要包括房屋信息的查看、编辑、新增和删除等功能。

（3）房屋租赁

系统需提供房屋租赁模块，具备对租户进行信息登记。

（4）楼栋房屋可视化

系统需提供楼栋房屋可视化分析功能，进行楼栋人员的关联及查询展示、同时系统需要按户对特殊人员进行标签化管理和查询。

3、单位组织管理子系统

（1）实有单位管理

系统需要具备对实有单位的增、删、改、查功能，实现对企业信息的动态管理。

（2）综治组织及综合业务

系统需要具备动态掌握各级综治组织和队伍建设情况，系统需要提供包括综治机构、综治队伍、群防群治组织、群防群治队伍、综治中心、综治视联网信息中心、公共安全视频监控、综治领导责任制、重特大案（事）件等组织业务的日常维护功能。

（3）组织管理

系统需具备对殡葬机构、养老院、福利机构、救助站、优抚单位、儿童福利院等组织的信息化管理和数据的动态更新。

4、民生服务子系统

（1）民情日志

系统需要针对网格内工作人员日常工作中，对重点人群、单位、场所等进行走访记录。

（2）民情日志统计

系统需根据民情日志走访情况对重点人员走访量、重点场所排查量等进行分类统计，并实现网格间各类工作量的统计。

5、隐患排查子系统

（1）护路护线管理

系统需要对护路护线类数据进行汇集、数据管理。

（2）校园及周边安全管理

系统需提供校园及周边安全管理数据汇集、管理。

6、公众端后台管理系统

（1）用户管理

系统需要汇聚所有高级认证的百姓信息，并且通过消息发布功能发送给所属社区。同时系统需具备百姓注册信息与人口库信息互通。

（2）随手拍管理

系统需提供随手拍查询功能，指挥中心人员可通过随手拍管理查看辖区下百姓所有上报的、网格员审核通过的随手拍信息及当前随手拍处理的结果和办案过程。

（3）房屋确权管理

百姓进行房屋确权认证后，系统需提供查看房屋信息功能，指挥中心通过房屋确权管理查看辖区下网格员审核的房屋信息。包括审核通过和未通过的，需要能够同步更新实有人口和实有房屋库，需能做到人房的绑定关联。

（4）房屋解绑管理

系统需要提供解绑功能和网格员审核功能，系统需提供查看网格员审核的房屋信息。审核通过的需要同步更新人房绑定关系。

（5）网格配置

系统应具备百姓查看当前绑定房屋的民警信息、社区信息、网格员信息。系统需提供对网格内网格员、民警、社区的维护、配置功能。

（六）考核评价平台

1、岗位评价子系统

系统需要对网格员配备情况、上岗情况、信息采集质量、数量，核实核查效率情况及得分情况进行统计并生成数据报表。同时需要基于岗位的工作内容，按照预先制定的岗位评价指标和评价体系生成评价结果，并进行展示。

2、专业部门评价子系统

系统需要按照固定的周期，对各级责任主体，按照预先制定的部门评价指标和评价体系进行分析、计算、统计并生成评价结果。

3、区域评价子系统

区域评价需要按照固定的周期，对行政区、街道办、社区区域，按照预先制定的区域评价指标和评价体系对历史案件数据进行分析、计算、统计并生成评价结果。可以生成各区域的评价得分折线图。

4、评价配置子系统

系统需要灵活、动态的定义各种考评模型、各指标所占比重,使得系统可以适应不同用户的考核机制，实现个性化考核。系统通过考评模型的选择、配置，通过配置项形成考核标准，制定专业部门、区域、岗位的考核体系。

（七）涉企服务平台

1、企业网格员管理子系统

系统需提供企业网格员管理功能，可为企业添加企业网格员，可对企业信息进行采集、企业诉求进行上报、企业注册进行审核，企业相关政策进行传达。

2、企业信息管理子系统

系统需提供企业基础档案管理功能，企业网格员可对企业信息进行更新维护，企业员工进行添加，企业周边信息进行上报。

3、企业诉求管理子系统

系统需要可以通过企业自行上报、企业网格员上报企业诉求，可以对企业诉求进行管理、派发、处置，完成企业诉求闭环流程，同时企业可通过移动端查看处置情况，并对其进行评价。系统可对企业诉求数据进行分析。

（八）综合查询平台

综合查询平台需要具备人口信息查询子系统、房屋信息查询子系统、事件信息查询子系统、民情日志查询子系统、企业信息查询子系统的功能，借助系统预设的筛选条件，具备对人口、房屋、事件信息、考勤、登录情况、实有单位数据进行查询或全文检索。

人口信息查询子系统：系统应具备通过输入姓名、身份证号，针对辖区内某一个人的基本信息进行查询，并且需要系统对人的信息进行标准化的脱敏处理。查询时应具备添加筛选条件，如性别、年龄分布、地区选择等进行批量人员搜索。

房屋信息查询子系统：系统应具备通过输入详细地址、模糊地址、片区等数据，搜索某一特定地址房屋信息或某一片区域所包含的房屋信息功能。

事件信息查询子系统：系统应具备提供对事件的查询功能，查询已上报至已结案处于不同阶段的事件,并可通过筛选进行联合搜索,筛选条件至少包括区域、时间、事件类型等条件。

民情日志查询子系统：系统应具备提供网格员上报的民情日志查询功能，并可通过网格员、走访详情、走访时间等条件，查询对应的民情日志，并且需提供

查看民情日志的详细信息功能。

企业信息查询子系统：系统应具备通过输入详细地址、名称等关键字，搜索企业或组织信息，并且需具备查看企业详情及涉企的相关事件信息功能。

（九）大数据分析平台

1、大数据分析子系统

系统需要具备匹配指挥中心大屏分辨率，并基于定制中心数据分析界面，整合各类网格数据，将事件、人员与 GIS 地图进行联动，用于实现事件、人口、房屋、组织等数据的分析和统计，需要具备以图形化展示网格化工作的运行结果，其中包括实有人口、楼栋房屋、事件统计与趋势、网格和网格员、走访日志等内容。

（1）网格员分析

系统应具备统计所有专属网格员、专职网格员、专业网格员、兼职网格员在线情况，并且需要实时了解网格员轨迹位移、事件上报信息、人口房屋采集信息，并根据实际情况可与网格员进行视频连线，完成指挥调度工作。

（2）人口分析

系统需要根据人口数据及人房绑定情况，对人口数据进行分析，并且需要在地图上进行人口分布热力分析。

（3）人房统计

系统需要通过人房关联后的数据对人房进行分析，应需要看到一人多房、有房无人、出租房统计等分析数据。

（4）单位组织统计

系统需要实现对单位组织类别、企业性质、经营情况、诉求等数据进行统计分析功能。

（5）事件分析

系统需要根据事件上报和处理的情况在地图上进行今日、本月、本年的热力分析，并根据事件描述的高频词汇，分析其高发事件的高频词，确保能在多个类型下同一人群事件的集中性爆发进行提前的预警。

2、网格一张图子系统

网格一张图系统需要具备基于 GIS 技术，实现全市区一张图展示，需要具备

在地图上集中展示实有楼栋、实有房屋、实有人口、特殊人群、事件处置、实有单位和网格员等数据信息。通过建立网格管理层级，从而实现市、区域、街道、社区和网格五级管理模式，深化管理层次，强化管理层级。

（1）市级网格一张图

市级指挥中心通过网格一张图功能，需要具备查看全市总网格员、人员、房屋、楼栋、事件等总体信息，逐层查看下级区县、街道、社区网格内相关数据。

（2）区县网格一张图

区县级指挥中心需要根据自己区县权限查看辖区下各街道、社区、网格内的人员、房屋、楼栋、网格员、事件等信息。

（3）街道（乡镇）网格一张图

街道（乡镇）指挥中心需要根据自己乡镇权限查看辖区下的各社区、网格内的人员、房屋、楼栋、网格员、事件数据。

（4）社区（村）网格一张图

社区服务站需要具备通过一张图查看自己社区下的人员、房屋、楼栋、网格员、事件等数据。

3、台账报表子系统

需要具备将汇集的数据进行统一的归档分类，生成各业务主题的报表，并提供统一的报表服务，通过 web 表单、图表等方式展现统计的数据以及数据分析的报表，并能够提供数据导出、打印等基本功能。

4、事件统计子系统

系统需要站在市级指挥中心角度，统计全市事件及日志处理情况，需要具备通过图表的形式展示事件分类、事件实时播报、事件响应率、办结率等相关数据。同时根据数据项进行智能的分析。

5、区县事件分析子系统

系统需提供以区县为基础的事件分析功能，用来统计各区县事件上报情况、受理情况及各区县上报事件排名情况。能够通过区县分析直观了解各区县的工作进展和完成质量。

6、职能部门统计分析子系统

系统需要统计职能部门事件办理情况，能够根据各职能部门处置事件的时

效、缓办的数据、延期的数据、督办的数据，对职能部门处置的事件质量进行统计评价，形成部门排名。

（十）基础维护平台

基础维护平台需包含工作流维护子系统、地理编码子系统、基础资源管理子系统、网格员管理子系统、业务应用维护子系统的建设，需要具备通过配置相关用户、角色、权限、区域、网格、组织（部门）、流程等基础数据，业务流程、操作菜单、工作表单、专题图层等功能实现。

（十一）移动端应用

1、网格通

（1）网格员端

系统需要实现网格员通过操作网格员 APP，需要具备信息采集、事件上报、事件核实核查处置、工作日志管理。同时需要具备指挥中心在指挥调度时给网格员发送调度信息，网格员可以查看并回复调度信息。借助手机终端，实现对网格员的视频及定位功能，进行动态指挥网格员的巡查任务和处置突发矛盾纠纷事件。在网格员移动端开启运行时，提醒网格员进行视频通话。并且移动端需提供智能的拍照及语音识别功能，可将多媒体上传至服务器，在事件流转的过程中可随时查看上传的多媒体数据。同时系统可根据语音进行识别转化成文字，随时查看地图信息、位置定位。并且系统需提供网格员企业诉求上报功能及随手拍审核和房屋确权审核等功能。

（2）领导端

领导端需要提供按照不同行政区域、事件分类、事件来源等信息进行事件的统计和排序，并且需要具备查看事件运行情况、网格员轨迹、位置、信息等数据的监察。同时需要提供辖区事件的查询及对事件、人口、房屋、企业等相关数据的统计信息。

（3）职能部门端

职能部门需具备通过移动端对事件派发流转内容，进行现场处置并反馈处置结果，上传结案佐证图片。同时系统需在移动端具备查看超时事件、急要事件、地图浏览及实时接收系统派发的公告消息。并且需要提供对各职能部门所处理的事件，根据事件类型、处置情况进行统计，以图表的形式进行展示。

2、百姓端

百姓移动端应用需要建立百姓微信小程序、支付宝小程序，需要与哈尔滨现有 e 冰城 APP、小程序做统一融合，并且可进行随手拍上报、房屋确权、高级认证、房屋绑定，随时查看所在专属社区、专属网格员、专属民警等联系方式。随时关注上报事件的进度和处理完成情况，并对事件处置情况进行打分评价。同时在党建方面，系统需提供“党群服务中心”查询，让已完成认证的百姓随时查看全区域党群服务中心运营信息，可查询相关活动及预约场所、服务。并且指挥中心针对各负责社区相关信息为百姓发送系统消息，百姓应通过我的消息功能查看其上报的事件进度和本社区通知的消息。同时可在个人中心中进行个人信息的管理。

专属民警查询：系统需提供“专属民警”查询，已完成认证的百姓可查看管辖自己片区民警信息。

专属社区查询：系统需提供“专属社区”查询，已完成认证的百姓随时可查看自己所属社区信息。

专属网格员查询：系统需提供“专属网格员”查询，已完成认证的百姓随时可查看自己所属网格员信息。

党群中心服务：系统需提供“党群服务中心”查询，已完成认证的百姓随时可查看全区域党群服务中心运营信息。

房屋确权：系统需提供百姓自主房屋确权功能，添加房屋后需要网格员审核，审核通过后，房屋确权认证成功。对于房屋出售或转租的百姓可对房屋进行解绑处理。

随手拍：系统需提供百姓随手拍事件上报功能，上报后由各级协调指挥中心协调处置，移动端可随时查看处置过程和结果。

随手拍评价：系统应具备百姓对随手拍处置结果进行评价，根据评价内容可实时传回指挥中心，指挥中心根据百姓反馈对职能部门处置事件进行考核。

高级认证：系统需提供人脸识别活体检测实现实名认证，并与实有人口库比对，在实有人口库的用户，自动认证成功，未在实有人口库的用户，可根据高级认证进入实有人口库，并可绑定房屋信息进行人房关联。

我的消息：系统需具备各级指挥中心向各负责社区推送相关信息，百姓通过

我的消息功能查看其上报的事件进度和本社区通知的消息。

个人信息：系统需具备对个人信息如手机号、性别、籍贯、微信认证等基础信息进行修改维护，也可进行微信的解绑操作。

3、企业端

企业需要通过微信小程序与 e 冰城做统一融合，并且可进行注册、人员添加、基本信息维护，同时可对企业诉求进行上报，并具备实时查看事件答复和处置的进度。企业端可对管辖内的专属网格员、专属社区、专属民警进行查看。包联企业可查看其包联领导信息。同时系统需要提供信息发布功能，针对性的对企业进行发送政策信息，认证后管理人员可通过政策导读，查看与企业相关的政策、福利等信息。

（十二）与其他系统互联互通服务

1、与省级网格平台互联互通服务

需具备统一制定的城市网格划分，将网格事部件资源数据落实在地图中。实现与省级网格平台及市级数据资源中心互联互通，提供网格数据的信息更新支撑。

2、与地理信息系统互联互通服务

需通过对接勘测院的地图数据服务接口，对系统中所有涉及调用地图服务的功能进行系统业务功能的调整。如：地图展示、缩放；地图标记点、线、面，轨迹播放；地图扎点，获取经纬度等业务应用。

3、与数字城管互联互通服务

需具备对接城市运行管理服务平台的城市部件普查数据，用于增强网格化基层治理平台对于城市部件的管理精细度。同时，接收网格化管理服务平台的事件派单，内部处置流转完成后，反馈相应处置过程与结果。

4、与智慧综治互联互通服务

网格化管理服务平台需要具备与综合治理平台对接进行数据的交互、事件的流转，通过 HTTP 接口的方式对接综合治理平台的实有人口、特殊人群等数据的台账信息，网格系统对于数据的更新等内容可同步给综治平台，形成数据的统一，从而保证数据的及时性和准确性。

5、与视频前端互联互通服务

需要具备与智慧城市之前建设的视频前端设备或视频平台对接，并且采用基于 GB/T28181 协议的视频推拉流的方式，用于增加网格化管理平台对城市前端的感知能力，需要具备将各视频前端定位于地图上，实时调取相关位置视频录像，增强指挥中心的协调调度能力。

6、与 12345 平台互联互通服务

通过网格化管理服务平台与 12345 平台双向融合，拓宽民生问题上行通道，12345 热线与网格化完成一体化运行，从热线到网格，以“12345 热线”为民生问题触角，指挥中心为事件流转枢纽，网格员落实具体网格事项，点对点对接服务对象，精准服务，同时话务人员可查看事件进度及时反馈给百姓，整体提升为民服务的办事质效。

7、与区县网格平台互联互通服务

需要具备与已建的平房区网格化平台、道里区网格化平台、香坊区网格化平台互联互通。基于 HTTP REST 架构进行业务数据整理与区县网格化平台对接，网格化管理服务平台对区县已建网格平台进行事件派单，区县网格平台内部处置流转完成后，反馈相应处置过程与结果。

（十三）数据摆渡与处理服务

1、数据摆渡服务

需要具备互联网与政务外网数据的交互，并且具备相关接口的服务发布、服务订阅、数据交换以及接口状态自动监控等能力。

2、数据处理服务

需要具备对用户提供的人口、房屋、楼栋等一标三实信息台账完成相关数据建库及数据处理服务。

（六）数字政府运营指挥中心建设

1．数字政府运营大屏展示专题

具体技术（参数）要求
数字政府运营大屏展示专题 利用省市共建哈尔滨市市民大厦9楼的数字政府运营中心硬件资源，建设市级数字政府运营中心、接入各部门数据资源，形成若干通用主题和市级专题，实

现一屏统览，并与省级数字政府运营中心对接。

本项目建设以业务需求设计为驱动，依托政务大数据平台的数据汇聚、数据治理能力所提供数据，通过指标业务分析模型的构建，充分释放数据价值。

（一）市级运营指挥中心大屏-专题应用

1、（市级）政务服务专题

政务服务专题需围绕“事前事项、事中办理、事后评价”的全生命周期过程，着力解决企业和群众反映强烈的办事难、办事慢、办事繁的问题。从服务事项、服务办理、服务评价维度进行深度分析。协助政府持续优化政务服务，推进政务服务建设，提升政务服务水平。主要展示内容如下：

（1）服务事项

服务事项需从事项梳理、高频事项、区县排名、层级分布维度进行分析，直观呈现事项的精细化梳理成效，实现事项规范化。

（2）服务办理

服务办理需围绕办件概况、办件来源分布和热门事项维度分析，通过受理率同比变化，精准感知线上线下渠道在群众办事中的应用情况。同时对存在超期办件的区县进行排序，警示并激励其减少此类情况。

（3）服务评价

服务评价需以评价全覆盖、以评促改两个方面进行展示，服务评价汇聚了全渠道的评价数据，实时感知群众的满意度，呈现评价和差评量以及差评详情。然后以差评为出发点，对区县进行排名并对差评整改情况进行统计分析，从而达成以评促改、问题导向的良性循环管理，进而提升政务服务的科学化和规范化水平。

2、（市级）六最品牌专题

六最品牌专题需以“数跑龙江”为统领，以“六最”目标，从“环节最简、材料最少、时限最短、费用最小、便利度最优、满意度最高”六个维度构建指标体系，同时找差距、补短板，为夯实业务基础、重塑业务流程提供支撑依据。

（1）环节最简

在“环节最简”方面，共选取一件事一次办、告知承诺和一业一证3个特殊场景，提取7个指标与先进省份进行对标分析。“一件事一次办”目前已完成企业主题 5个、个人主题8个的上线，结合目前各主题联办效能提升情况推动更多

事项实现“一件事一次办”，提升已上线主题效能。

（2）材料最少

在“材料最少”方面，共选取电子证照、电子印章、电子材料三类材料，提取3个指标与先进省份进行对标。通过自动关联电子证照、电子印章、电子材料等共享数据，简化办事材料提交，并通过区县排名的方式对比优化成效，进而实现材料最少。

（3）时限最短

在“时限最短”方面，共选取减时限、即办件、秒批秒办3个特殊场景，共提取3个指标与先进省份进行对标。通过减时限成效即平均承诺时限压缩比的对标以及各区县的排名情况，梳理改造即办件、秒批秒办事项清单，实现群众在办事过程中“零跑腿、零排队、不见面、全自动”的时限最短的高质量服务。

（4）费用最小

在“费用最小”方面，则是选取了 收费标准化、免中介费、邮寄办 3个特殊场景，共提取3个指标进行对标分析。通过政务服务事项收费标准化、中介免费办、邮寄办服务事项梳理和区县成效排名，推进实现降低企业和群众线下办事的高昂费用。

（5）便利度最优

在“便利度最优”，共选取网办、最多跑一次、跨省通办等9个特殊场景，提取9个指标进行分析。通过对可网办率、实际网办率、最多跑一次事项占比分析以及跨省通办、省内通办、一窗通办和自助办等方式优化政务服务事项，实现跨区域办事和服务大厅的便利性，最大限度实现便利性最优。

（6）满意度最高

在“满意度最高”方面，共选取服务评价、政民互动、12345投诉、涉外服务四个特殊场景，提取4个指标与先进省份对标分析。结合好评数据、政民互动留言数据进行分析，提升企业和群众办理服务满意度，在各级政务服务大厅、便民服务站，建设“办不成事”服务窗口以及外语服务窗口，解决企业和群众办事过程中遇到的疑难事项和复杂问题，进而实现满意度方面的优化。

（二）市级运营指挥中心大屏-指标管理平台

指标管理平台用于支撑数据指标计算，可以根据业务部门需求，及时进行指

标新增、删除、修改操作；同时，可以对指标进行预警规则配置，实现运行潜在风险或具体问题预警。

1、数据源管理

数据源管理是指标数据来源的接入入口，具备接入关系型数据库、分析型数据类型的数据源，和对已接入的数据源的统一管理。

2、业务标准管理

规划制定数据标准，通过规范约束专题库属性、专题库字段等属性，来保障数据的标准化生产，节约后续数据应用和处理的成本。

3、专题库标准管理

专题库标准功能主要用于专题库的配置及分类展示，具备展示专题库标准类型、类型下数量等信息。同时具备对专题库的查询、编辑和删除功能。点击删除按钮并确认后可删除对应的专题库标准。

4、专题库标准导入模板下载

具备下载专题库标准的导入模板至本地，用于批量填入专题库标准信息。

5、专题库标准文件导入

具备专题库标准的批量导入功能。

6、专题库标准文件导入校验

导入时校验各字段的合法性。包括空值校验、格式校验、选项校验。

7、资产目录管理

具备给数据库内各库表添加各类业务属性进行管理，包括目录名称、目录描述、数据领域、服务类型、数据来自行政单位等，形成数据资产。

8、指标标准管理

具备对指标分类、指标政策、单行指标、多行指标的管理和维护，可通过手动录入、规则配置的方式生成指标计算结果。

9、指标申请

用于业务单位申请其他业务部门共享的指标，包括指标需求入篮出篮、指标申请等。

10、指标预警管理

可通过配置预警条件、对预警条件进行逻辑组合的方式配置预警规则，触发

预警规则时形成告警数据。

11、卡片管理

具备将指标库内的指标数据同步至缓存数据库，具备指标类、列表类、趋势类三种卡片的缓存数据库键值、指标/资产目录配置。

12、决策分析模型

用于对决策分析的报告模型进行文字、指标数据、图片等内容的编辑、配置、预览，具备导出成HTML、PDF、图片三种类型的报告。

13、指标配置

根据所设计建设的各专题指标体系配置全市相关业务数据指标计算逻辑规则，包括政务服务、六最品牌专题指标计算规则的配置。

（三）其他要求

1、本次专题建设是围绕政务服务和六最品牌，目的在于全面推进数字化技术在政府服务、监管和治理中的变革。本项目所展示的内容与政务服务指标密切相关。在实施过程中，必须与哈尔滨市营商局进行充分对接，并根据实际业务需求进行建设。

2、为了按照“统筹规划，整体推进”的思路建设哈尔滨市级运营指挥中心大屏，本项目的实施必须满足国家和省级相关技术标准以及业务规范要求。在充分整合现有资源的基础上，结合当前和潜在的业务需求，进行项目实施。此外，建成后大屏系统必须能够与省级运营指挥大屏系统适配对接，并可在哈尔滨市民大厦 9 楼省市共建运营指挥中心硬件上展示。

2．城市运行监测系统

具体技术（参数）要求
城市运行监测系统 升级改造党政办公区 5 楼电教室，建设城市运行监测展示大厅。基于智能应用平台和网络融合技术，搭建城市运行监测平台，接入并融合哈尔滨市重要领域应用系统，建设城市热点、生态环境、政务大数据应用展示、政务云网平台、公共数据开放、政府网站平台及视频共享等专题库，对城市运行各项指标数据进行汇聚、监测和分析；建设融合通讯及协同会商系统，实现多屏展示、一体化联动

交互、音视频指挥调度等功能。

城市运行监测系统通过获取各部门的基础数据，建设信用体系、经济发展、生态环境、公共安全、民生保障、数据共享、云网态势等专题库，构建融合共享、协同一体的哈尔滨市智慧城市运营管理中心可视化监测平台。

（一）专题设计

城市运行监测中心需通过建设信用体系、经济发展、生态环境、公共安全、民生保障、数据共享、云网态势等专题库，构建融合共享、协同一体的哈尔滨市智慧城市运营管理中心可视化监测平台。

1、信用体系

基于运用大数据技术提供对信用数据进行分析。需实现提供信用数据采集专题、平台运行情况分析、信用承诺专题分析、重点人群主题分析、信用主体画像分析、信用主体信用评价信息分析、重点行业信用评价分析等专题分析。

2、经济发展

需提供接入市统计大数据平台、经济运行云、营商一体化平台等系统数据，整体展现全市经济运行情况，对经济走势、态势进行初步分析和预测预警，为经济管理提供数据支撑。主要功能包含经济总览、宏观指标运行监测、产业发展监测、企业发展监测、重点行业监测分析、产业政策分析等。

3、生态环境

需提供接入环保云水环境质量监测、大气环境质量监测、重点污染源监测等关键数据，建设一体化生态环境与安全监测体系，以水污染治理、大气改善、土壤污染防治、清废行动、节能环保、生态融合等为重点构建绿色发展格局。

4、公共安全

需提供接入应急安全各类数据，从安全处置报告、先期处置、响应情况、善后处置、人力资源保障、财力保障、物资保障、医疗卫生保障多角度进行分析，充分展示公共安全问题各角度情况，构建公共安全体系智能分析应用。

5、民生保障

需提供对接哈尔滨市人力资源与社会保障局从社会保险、业务办理情况、社保卡经办网店、民生类事项、民生类办件、没满意度、服务概况、事项热度、服务量评价等多角度对民生保障业务进行数据分析，充分了解民生服务各项情况。

6、数据共享

需提供依据数据共享分类，数据共享分类明细信息进行数据共享情况汇总，能够有效分析数据纳入数量、数据处理情况、数据共享情况等，能够以领导驾驶舱的形式对数据共享内容进行整体展示，有效解决数据共享情况整体分析问题。同时包含服务目录分析、共享接口、运行情况、分类排行等具体分析内容。

7、云网态势

需提供通过对接哈市云资源、网络资源、数据资源等系统平台，通过对接各类实时数据，动态展现云网平台的各类资源监测情况。动态展现全市各类资源动态监测情况。

（二）统一可视化

统一可视化作为专门的可视化平台，它负责将各业务中需要展示的内容与业务逻辑，通过可视化的手段进行配置管理，实现业务的统一展现。由于数据来源的多样性，平台系统需要具备多种类型数据源。

1、可视化呈现

基于布局设计管理与接入中定义的展示内容与展示样式，进行数据解析和可视化呈现。提供丰富的图形展示方式，包括柱状图、累积柱状图、饼图、曲线图、地图等可视化展示方式。

2、数据接入

需提供数据接入功能，能通过各系统发布的数据服务来进行图表和三维可视化呈现，还需要具备各系统发布的与大屏风格统一的相关各种图表资源，具备决策分析的 BI 工具形成的各种指标图表。

3、大屏显示控制

大屏显示控制需具备屏幕复制模式与跟随联动模式。

4、接口设计

需提供接口服务功能，具备可视化平台与其它应用系统的接口，可以直接接入已经开发好的页面资源；具备数据传输接口服务。

（三）数据支撑

数据支撑需提供数据采集、数据处理、数据质量管理、数据资源管理和相应业务的统计分析。

1、数据采集

需满足从政府各部门、机关、事业单位等相关信源单位，根据资源目录为信源单位提供数据采集功能，采集本项目所需各部门的基础数据，通过服务对接、批量导入、手动录入等多种方式，实现本项目所需数据的综合采集管理。

2、数据处理

需满足在已采集数据的基础上，通过数据仓库技术，对已采集的数据进行去重，清洗、转换、比对、组合、抽取等过程，整合优化数据，确保数据的准确性和完整性。

3、数据质量管理

数据质量管理包括数据质量检测流程管理、数据质量检测模型定义、数据质量模型运行管理和数据质量监测监控，保障整体系统的数据实现高可用。

4、数据资源管理

数据资源管理须包括资源目录管理、资源目录变更记录、资源目录发布记录、资源编目与注册、资源审核与发布、资源对象管理。

（四）统计分析

需提供对已采数据按采集部门、采集时间、数据类别、采集数据量、采集方式等进行综合的统计分析功能。对数据处理过程进行综合统计分析，并以统计图表的方式进行展示。

二、融合通讯平台

通过建设融合通信平台实现视频融合、音频融合、终端融合，建立一套标准、统一的指挥调度系统，推动各层级部门之间的沟通协作，可提升多部门联动、重大保障、公共安全、应急服务的水平，缩短响应时间、高效协同、资源充分利用等手段，为当地民众提供更好的服务。

融合通信可实现视频会议、视频监控、eLTE 集群、运营商 IMS 网络等多个系统的全连接，实现固定电话、移动电话、集群终端、会议终端、监控摄像头、无人机、智能眼镜、执法记录仪、VoLTE 终端和大屏拼控等不同通信设备之间的互联互通，通过多种网络融合的全视频通信，实现现场信息回传、大屏统一上墙调度、全视频融合决策会商等场景，具备应急事件处置的统一指挥调度和应急决策信息的快速传达，满足指挥调度及时、高效、无障碍的沟通需求。同时对上层

应用层开放统一接口提供音视频的能力，包括语音集群、视频监控、GIS 调度、视频会商等。

功能要求：

（一）语音电话融合调度

与运营商电话系统对接，实现将座机和手机接入到视频会商会议中来，方便领导、专家以及应急人员随时加入会商会议。

首先向运营商申请一条语音专线，这个语音专线接入语音网关，语音网关通过标准的 SIP 或者 H.323 协议，接入到融合通信平台中。

固话和座机，可以通过语音网关，被可视决策平台的媒体资源处理平台呼叫入会。

（二）视频融合调度

融合通信系统系统，通过国标 GB28181 实现与周边视频监控系统的互联互通，实现将视频监控图像，接入系统，将现场监控图像直接调入应急会商现场和指挥大厅大屏上，方便快速研判和决策。

监控融合网关具备标准的 SIP/H.323 协议以及具备 GB28181 协议，可以实现视频会商系统与视频监控系统的对接。单台监控融合网关最大具备 195 路监控并发通道和 300000 路监控摄像头列表，视频清晰度最大达到 4K30fps，同时具备多监控平台同时对接。

（三）与 GIS 系统对接

系统可对外提供基于标准协议的第三方 API 统一开放业务接口，上层应急指挥 GIS 地图可基于标准 API 接口协议，调用融合通信系统的视频、语音融合能力，在 GIS 地图上实现一键点调，圈选调度等应急指挥调度操作。

具体设备包括：

序号	项目	参数	数量
1	融合通信资源管理平台	1、采用国产自主的处理芯片、操作系统和数据库软件。 2、配置 50 路硬件设备管理 License,50 路硬件设备注册 License。双机许可、2 个第三方高级用户并发授权、20 路监控融合接入路数许可。 3、具备即时会议、预约会议、周期会议、永久会议等会	1

		议模式。 4、具备一键静闭音、广播/选看会场、辅流加入多画面、设置多画面、锁定会议演示、指定会场发送辅流、声控切换、设置主席、点名等功能。 5、具备会议锁定功能，管理员锁定会议后不允许其他终端主动加入会议。 6、硬件双机热备部署		
2	融合通信注册及公私网穿越专用设备	1、采用国产自主的处理芯片、操作系统和数据库软件。 2、配置 8000 个软终端同时注册、100 个软终端并发呼叫能力 3、具备 H.323 Gatekeeper、Sip Server、SIP Proxy 等功能。 4、具备 H.460、ICE、STUN、TURN 等标准的 H.323/SIP 穿越协议。 5、配置 100M 公私网穿越能力 6、硬件双机热备部署	1	
3	融合通信媒体处理单元	1、采用国产自主嵌入式操作系统及国产自主处理芯片 2、具备 ITU-T H.323、IETF SIP 协议，具备良好的兼容性。 3、具备 64Kbps-8Mbps 呼叫带宽。 4、4K30fps、1080p30/60fps、720p30/60fps、4CIF 分辨率的活动视频。 5、具备 ITU-T H.263、H.264BP、H.264HP、 H.265、H.264 SVC、H.265 SVC、H.265 SCC 视频协议。 6、具备 G711、G722、G722.1C、G729、AAC-LD、Opus、iLBC 音频协议。 7、本次配置 32 路 4K30fps 全编全解端口（可动态转换为 40 路 1080P60fps 全编全解端口/80 路 1080P30fps 全编全解端） 8、在全编全解模式下，单台 MCU 硬件最大具备 32 个 4K30fps 视频端口 64 个 1080P60fps 视频端口或者 128 个	1	

		1080P 30fps 视频端口或者 128 个 720P30fps 视频端口。 9、具备 ITU-T H.239、IETF BFCP 双流协议。 10、具备电子白板功能，具备白板批注、缩放、保存、多方互动等功能，具备不少于 72 方同时协作。 11、硬件双机热备部署		
4	融合通信专用设备	1、具备多种调度模式，包括预案调度、跨级调度、融合调度和多调等模式。 2、配合触控 PC 具备触控、拖拽、双击、键盘快捷键等方式操作控制。 3、具备按用户操作习惯，自定义会控功能按钮的优先顺序，不同的账号可拥有各自界面布局，布局设定后下次登录自动应用，无须重新设置。 4、具备一键会控操作，包括呼叫/挂断、设置/取消主席、点名、轮询、广播、静音/闭音、指定会场辅流发送、延长会议、开启/停止录像等功能。 5、具备实时音视频预览，视频清晰度不低于 720P30fps，实现本地终端同步预监、远端会场预监、预览画面截图保存、远端摄像机 PTZ 控制、镜头变倍等。 6、具备辅流预览功能，通过调度台可实时预览辅流画面。 7、具备资源可视化管理，调度资源可以树状列表及棋盘式布局显示。 8、具备 H.264 BP、H.264 HP、H.265 监控视频融合接入，最大视频清晰度具备 4K30fps。 9、具备级联会议选看上下级 MCU 的终端画面，上级平台的调度台可选看多路下级平台的终端画面。 10、配置 16 路语音融合授权、16 路监控融合授权、16 路会议上墙能力、16 路监控上墙能力 11、开发接口给上层应用调用 12、具备基于 GB/T.28181-2016 协议与视频监控平台融合	1	

		互通。 13、具备会议视频、监控视频、手机/固话等音视频资源融合调度，资源列表可通过网络实时获取，无须在多个界面间切换操作。 14、硬件双机热备部署	
5	语音网关	数字中继语音网关，1E1/T1，双千兆网口；具备 30 路并发；具备 SIP、RTP、TFTP、FTP、HTTP、STUN 协议，ISDN PRI 信令。	1
6	电视墙控制器	1、标准机架式设计，嵌入式操作系统，非 Windows、非工控机，MCU 和电视墙解码器之间距离不受限制。 2、具备 H.264BP、H.264HP、H.265 等视频协议。 3、具备 4K30fps、1080P60fps、1080P30fps、720P30fps 等视频解码能力。 4、具备 18 路 HDMI 高清输出接口，具备堆叠扩展。 5、2×10M/100M/1000M 自适应网口。 6、2×RS-232 控制接口。 7、单视频输出口口具备 1/4/9 画面显示。 8、具备图像切换时保留最后一帧图像，画面切换过程无黑屏现象 9、具备通过局域网和互联网接入的 H.323/SIP 会议终端，解码上墙观看。	1
7	监控汇聚网关	1. 设备采用全模块化无线缆设计，独立主控模块、热插拔硬盘、独立电源模块 2. 配置≥两颗 8 核处理器，主频≥2.0GHz，三级缓存≥11MB，内存配置≥48GB 3. 具备硬盘缓启动功能 4. 具备视频流和图片流直存与混存，无需额外接入单独的转发设备 5. 具备 10000 路摄像机接入	1

		6. 具备 H.264，H.265，MJPEG 等多种编码格式设置选项 7. 具备对编码后的视频网络数据进行加密后传输 8. 具备录像的快进慢进播放和快退慢退播放等操作，具备多通道同步回放 9. 具备将重要录像片段锁定，不会被自动循环覆盖，到锁定周期后自动解锁 10. 具备自动搜索、检测、查询联网系统内设备数量、在线情况、图像质量以及运行状态		
8	标绘指挥终端	1、设备须采用一体化设计，具备内置摄像头、麦克风、扬声器、触摸屏等，外部无任何可见内部功能模块及连接线，整体美观、大方，可有效屏蔽内部电路器件辐射，具备固定支架和移动支架安装部署，附带不少于 2 只磁吸式触控笔，适应多种使用环境。 2、液晶屏显示尺寸≥86 英寸；显示比例 16:9；分辨率≥3840*2160，可视角度≥178°，屏幕显示灰度分辨率等级达到 256 级以上灰阶。 3、采用红外感应技术，在双系统下均具备不少于 20 点触控；触摸精度≤±1mm；触摸高度≤2mm；最小识别直径≤2mm。 4、设备须采用内置一体化摄像头，像素≥800 万，镜头水平视角≥80°、垂直视角≥50°，可拍摄不低于 4K 30fps 的高清视频画面。 5、设备须内置≥6 个非独立外扩展的麦克风，具备前向≥180°拾音，拾音距离≥12 米。 具备音视频会议，采用硬件编解码方式，非 PC 结构，稳定可靠。具备 4K、1080P、720P 视频解码能力，非安装第三方 APP 功能。 6、须具备音视频会议，具备自主发起多方会议的功能、可实现广播会场、观看会场、添加/删除会场、静闭音、	1	

		结束会议等功能，可同时显示远端图像、本端图像和辅流图像。 7、须具备通过会议 ID 方式加入会议，加入会议后可查找选看会场、静闭音、申请主席、离开会议等功能。 8、须具备 ITUT H.323 和 IETF SIP 通信协议，G.711A、G.711U、G.722、G.729A、G.722.1C、OPUS、AAC-LD 单双声道等音频协议，H.265、H.264 HP、H.264 BP 等视频协议，从而保证良好的互通性。 9、须具备召开双流音视频会议，要求主流最高达到 4k30fps 的情况下，辅流可同时达到 4k30fps，持控制辅流的自动发送和停止。 10、须具有良好的视频处理能力，呼叫带宽范围具备 1Mbps - 8Mbps。在 384Kbps 带宽下可实现 1080P 30fps 图像格式编解码，在 256Kbps 带宽可下实现 720P 30fps 图像格式编解码，最大限度节省用户网络资源。	

三、视频会议系统

建设市级层面与委办局、区县两级的视频会议系统，在市级建设多点控制单元 MCU 和会议管理平台。通过市级的多点控制单元 MCU 的标准和能力，实现市级与委办局、区县两级视频融合通讯的需求；会议管理平台的管理机制，实现委办局和区县会场信息上传给市级会控平台，市级会控平台能显示和控制全市委办局和区县的会议终端，实现市级指挥中心直接调度委办局和区县的会场。

具体设备如下：

序号	设备	参数	数量
1	MCU	1、采用国产自主嵌入式操作系统，非 Windows、非 Android 系统。 2、具备 ITU-T H.323、IETF SIP 协议，具备良好的兼容性。	1

		3、具备 4K30fps、1080p30/60fps、720p30/60fps、4CIF 分辨率的活动视频 4、具备 ITU-T H.263、H.264BP、H.264HP、H.265、视频协议。 5、具备 G711、G722、G722.1C、G729、AAC-LD 音频协议。 6、在全编全解模式下，单台 MCU 硬件能力最大具备≥16 个 4K30fps 视频端口或者 32 个 1080P60fps 视频端口或者 64 个 1080P 30fps 视频端口或者 128 个 720P30fps 视频端口。 7、具备全编全解技术，确保每个接入的会场均能以任意不同的协议、带宽、格式、帧率参加同一组会议，会议中任何一个参会终端出现丢包仅影响该会场，不会影响整个会议效果 8、具备多台 MCU 组成资源池，实现 MCU 资源统一管理，根据 MCU 资源使用情况，动态分配 MCU 资源，以实现 MCU 资源负载均衡。 9、具备芯片备份、媒体板备份、网口备份、电源备份、风扇备份。 10、具备≥7×24 小时连续正常工作。 11、具备最大 4K30fps 收发对称的 25 多画面分屏。 12、具备 ITU-T H.239、IETF BFCP 双流协议。 13、具备电子白板功能，具备白板批注、缩放、保存、多方互动等功能，具备不少于 72 方同时协作。（如 MCU 不具备此功能，可额外配置电子白板配套设备满足） 14、具备虚拟会议室功能，系统可为个人用户独立分配虚拟会议室，无须平台预定即可召集多方	

		会议；虚拟会议室没有会场加入时，不占用 MCU 端口资源。 15、具备 IPV4 和 IPV6 双协议栈。 16、具备 30%网络丢包下，语音清晰连续，视频清晰流畅，无卡顿、无马赛克；具备 80%网络丢包下，声音清晰，不影响会议正常进行。 17、具备断线重呼功能，MCU 可自动重邀掉线或断电的终端再次入会。	
2	MCU 端口授权	分会场 MCU 并发端口许可	20
3	高清会议终端	1.采用分体式结构，嵌入式架构，非 PC、非工控机架构。 2.采用国产自主的操作系统及编解码处理芯片。 3.终端主要元器件须国产自主，至少包括视音频编解码单元、CPU 处理单元、可编程逻辑芯片、电源模块、时钟芯片、视频输入输出芯片等。 4.具备 64Kbps-8Mbps 呼叫带宽。 5.具备 ITU-T H.323、IETF SIP 协议，具有良好的兼容性和开放性。 6.具备 H.264 BP、H.264 HP、H.265 等图像编码协议。 7.具备 4K30fps、1080p60fps、1080p30fps、720p60fps、720p30fps 等分辨率。 8.具备 G.711、G.722、G.722.1C、G.729A、AAC-LD、Opus 等音频协议，具备双声道立体声功能。 9.具备 H.239 和 BFCP 双流协议。 10.具备≥3 路高清视频输入接口、≥2 路高清视频输出接口。 11.具备≥6 路音频输入接口、≥5 路音频输出接口，至少具备卡侬头、RCA 等音频接口	21

		12.具备摄像头一线连接终端，实现同时传输视频信号、控制信号和摄像头供电 13.具备高清视频信号远距离传输，通过以太网线无需借助额外设备，1080P60fps 高清信号传输距离不少于 120 米。 14.具备不少于 2 个 10M/100M/1000M 自适应网口。 15.具备 30%网络丢包时，语音清晰连续，视频清晰流畅，无卡顿、无马赛克.具备 70%的网络丢包时，声音清晰流畅、无卡顿。 16.具备 1Mbps 会议带宽下，实现 4K30 帧图像格式编解码；具备 512Kbps 会议带宽下，实现 1080P60 帧图像格式编解码；384Kbps 会议带宽下，实现 1080P30 帧图像格式编解码；256Kbps 会议带宽下，实现 720P30 帧图像格式编解码. 17.具备 IPv4 和 IPv6 双协议栈. 18.具备单屏三显功能，在一个显示设备上显示远端图像、本端图像及双流图像。 19.具备在终端前面板显示启动、升级、休眠、异常信息（温度异常、外设连接异常）、IP 地址、H.323 号码、SIP 号码等信息。 20.具备在 H.323 协议下，H.235 信令加密；具备在 SIP 下，TLS、SRTP 加密；具备 AES 媒体流加密算法，保证会议安全。 21.标配触控终端，触控屏尺寸≥10 英寸，分辨率≥1280×800。 22.具备终端休眠和唤醒、设置/取消静音、音量调节、摄像机 PTZ 控制、预置位设置及调用、双流共享、呼叫/挂断会场、添加/删除会场、观看	

		/广播会场、结束会议、申请及释放主席等功能。	
4	高清摄像机	1、具备≥800 万像素 1/2.5 英寸 CMOS 成像芯片，具备 WDR 图像数字宽动态功能。 2、具备 4K30fps、1080P60fps、1080P30fps 等视频输出格式。 3、具备≥12 倍光学变焦。 4、具备水平视角≥72°。 5、水平转动范围：≥+/-110°，垂直转动范围：≥+/- 30°。 6、具备≥254 个预置位。 7、具备≥2 路高清视频输出接口。 8、具备摄像头一线连接终端，实现同时传输视频信号、控制信号和摄像头供电。 9、具备≥2 个控制接口。 10、具备红外透传功能，实现终端遥控器通过摄像机控制机房内会议终端，方便调试。 11、具备图像倒转功能，方便摄像机安装在天花板上。	21
5	调音台	1.输入：不少于 12 通道;4 单声道，4 立体声; 2.输出：输出：平衡 XLR 输出;4 辅助编组，2 推子前折返，1 衰减后辅助，1 组立体声输出;LR 主要 TRS 输出; 3.外接立体声效果输入与内部效果;9 段立体声均衡;24DSP 效果;MP3 播放器;低通滤波 XLR 输出;+48V 幻象电源开关; 4.具有 100MM 推子;USB 录音功能;12 路可机架安装. 5.总谐波失真：低于 0.1%; 6.频率响应：20Hz-20KHz，+1dB-3dB	1

		7.输入和输出阻抗：话筒输入：2.4KΩ，线路输入：11KΩ，立体声输入：100KΩ，主输出阻抗：75Ω，编组阻抗：75Ω，AUX 输出阻抗：75Ω 8.EQ（单声道输入）：高频：12KHz±15dB，中频：120Hz~4k±15dB，低频：80Hz±15dB	
6	全频扬声器	1.频率响应：≥180Hz-18KHz 2.灵敏度：不低于 93dB 3.标称抗阻：6Ω 4.额定功率：不低于 240W AES,960W peak 5.全频单元：6X4""(100mm) voice coil 6.扩散角度：水平不小于 130°x 垂直不大于 24° 7.最大声压级：不小于 116dB continuous, 122dB peak	4
7	功率放大器	1.采用 2U 标准机箱，高强度的钢机架结构； 2.采用 SMT 贴片技术，保证了产品的一致性和稳定性；可选择立体声、并联、桥接三种工作模式环形变压器，有效的隔离干扰； 3.额定功率(rms)立体声 8Ω:≥2×300W; 4.额定功率(rms) 立体声 4Ω:≥2×450W; 5.桥接 8Ω:≥900W; 6.信噪比:>112dB 7.转换速率:>100V/US 8.阻尼系数:>1500:1 9.频率响应:20Hz-20KHz ±0.2dB; 10.总谐波失真:< 0.025% 11.互调失真:< 0.05% 12.输入灵敏度:0.775V/1.4V（32dB) 13.输入阻抗:20KΩ,BLANCE/10KΩ,UNBLANCE	2

		14.输入共模抑制比:>80dB 15.串音干扰/分离度: >80dB 16.保护电路：保护电路包括温度（过热）、短路、直流、压限、过载、过流、失真限幅、欠压/过压、开关机噪音、负载不匹配（低阻）开机软启动、开机防浪涌、无线电干扰、次生波、高频输出自动检测（超高频）等保护 17.冷却系统：自动无级变速双风扇强制冷却 18.输出电路类型：H 类	
8	数字音频矩阵	1.具备手机、平板控制与分布式云控制 2.自带 B/S 架构服务端，通过网页浏览器访问，不仅实现了通道控制和场景选择,而且直接提供 PC 客户端及平台组件的下载链接 3.系统内置锁屏功能，有效避免发生误操作 4.DSP 音频处理，内置自动混音，矩阵混音，噪声消除、回声消除、反馈消除、自动增益 5.输入每通道：前级放大、信号发生器、扩展器、压缩器、5 段参量均衡 6.输出每通道：31 段图示均衡、延时器、分频器、限幅器 7.全功能矩阵混音功能 8.具备场景预设功能 9.断电自动保护记忆功能 10.模拟通道数:不少于 8 路输入+8 路输出； 11.Dante 通道数:不少于 4 路输入+4 路输出 12.DSP 处理：Ti 456MHz FLOPS DSP 13.GPIO：不少于 2 个输入 14.Rs485：不少于 1 个 15.Rj45 控制接口：不少于 1	1

		16.模拟最大增益：不低于 51dB 17.量化位数：24bit 18.采样率：48kHz 19.频率响应（20~20KHz）：±0.2dB	
9	电源时序器	1.设备总电流：不小于 60A 2.单路输出电流：不小于 16A 3.输出路数：不少于 8 路可控+2 路常开插座 4.具有 2 英寸 TFT 彩色液晶屏，实时显示当前日期时间、当前电压、通道开关状态等信息，具备中英文； 5.具有 8 路可控电源输出，各路延时开启和关闭时间可设置为 0~999 秒 6.面板锁功能防止误操作，保障设备安全可靠 7.内置实时时钟，可灵活设置定时开关机（按照月、日、年星期等周期阶段循环） 8.RS485 端口具备级联不少于 50 台，便于较大应用系统统一控制 9.网络 RJ45 端口、RS232 端口及外部启动触发端口，具备外部中控设备控制 10.具有不少于 10 组设备开关模式，方便灵活存储和调用 11.完善的过压、欠压保护机制，且可灵活设置	1
10	无线会议话筒（一拖四）	1.四通道通道接收机面板采用 LED 显示窗口，显示各项功能与数据 2.具有电子音量旋钮。 3.高频高动态范围电路，提升互调动态之性能，数字导频,动态独立 ID 码,降低谐波干扰，以增加更多机器同时使用互不干扰的频道数。4.接收距离不低于 60 米	2

		5.接收机载波频段：UHF520~940MHz（选配） 6.通道数：四通道 7.调制方式：FM 8.灵敏度：输入 6dBv 时，S/N>60Db 9.频带宽度：30MHz 最大偏移度:±45KHz 10.综合 S/N 比：>105dB 11.综合 T.H.D:<0.7% @1KHz 12.综合频率响应：45Hz~18KHZ ±3dB 13.会议式发射机载波频段：UHF520~940MHz（选配） 14.振荡方式：PLL 相位锁定频率合成 15.谐波幅射：<-65dBm 16.最大偏移度：±45KHz 17.频率响应：45Hz~18KHZ ±3dB 18.频带宽度：120MHz 19.音头：电容式 20.RF 功率输出：15MW 21.连续工作时间:不低于 12 小时	
11	机柜	1.容量:22U 2.标准:19 英寸标准。 3.尺寸:1200mm×600mm×600mm 4.材质：冷轧钢板	1
12	音箱壁架	1.最大承重:≥40 Kg 2.水平角度:-90°~+90° 3.垂直下倾角度:-7.5°~+90° 4.离墙最远距离:100 mm 5.材质:冷轧钢板	4
13	调音台	1.不少于 8 路通道输入;每通道 3 段均衡器; 2.不少于 2 路 AUX，1 组立体声输出;	20

		3.内置 99 种 DSP 数字效果器; 4.内置提供直流 48V 幻象电源; 5.高品质 USB 播放器带显示;蓝牙显示器;60mm 推子。 6.总谐波失真：低于 0.1% 7.频率响应：20Hz—20KHz,+1dB-3dB 8.输入和输出阻抗：话筒输入：2.4KΩ，线路输入：11KΩ，立体声输入：100KΩ，主输出阻抗：75Ω，编组阻抗：75Ω，AUX 输出阻抗：75Ω 9.EQ(单声道输入) 高频：12kHz±15dB，中频：120Hz~4k±15dB， 低频：80Hz±15dB	
14	全频扬声器	1.频率响应：≥180Hz-18KHz 2.灵敏度：不低于 93dB 3.标称抗阻：6Ω 4.额定功率：不低于 240W AES,960W peak 5.全频单元：6X4""(100mm) voice coil 6.扩散角度：水平不小于 130°x 垂直不大于 24° 7.最大声压级：不小于 116dB continuous, 122dB peak	40
15	功率放大器	1.采用 2U 标准机箱，高强度的钢机架结构； 2.采用 SMT 贴片技术,保证了产品的一致性和稳定性；可选择立体声、并联、桥接三种工作模式环形变压器，有效的隔离干扰； 3.额定功率(rms)立体声 8Ω :≥2×300W; 4.额定功率(rms) 立体声 4Ω :≥2×450W; 5.桥接 8Ω :≥900W; 6.信噪比:>112dB	20

		7.转换速率:>100V/US 8.阻尼系数:>1500:1 9.频率响应:20Hz-20KHz ±0.2dB; 10.总谐波失真:< 0.025% 11.互调失真:< 0.05% 12.输入灵敏度:0.775V/1.4V（32dB) 13.输入阻抗:20KΩ ,BLANCE/10KΩ ,UNBLANCE 14.输入共模抑制比:>80dB 15.串音干扰/分离度: >80dB 16.保护电路：保护电路包括温度（过热）、短路、直流、压限、过载、过流、失真限幅、欠压/过压、开关机噪音、负载不匹配（低阻）开机软启动、开机防浪涌、无线电干扰、次生波、高频输出自动检测（超高频）等保护 17.冷却系统：自动无级变速双风扇强制冷却 18.输出电路类型：H 类	
16	数字音频矩阵	1.不少于 2 路模拟输入，4 路模拟输出 2.采用第四代 SHARC ADSP-21489 高性能浮点 DSP 芯片 3.具有 96Khz 采样频率保障捕捉声音细节，AD/DA 动态范围 118dB 4.性能指标：动态范围>110dB，THD+N<0.0025%，设备最小固定延时<2ms 5.内置粉红/白噪声/正弦发生器 6. 参量均衡器类型：PEQ/Lo-Shelf/Hi-Shelf/Allpass1/Apass2（全通滤波器可用作相位调节） 7.高低通滤波器：Bessel/Butterworth/Link-Riley 的斜率从 6~48dB/Oct 范围内可选	20

		8.输入输出可调延时达到 1000ms，精度 0.02ms 9.输入通道：噪声门、反馈抑制器、10 段参量均衡、3 段动态均衡器、高低通、压缩器、延时 10.输出通道功能：矩阵混音，10 段参量均衡、高低通、压缩器、限幅器、延时器 11.以太网+USB+RS232/485 控制接口，开放 TCP/IP 及串口协议实现第三方控制 12.GPIO 端口（输入输出各 2 个）便于系统集成联控，可选 GPIO 扩展盒 13.PC 软件搜索发现处理器，具备不少于 23 组场景预设，可灵活调用	
17	电源时序器	1.设备总电流：不小于 60A 2.单路输出电流：不小于 16A 3.输出路数：不少于 8 路可控+2 路常开插座 4.具有 2 英寸 TFT 彩色液晶屏，实时显示当前日期时间、当前电压、通道开关状态等信息，具备中英文； 5.具有 8 路可控电源输出，各路延时开启和关闭时间可设置为 0~999 秒 6.面板锁功能防止误操作，保障设备安全可靠 7.内置实时时钟，可灵活设置定时开关机（按照月、日、年星期等周期阶段循环） 8.RS485 端口具备级联不少于 50 台，便于较大应用系统统一控制 9.网络 RJ45 端口、RS232 端口及外部启动触发端口，具备外部中控设备控制 10.具有不少于 10 组设备开关模式，方便灵活存储和调用 11.完善的过压、欠压保护机制，且可灵活设置	20	

18	无线会议话筒（一拖四）	1.四通道通道接收机面板采用 LED 显示窗口，显示各项功能与数据 2.具有电子音量旋钮。 3.高频高动态范围电路，提升互调动态之性能，数字导频,动态独立 ID 码,降低谐波干扰，以增加更多机器同时使用互不干扰的频道数。4.接收距离不低于 60 米 5.接收机载波频段：UHF520~940MHz（选配） 6.通道数：四通道 7.调制方式：FM 8.灵敏度：输入 6dBv 时，S/N>60Db 9.频带宽度：30MHz 最大偏移度:±45KHz 10.综合 S/N 比：>105dB 11.综合 T.H.D:<0.7% @1KHz 12.综合频率响应：45Hz~18KHZ ±3dB 13.会议式发射机载波频段：UHF520~940MHz（选配） 14.振荡方式：PLL 相位锁定频率合成 15.谐波幅射：<-65dBm 16.最大偏移度：±45KHz 17.频率响应：45Hz~18KHZ ±3dB 18.频带宽度：120MHz 19.音头：电容式 20.RF 功率输出：15MW 21.连续工作时间:不低于 12 小时	40
19	机柜	1.容量:16U 2.标准:19 英寸标准。 3.尺寸:800mm×600mm×600mm 4.材质：冷轧钢板	20

20	音箱壁架	1.最大承重:≥40 Kg 2.水平角度:-90°~+90° 3.垂直下倾角度:-7.5°~+90° 4.离墙最远距离:100 mm 5.材质:冷轧钢板	40
21	线材安装调试	线材安装调试	20

四、城市运行管理指挥中心配套设备

监控中心展示大屏设计为两部分，一是主展示屏，二是侧面两个智慧屏。采用 COB 屏，包括展示屏的配套设施。

设备如下：

序号	设备	参数	数量
1	COB 全彩屏	COB 全彩屏，尺寸 7.2X2.36，COB1.25，分辨率 5760 X1890 1.像素点间距：≤1.25mm，COB 封装：RGB 全倒装封装； 2. 箱体尺寸：600mm×337.5mm；箱体采用 16：9 比例设计； 3. 暗室对比度：≥1000000:1； 4. 采用无风扇自然散热结构；具备模组、接收卡、电源完全前维护； 5.光学参数：水平、垂直视角≥160°；亮度均匀性校正后≥98%； 6.可实现箱体拼接、自动对位，具备拼缝微调节机构，保证拼缝精度达到≤0.05；； 7.色域覆盖率：≥97%；； 8.安全电路内导体和地之间的电压不应超过 42.4V 交流峰值或 60V 直流值； 9.电气参数：平均功耗≤125W/㎡；	16.99 平方米

		10.采用雾面膜可以达到抗反射，抗眩光，一体黑的效果； 11.具有鬼影消除功能； 12.具有整屏色平衡调整功能，确保基色一致性； 13.具备 USB、TCP/IP、手机三种控制方式； 14.模组可存储校正数据，更换模组，可自动回度模组中校正数据； 15.具备匹配运维管理软件，可通过软件进行控制； 16.模组、接收卡与主板采用硬接口设计，无排线，具备直接插拔，每个单元具有独立网口； 17.包含原有背景墙拆除及重新装饰、安装调试、综合布线		
2	发送卡	发送卡，定制	6	
3	视频控制器	视频控制器，匹配 COB 屏视频控制	1	
4	预间板卡	预间板卡，定制	1	
5	显示屏钢结构	显示屏钢结构，定制	16.99 平方米	
6	扩展系统软件	1.具备拓展羽化功能； 2.具备 4K 信号输入，具备数字 4K 信号输出，具备外景信号输入，具备 REF 信号输入； 3.具备摄像机变化数据记录，摄像机做平遥、俯仰、变焦等取景构图变化时，系统具备实时地生成相应的运动数据并记录； 4.具备启用 HDR 显示器的编辑器设置； 5.具备在配置软件中添加切换器型号和端口，具备在切换设置里设置对应的切换延时；	1	

		6.具备配置软件同步、硬件同步。	
7	综合布线	综合布线	1
8	移动控制器	移动控制器，匹配大屏控制	1
9	功放+4 个音柱+调音台+6 个无线麦克	功放+4 个音柱+调音台+6 个无线麦克	1
10	运输	运输	1
11	COB 全彩屏 1	COB 全彩屏，尺寸 3X2.36，分辨率 2400X1890 1.像素点间距：≤1.25mm，COB 封装：RGB 全倒装封装； 2. 箱体尺寸：600mm×337.5mm；箱体采用 16：9 比例设计； 3. 暗室对比度：≥1000000:1； 4. 采用无风扇自然散热结构；具备模组、接收卡、电源完全前维护； 5.光学参数：水平、垂直视角≥160°；亮度均匀性校正后≥98%； 6.可实现箱体拼接、自动对位，具备拼缝微调节机构，保证拼缝精度达到≤0.05； 7.色域覆盖率：≥97%； 8.安全电路内导体和地之间的电压不应超过 42.4V 交流峰值或 60V 直流值； 9.电气参数：平均功耗≤125W/㎡； 10.采用雾面膜可以达到抗反射，抗眩光，一体黑的效果； 11.具有鬼影消除功能； 12.具有整屏色平衡调整功能，确保基色一致性；	7.08 平方米

		13.具备 USB、TCP/IP、手机三种控制方式； 14.模组可存储校正数据，更换模组，可自动回度模组中校正数据； 15.具备匹配运维管理软件，可通过软件进行控制； 16.模组、接收卡与主板采用硬接口设计，无排线，具备直接插拔，每个单元具有独立网口； 17.包含原有背景墙拆除及重新装饰、安装调试、综合布线；	
12	视频控制器	视频控制器，具备大屏视频控制	1
13	显示屏钢结构	显示屏钢结构，定制	7.08 平方米
14	综合布线	综合布线	1
15	功放+音柱 2 个	功放+音柱 2 个	1
16	运输	运输	1
17	COB 全彩屏 2	COB 全彩屏，尺寸 3X2.36，分辨率 2400X1890	7.08 平方米
18	视频控制器	视频控制器，具备大屏视频控制	1
19	显示屏钢结构	显示屏钢结构，定制	7.08 平方米
20	综合布线	综合布线	1
21	功放+音柱 2 个	功放+音柱 2 个	1
22	运输	运输	1

五、城市运行管理指挥中心场所改造

1. 硬件设施。监测中心需要采购的设备有：大屏子系统、坐席管理系统、操作台、会议系统、扩声系统、矩阵切换系统、会议录播系统、集中控制系统、辅助材料、办公桌椅、监控系统、调度中心小机房、安全防护等。

2.网络环境。依托党政大楼电子政务外网安全环境支撑，接入智慧城市运行监测系统；按需接入部分委办局专线及业务系统，作为专网的接入客户端使用专网资源，实现跨系统数据调用和集中展示。 3.场地装修。党政机关大楼东配楼5楼电教室房间总面积约120平方米。本项目基于既有办公环境，增配、改造为可支撑日常监管、大屏展示、会议磋商等应用的多功能调度中心大厅的环境改造（含网络布线）。

（七）一体化运维服务平台建设

1．运维服务平台

具体技术（参数）要求
运维服务平台 建立规范化、标准化、制度化的运行维护体系，完成对系统运行状态的全面监控和故障的及时处理，支持应用系统的安全、稳定、高效、持续运行。对业务系统的基础资源、业务系统可用性能、中间件及数据库状态等进行统一运维监控告警，具有全层级监控能力的一体化运维服务平台。 （一）采控中心 1、主机管理 主机管理功能需具备对接入采控中心的物理机、云主机、虚拟机、容器等资源进行统一管控。主要功能包括： （1）统计页面：需具备实时统计并展现当前运维管理平台已纳管的主机、Agent总数以及对应分类下的数量。 （2）添加主机：需提供普通和远程安装两种添加主机的方式。两种模式下均可通过添加扩展插件、指定主机标签、选择使用不同的配置文件进行注册等。同时，添加主机功能还具备主机模板，Agent关联选择、主机添加等管理功能。 （3）主机列表：需具备将Agent发现的主机生成主机列表，实现主机IP、名称、操作系统、标签、状态、Agent名称版本等相关主机信息的统一展示和管理。 （4）批处理主机Agent：需具备最大并发1000台的主机处理量，包括批量安装插件，批量升级、卸载、重启Agent以及批量删除离线主机等操作。

（5）管理单个主机 Agent：需具备对特定主机上的 Agent 进行状态更改。

（6）筛选主机：需具备通过搜索框对主机资源进行搜索，可通过状态，IP、主机名称、标签进行精准或模糊搜索。

（7）管理容器：需具备对容器环境进行管理，可查看容器环境运行状态，发现的服务。

（8）管理插件：需具备对预置或上传的插件进行批量管理以及监控详情展示。

（9）管理标签：需具备为主机配置标签信息，可以对主机进行标注、分类管理。

（10）主机操作记录：具备对主机和插件相关的操作（例如添加主机、安装升级 Agent，启停 CDC 等）进行实时日志记录。

（11）集群管理：具备对主机组建集群，集群内的主机自动组建高可用集群，当单主机故障时，具备根据集群内其他主机负载情况自动将任务分配到其他节点。具备通过普通安装或远程安装的方式安装主机组集群。

2、集成服务

需具备将 Agent 安装、指标监控和日志采集配置等流程封装标准化模板，实现对主机不同监控指标、不同数据源日志的采集。具备根据模板创建的任务进行归类监控和操作。主要功能包括：

（1）集成服务：需具备在采控中心集成服务显示已应用和可应用的集成服务列表，同时提供根据应用名称进行搜索查询的功能。

（2）自定义采集：模板库需内置部分采集模板，可预览模板的详情，需具备直接通过应用模板创建采集监控任务，提供根据应用名称进行搜索查询的功能。

（3）采集监控任务管理：具备对采集任务进行监控、管理等功能。

3、自动发现

需具备通过安装远程自动发现插件自动发现所属同一网段内的所有物理节点设备信息和该节点上对应的相关应用及服务，将所属节点设备信息和该节点对应服务信息进行展示，具备输出给 CMDB 入库保存。主要功能包括：

（1）管理扫描任务：需具备新建扫描任务，周期性的扫描 IP 范围内的节点

设备。

（2）管理发现结果：需具备匹配 CMDB 模型，分类展示所属节点设备信息和该节点对应服务信息，具备选择是否输出入库保存，将发现结果导入 CMDB 库中。

（3）管理导入结果：需具备对发现的设备信息和该节点对应的服务信息入库保存，并将结果进行展示。

（4）深度发现管理：需具备对远程发现的设备执行深度发现采集任务，采集该设备的属性相关信息，采集到的属性信息具备自动导入 CMDB 入库保存。

（5）脚本管理：需具备自动探测目标节点上所具有的服务，自动执行深度发现脚本，深度采集设备或服务属性相关指标信息。

（6）任务管理：需具备对创建的采集任务进行管理，监控任务的采集状态和信息查看，并将操作汇总形成任务操作日志。

4、Agent 版本管理

需具备对采控中心部署的所有 Agent 版本进行管控，包括批量上传安装解析安装包，查看性能测试报告等。主要功能包括：（1）添加 Agent：需具备对 Agent 的添加操作。

（2）查找 Agent：需具备通过索引条件对 Agent 进行查询操作。

（3）删除 Agent：需具备对 Agent 的删除操作。

（4）查看 Agent 详情：需具备通过索引条件对 Agent 进行详情查看。

5、监控告警

需具备对 Agent 异常状态以及采集任务的异常状态进行告警设置，实现对采控 Agent 以及任务的监控需求，具备对接其他告警源。主要功能包括：

（1）配置告警规则：需具备对采控中心纳管的所有 Agent 和任务进行告警设置，监控 CPU、内存、磁盘和网络等资源消耗情况，当资源消耗超过设定的告警规则时，第一时间通知运维人员对异常进行处理。

（2）修改告警规则：需具备对采控中心纳管的所有 Agent 和任务进行告警规则修改。

（3）删除告警规则：需具备对采控中心纳管的所有 Agent 和任务进行告警规则删除。

（4）查看告警信息：需具备对采控中心纳管的所有 Agent 和任务进行告警

规则查看。

6、系统设置

配置管理需具备添加配置规则、查找配置规则、查看配置规则详情、下发配置规则、管理适配主机、删除配置规则、修改配置规则。主要功能具备：

（1）配置管理：需具备根据具体使用情况对配置文件的配置项进行批量编辑修改，并下发给目标主机，配置文件的下发具备热加载。

（2）熔断设置管理：需具备针对不同 Agent 进行设置，当监控到 CPU、内存、磁盘和网络使用情况超过设定的阈值时，自动触发熔断机制，对主机进行保护，防止因为资源的持续消耗造成主机系统瘫痪对业务造成影响。

（3）模块版本查看：需显示模块版本号，方便模块的管理。

（4）统一认证平台对接：系统需和统一认证平台对接，可同步用户、组织、权限等数据，实现单点登录。

（二）告警处置中心

1、告警源管理

告警源模块需接入来自各类告警源的原始告警消息以及数据指标，可接入的告警源消息类型包括：自有告警消息、监控告警消息、接口告警消息以及消息队列告警消息。主要功能包括：

（1）告警源模板管理：告警源模块需接入来自各类告警源的原始告警消息以及数据指标。

（2）告警源采集管理：需具备通过告警源模板配置告警采集任务，并对告警采集任务进行管理。

2、事件概览

需具备通过事件仪表盘对事件管理系统中的问题事件进行全局管理和多维度分析。具备查看最近 7 天/14 天的数据。主要功能包括：

（1）基础概览页面：需具备对基础概览页面的数据查看。

（2）统计概览页面：需具备对统计概览页面的数据查看。

3、事件管理

主要功能需包括：我的事件处理中列表、我的事件已解决列表、我的事件检索、我的事件自定义检索项。主要功能包括：

（1）告警事件列表：需展示我的事件、所有事件以及归档事件的事件列表以及事件详细信息。

（2）事件详情展示：需具备查看告警压缩合并后形成的事件的详细信息，包括事件信息、告警信息以及处理记录，知识推荐等内容。

（3）处理告警事件：需包含对触发的告警的解决流程操作。

4、事件设置

对系统内的规则需进行统一的展示与管理，可具备自定义合并规则。并具备可对规则进行查看、编辑、启用/暂停以及删除操作。主要功能包括：

（1）合并规则：合并规则需对系统内的默认合并规则以及自定义合并规则进行统一的展示与管理，可自定义合并规则。并可对合并规则进行查看、编辑、启用/暂停以及删除操作。

（2）事件处置策略：可自定义事件处置策略，将符合条件的问题事件需按照设置好的处置规则进行分派，被处置的对象可以在工作台中查看和处理。处置规则中具备告警事件筛选、循环时间设置、告警恢复通知、告警升级等选项。

（3）告警直发策略：告警处置中心的告警直发策略列表展示内容需包括处置策略名称、类型、描述、合并规则、状态、最近修改时间和操作。

（4）静默规则：告警处置中心需提供告警静默策略的配置功能，具备对系统维护时间窗口内的告警进行静默处理，减少不必要的告警骚扰。比如：当系统升级，软件/平台/服务/主机等维护期间，不发送告警。具备无数据搜集告警静默以及有数据搜集告警静默。告警静默类型具备设定一次性任务、每日任务、每周任务、每月任务等周期性任务，满足不同告警静默事件管理需求。

（5）通知模板：事件通知功能需具备手机短信、电子邮件、URL 回调等多种通知方式，具备自定义通知模板，确保问题事件通知能够被及时送达。

（6）分派记录：告警事件匹配相应的处置规则后，需分派给相应的处理人或自动创建工单。在分派记录中，可以查看相应的分派记录以及告警通知发送的状态。

（7）字段映射规则：需具备对原始告警消息中的字段进行统一定义，可以新增字段、扩展 CMDB 属性字段，丰富告警消息字段。

具备对原始告警的字段和内容进行修正，可以使告警中具有统一的字段，方

便展示界面进行排序、搜索、展示等，同时方便后续的生成事件的流程，如将来自不同数据源的告警信息的字段统一起来，方便设置关联。需具备利用额外的数据赋予告警消息更丰富的信息，譬如主机、服务等其他信息；并可对 CMDB 中维护的资源信息和告警信息进行关联。

（8）刷新频率设置：需具备设置概览、我的事件页面及所有事件页面的刷新频率。

5、系统管理

系统管理内工单系统对接需具备调用工单系统手动创建工单、对接工单系统工单创建配置接口、开发工单调用接口、对接工单自动创建接口、告警消息信息变更同步、信息同步推送接口、工单处理结果同步。

（三）资源配置中心

1、资产概览

需具备对系统中的资源进行统计以及可视化展示，展示系统环境中的基本信息（包括模型总量、配置项总量、配置项关系总量、拓扑图总量以及业务总量数据）、关注的业务线/资源分区列表、近 7 日配置项变更统计以及各模型下配置项的分组统计数据。主要功能包括：

（1）统计与可视化展示：需具备对 CMDB 中的资源进行统计以及可视化展示，展示系统环境中的基本信息（包括模型总量、配置项总量、配置项关系总量、拓扑图总量以及业务总量数据）、关注的业务线/资源分区列表、近 7 日配置项变更统计以及各模型下配置项的分组统计数据。具备下钻跳转到对应的模型或者资源仓库中的配置项列表页面。

（2）全局搜索：针对配置项以及配置项属性进行检索，需具备复杂语句搜索（AND 和 OR）、具备根据配置项单行文本、多行文本、整数、小数、表格等属性进行搜索、具备根据模型对配置型进行二次搜索。

（3）配置项关系路径搜索：需具备通过搜索两个配置项之间的关键路径和途径配置项，从而发现整个链路关系。

2、模型管理

需具备对模型分类分层、模型分类检索、新增模型分类、删除模型分类、编辑模型分类、折叠模型分类、展开模型分类。主要功能包括：

（1）模型分类管理：需具备对模型类别进行层级设置、分类名称检索，可添加、编辑以及删除模型的一级分类和模型的子分类名称。

（2）模型定义与管理：需具备通过模型的属性以及模型关系来完整地定义模型，可定义模型的属性和关键属性，通过关键属性来标识配置项的唯一性，并可对属性动态定义。

（3）关系类型管理：需具备定义模型与模型、以及配置项与配置项的关系。

（4）模型拓扑：需具备从全局视角直观查看各个模型之间的关联关系，可新增或者删除模型之间的关系。

（5）模型模板管理：需具备将重复使用的通用属性单独定义为模板，直接导入已梳理好的模型将其沉淀为模板，达到复用模型的目的。

3、资源仓库

配置项管理需在资源仓库中以资源的视角具备对所有配置项进行统一组织和管理，配置项可手工录入或者批量导入，并具备配置项关系定义、配置变更历史查看以及配置项查询等功能。

4、拓扑管理

配置项拓扑具备从图形化的视角来构建配置项（资源）之间的关联关系，可自定义配置项拓扑，满足不同的业务场景下对配置项（资源）关系的查看需求。需具备拓扑图的查找、新建、编辑、删除。

（5）查看拓扑图详情

5、业务管理

需具备自定义业务层级以及基于业务层级来建立模型，通过业务层级来直观地查看模型之间的业务关系，可按照业务线进行数据授权，管理业务线下的配置项，保证数据的安全性。主要功能包括：

（1）业务层级管理：可自定义业务层级以及基于业务层级来建立模型，需具备通过业务层级来直观地查看模型之间的业务关系。并可跨层级建立模型关系。

（2）业务线管理：以业务层级拓扑为基础，从业务和应用的视角来组织和维护软硬件、网络、服务等资源的配置项信息和关联关系。需具备按照业务线进行数据授权，管理业务线下的配置项，保证数据的安全性。

6、资源分区

资源分区需从资源的视角对配置项进行组织和维护，具备按照资源分区授权，从资源维度对资产配置管理模块进行分权管理。主要功能包括：

（1）资源分区管理：资源分区从资源的视角对配置项进行组织和维护，需具备按照资源分区授权，在 CMDB 中从资源维度的分权管理。

（2）资源分区中管理配置项：资源分区需具备从资源的视角对配置项进行组织和维护

7、系统设置

系统设置提供标签管理、数据字典管理、校验规则管理以及关系自动生成规则管理功能。系统设置提供主要功能需包括：

（1）校验规则管理：校验规则的定义和管理，用于配置项属性数据的校验，在一定程度上提高数据的准确性，防止误操作或者不规范的录入行为造成的数据质量问题。需设置校验规则，在配置项中录入属性数据时，可按照规则进行校验。

（2）数据字典管理：数据字典是描述数据的信息集，为配置中心中需要设置固定值的某些属性提供标准数据，如列表、单选控件、复选控件等，方便管理员根据业务场景灵活扩展选项内容，在保证数据标准化的同时保证数据的可扩展性。

（3）标签管理：配置项可添加标签，通过标签管理实现配置项的分类、分组管理，并按照标签分类展示配置项。

（4）通知管理：通过订阅的方式将配置项的变更情况，通知给订阅的管理员，管理员能够及时地关注并处理变更。

（5）关系生成规则：提供关系生成规则的定义和管理能力。可根据配置项关系自动生成规则，自动建立配置项间的关联。

8、自动采集

对操作系统基础信息、主机规格信息的采集。如操作系统名称、版本、CPU 核数、内存容量、存储容量等。需实现自动采集主机信息、自动采集中间件信息、自动采集数据库信息、自动采集云资源信息。

9、统一权限管理

系统和统一认证平台对接，可同步用户、组织、权限等数据，实现单点登录。

需实现单点登录、用户信息对接、功能权限对接、数据权限对接、角色信息对接、组织结构信息对接。

（四）业务可用性监控中心

业务可用性监控中心需具备对业务数据以及主机、中间件等基础资源进行统一监控，具备构建业务接口监控能力，业务接口必须具备与省上相关应用的对接。结合监控指标、分析日志、告警详情等，帮助快速发现、分析并定位故障。

1、监控首页

需提供应用告警数 TOP5、告警级别占比、主机监控占比、数据库监控占比、中间件监控占比、活跃告警展示、告警数趋势等可视化展示。可以统计与展示的数据需涵盖应用告警数 TOP5 统计排行、获取全部租户信息、各告警级别告警数量统计、各监控类型告警数量统计、活跃告警列表、告警详情信息、跳转告警详情、跳转告警记录、跳转应用拓扑、近 7 天/近 30 天告警数量趋势统计。

2、应用监控

需具备以地市－单位－系统平台层级视角对应用展示，具备提供健康度、告警分布情况等信息。主要功能包括：

（1）应用监控：以地市-单位-系统平台层级视角对应用展示，提供健康度、告警分布情况等信息。应用监控主要功能包括：

同步租户信息定时任务。

（2）业务拓扑：提供业务拓扑展示能力，具备节点配置详情、节点健康情况、定位异常所在节点位置。

（3）系统健康评分：能够从业务维度、业务运行情况进行健康度评分，更进一步协助运维人员掌控系统运行状态。

3、监控视图

需具备提供实例监控的基本信息、指标清单、进程视图、告警情况展示。主要功能包括：

（1）主机监控视图：提供主机实例监控的基本信息、指标清单、进程视图、告警情况展现。

（2）数据库监控视图：提供数据库实例监控的基本信息、指标清单、告警情况展现。

（3）中间件监控视图：提供中间件实例监控的基本信息、指标清单、告警情况展现。

（4）数据同步：提供与 CMDB 接口同步，具备 CMDB 数据推送数据到监控中心，接口必须具备与省上相关应用的对接。

（5）实例详情：具备查看被监控基础资源（主机、数据库、中间件）实例对象的基本信息,指标清单仪表盘,具备查看对应实例当前活跃中告警列表功能。

4、接口监控

需具备创建基于 HTTP、PING、TCP/IP、SNMP、WEBSOCKET 等不同协议的拨测任务，展示客户端、服务端、全链路等接口调用情况。通过实时监测，统计拨测任务可用情况，提供实时告警，同时需实现接口拨测任务创建、接口拨测任务编辑、。协议适配及告警

（1）单多步骤接口监控配置：提供配置单步骤接口监控、多步骤接口监控配置，具备创建编辑时接口监控任务的管控。

（2）接口监控概览：展示已创建的接口拨测任务数据传输的稳定性，反映当前业务应用性能趋势，包括响应时间、可用率趋势。提供单步骤拨测、多步骤拨测概览能力。

（3）自定义节点管理：具备自建新的拨测节点，快速建立分布于各网络分区、地理位置的服务质量监测点。

5、指标管理

需具备从地市－归属单位－业务系统角度切入，并筛选目标监控资源，具备自定义配置监控告警条件,将监控对象采集后未经计算的原始指标数据纳管至告警规则，需实现基础资源监控管理、基础资源监控任务管理、主机及数据库监控数据采集、中间件监控数据采集、主机监控数据分析、数据库监控数据分析、常用中间件监控数据分析、其他中间件监控数据分析、监控数据分析配置。

（1）告警记录：将告警事件在列表展示及具备查询告警事件。

（2）告警信息推送：提供将告警信息推送给事件处置中心的功能。

（3）告警事件详情：提供已触发告警事件的监控对象相关指标走势、流转记录，具备查看触发告警规则，具备手动停止本次告警。

（4）通用模板管理：提供通用模板管理页面，具备模板上传、手动更新、

详情查看、删除模板、下载模板功能。

6、全局规则设置

需具备对监控分值公式的参数进行查看，具备对参数列表进行编辑，实现定制化的健康度评估标准。全局设置需涵盖查看告警分值公式与参数列表、编辑模式、告警级别基准分值列表查询、修改告警级别基准分值、监控类型项权重列表查询、修改监控类型项权重、监控指标基准分值按指标名称列表查询、修改监控指标基准分值、查询文本说明、修改文本说明。

（五）业务性能监控中心

1、应用端性能

业务性能监控中心的应用端需提供面向应用的性能管理整体解决方案，包含应用拓扑图以及代码层事物追踪等功能。应用端整合了真实用户的前端请求动作并从宏观视角分析系统运行的整体状态，同时从前端到后端细化追踪和分析代码堆栈和数据库，能精确到单条 SQL 的执行性能。主要功能包括：

（1）服务列表：展示服务的基本信息和运行状态，包括服务名称/服务别名、主机数、运行情况、响应时间、每分钟请求数、错误率和错误数。

（2）概览：点击对应按钮可以查看概览页面。

（3）拓扑图：展示当前应用及其关联应用的整体状态、请求数、响应时间以及错误异常的变化趋势。

（4）请求分析：通过响应时间和请求数的变化趋势图，展示响应时间正常、缓慢、非常慢和错误四类请求的变化及所有请求的平均响应时间变化，分析需要关注的请求。

（5）单个请求分析：通过响应时间和请求数的变化趋势图，展示单个请求响应时间正常、缓慢、非常慢和错误四类请求快照的变化及平均响应时间变化，分析需要关注的请求快照。

（6）单次请求快照分析：展示请求的基本信息和业务拓扑，发现潜在问题。展示请求的最慢元素。展示代码执行堆栈的详细树状信息，包括每个方法的总耗时、耗时占比、被调用次数。展示错误和异常信息的摘要列表。展示请求调用的外部服务信息，包括 API 接口、总耗时、调用次数等，api 必须具备与省上相关应用的对接。展示 HTTP 请求的参数名称和参数值。

（7）外部服务追踪：展示响应时间最长的 5 个外部服务及其响应时间变化趋势、吞吐率最大的 5 个外部服务及其吞吐率变化趋势、网络错误率最高的 5 个外部服务及其网络错误率变化趋势。展示外部服务性能分析，包括吞吐率及响应时间趋势、调用外部服务的事务耗时占比（最大的 5 个）及所有事务的响应时间占比、平均响应时间和访问次数。展示外部服务错误分析，包括发生次数最多的 5 个网络错误类型及其错误数变化趋势、错误列表。

（8）消息队列分析：展示代理服务器列表及所有代理服务器整体性能分析，包括 MQ 服务总耗时 TOP5、吞吐率及平均耗时、流量趋势。具备按平均耗时、消息总数、每分钟消息数、总流量、每分钟流量来查看代理服务器。

（9）数据库详情追踪：展示在不同数据库表中执行 SQL 操作时，响应最慢的 5 个 SQL 操作。具备对单条 SQL 的追踪，包括执行计划和堆栈信息等。展示 SQL 操作列表中每个 SQL 操作的平均响应时间、执行次数、错误率、缓慢率、最大响应时间、数据库表名、TP99、吞吐率。展示连接池列表中数据库 URL 连接的最大活跃连接数、连接峰值、平均活跃连接数、平均空闲连接数、最大空闲连接数、最小空闲连接数、初始连接数和连接池实例。同时具备查看单条数据库连接的分位数变化趋势图，包括活跃连接数、最大空闲连接数、最大活跃连接数的分位数变化趋势图。

（10）NoSQL 详情追踪：展示数据库的整体性能分析，包括 SQL 操作的响应时间变化趋势和吞吐量变化趋势、调用者耗时占比及调用该数据库的方法列表。对数据库中单个 SQL 操作进行性能分析，包括 SQL 操作的耗时和执行次数对比分析、调用者耗时占比及执行该 SQL 操作的 Web 事务的详细列表。

（11）JVM 监控：展示主机、进程名称、进程路径、JVM 版本和启动时间。点击进程名称查看 JVM 的内存和线程运行情况。展示内存使用状态的概要信息、堆内存及非堆内存的使用情况、垃圾回收情况。展示线程数变化趋势、所有线程的运行状态及各性能指标数据。展示线程池容量的变化趋势、队列容量变化趋势、所有线程池的运行状态及各性能指标数据。

（12）错误&异常信息追踪：展示请求错误率和错误数变化趋势、调用者错误 Top5 占比、错误发生时间及详情。具备将错误一键加入白名单。展示请求异常率和异常数变化趋势、调用者异常 Top5 占比、异常发生时间及详情。具备将

异常一键加入白名单。

（13）对比分析：从时间或者实例的维度对比应用（默认为域名加端口）或应用下事务（显示为URI）的性能及错误异常数目的变化趋势。

（14）应用设置：设置拓扑图中应用不同状态的判断条件。设置请求不同状态的阈值。将请求URL与业务名称对应。开启获取请求参数后，探针采集请求参数并具备展示，关闭则不采集。开启添加端到端后，拓扑图展示具体调用者与被调用者的调用关系。设置判断后台任务执行缓慢、非常缓慢状态的阈值。将后台任务与业务关联。设置异常白名单，设置为白名单的异常将不被统计为异常。适用对象具备应用服务和请求URL。

（15）应用高级设置：设置HTTP状态码白名单，设置为白名单的HTTP状态码将不统计为错误，默认400以上为错误HTTP状态码。适用对象具备应用服务和请求URL。设置SQL执行不同状态的阈值。设置Agent采集数据的比例，即实际采集数据与全量数据之比，默认为100%。设置Agent熔断的触发条件，包括主机/容器CPU使用率、主机/容器内存使用率、GC CPU时间消耗占比及Heap内存使用率。设置Agent熔断恢复的触发条件，包括主机/容器CPU使用率、主机/容器内存使用率、CPU时间消耗占比。

（16）自定义报告配置：设置将报告以PDF格式定期通过邮件发送至运维人员。具备每日、每周、每月定时发送。

（17）自定义报告查看：具备每日、每周、每月定时发送。

（18）告警管理：展示移动、应用、Agent及浏览器的告警消息列表。具备将告警配置模板与告警对象进行关联，关联后透视宝将根据告警对象的运行状态和告警指标发送告警通知。具备向普通告警组和高级告警组发送告警通知，实现问题的升级与分级发送。

（19）探针管理：展示组件（也称探针或Agent）的运行信息，包括组件类型、版本、所属应用、所属实例、部署路径、使用状态（使用中、停用，或者无响应）、内存使用率、心跳上报时间、组件使用状态（在使用或者已弃用）、采样率等。具备启动单个探针（仅 Java Agent）与批量启动。启动后的探针占用配额，license校验熔断恢复，探针开始采集数据。具备暂停单个探针（仅Java Agent）与批量暂停。暂停后的探针释放配额，但会继续上报心跳，触发license

校验熔断，探针停止采集数据。具备启用已弃用的探针，由于探针无响应，启用后不会上报心跳。无响应的探针自动释放配额，并具备弃用，弃用后的探针将不再继续上报心跳。

（20）设置管理：设置请求响应时间，小于等于请求过滤时间的正常请求数据，Agent 不予采集。设置拓扑图中应用不同状态的判断条件。设置日志级别、数量和大小等。设置 SQL 执行不同状态的阈值。设置 Agent 采集数据的比例，即实际采集数据与全量数据之比，默认为 100%。

2、移动端性能

需具备对移动端应用的性能进行分析，具备提供 APP 应用名称、响应时间、HTTP 错误、网络失败、崩溃率、APP 应用得分、APP 应用状态等信息。主要功能包括 APP 应用列表、概览、行为分析、用户分析、页面分析、网络分析、指标趋势图、CDN 分析、启动分析、问题趋势分析、问题 TOPN 分析、错误趋势分析、错误 TOPN 分析、终端分析、设备 TOPN 分析、设备数据分析、设置。

3、浏览器端性能

需具备对浏览器性能进行监控，展示浏览器应用名称、响应时间、白屏时间、Ajax 错误率、js 错误率、浏览器应用得分、浏览器应用状态等信息。主要功能包括浏览器应用列表、概览、页面分析、错误分析、用户分析、Ajax 分析、终端分析、设置。

（六）日志管理中心

1、日志分组管理

日志分组需包含日志分组目录以及日志分组两部分内容，可以新建、查看、删除日志分组。主要功能包括：

（1）日志分组目录：日志分组包含日志分组目录以及日志分组两部分内容，定义了日志筛选和访问的条件，能够提高日志检索的效率，增加数据访问的安全性。

（2）日志分组：可以新建、查看、删除日志分组。

2、常用搜索

主要功能需包括：常用搜索分组列表，搜索、新建、修改、删除、导入、导出常用搜索分组。

3、脱敏设置

主要功能需包括：搜索、新建、编辑、删除、启用、停用脱敏规则。

4、日志搜索

需具备对采集日志按照条件、内容进行检索，具备按照日志分组、查询条件以及搜索时间范围来查询日志。主要功能包括：（1）条件筛选：需具备采集日志的全文检索，具备按照日志分组、查询条件以及搜索时间范围来查询日志。

（2）内容搜索：需具备采集日志的按照时间进行搜索，可以查看搜索记录并将搜索结果另存。

（3）常用搜索管理：需具备使用常用搜索快速创建搜索条件，减少反复输入的次数，节约时间。

5、日志事件分析

需提供双引擎查询、日志数据变化趋势图、日志分组展示、按照格式查看日志内容、展示日志全部字段以及对应的字段值、设置日志展开行数、启用分词查询。主要功能包括：

（1）原始日志列表：提供原始日志的查看检索。

（2）字段列表与关注字段列表：提供字段关注功能，方便用户跟踪感兴趣的字段。被关注的字段优先排列显示。

（3）字段管理：对日志采集过程中提取的关键字段进行管理。

（4）字段值过滤与屏蔽：提供日志提取字段的过滤和屏蔽检索能力。

（5）导出日志搜索结果：具备导出日志搜索结果

（6）日志上下文检索：提供日志上下文查看能力

（7）日志划词分析：具备直接在原始日志上进行划词分析。

（8）日志可视化分析：提供快速便捷的可视化分析界面，基于搜索结果和配置信息快速显示可视化分析的结果，可应用于日志统计分析以及日志分析成果展示等场景。基于搜索结果对指标进行统计并可视化。

（9）日志监控：日志监控模块具备日志监控规则的统一展示与管理，该模块具备单一日志监控规则的新建、编辑、启用、停止、删除、复制、搜索，也具备批量日志监控规则的启用和停止。

6、用户权限设置

需具备系统和统一认证平台对接，可同步用户、组织、权限等数据，实现单点登录。

（七）云原生管控中心

1、概览模块

需提供集群资源使用情况概览、组件状态、集群节点状态等信息展示。主要功能需包括：集群资源使用情况、组件状态、集群节点状态、配置文件、控制台。

2、节点管理

节点管理需展示集群所有节点的情况，包含节点数量、主节点数量、工作节点数量展示。集群中各个节点的 IP 地址、运行状态、CPU 使用率、内存使用率、容器组数量、已分配 CPU 以及已分配内存状态。同时具备控制集群节点功能，停止容器组向该节点调度，可以编辑节点的标签和污点。主要功能包括：

（1）节点管理：需具备查询集群节点、停止调度、污点管理、更新集群节点列表、查看集群节点详情。

（2）集群节点详情：需提供当前集群下节点的运行状态，以及可以编辑删除节点，提供集群节点的详情展示等功能。

（3）服务组件:需提供集群内各项服务组件的健康状态监控，可以查看当前集群的健康状态和运行时间，能够帮助用户监测集群的状况和及时定位问题。

3、项目管理

需具备查看集群中各类项目的情况，可以观察到项目名称、状态、CPU 使用量、内存使用量、容器组数量信息，可以进行项目的创建、编辑、删除操作。项目管理主要功能需包括：创建项目、编辑项目、查看项目、删除项目、获取项目配置、项目资源状态预览、查看容器组信息、查看网关信息、查看项目配额。

4、应用负载

需具备进行容器平台集群中各类应用负载的管理，包括工作负载、任务和定时任务都、容器组、服务、应用路由的管理，可以查看集群中上述工作负载的名称、状态、所在项目、更新时间等信息，同时具备对工作负载进行配置管理，可对工作负载进行弹性伸缩。主要功能包括：

（1）工作负载：需具备容器平台集群中各类应用负载的管理，包括工作负载、任务和定时任务都、容器组、服务、应用路由的管理，可以查看集群中上述

工作负载的名称、状态、所在项目、更新时间等信息。可以对上述工作负载进行创建、编辑、重启、删除等操作。

（2）工作负载：需具备对工作负载进行配置管理，可对工作负载进行弹性伸缩。

（3）负载配置：需具备对工作负载进行编辑、查看、删除等操作。

（4）任务管控：需具备管控的任务负责批量处理短暂的一次性任务，即仅执行一次的任务，它保证批处理任务的一个或多个容器组成功结束。

（5）定时任务管控：需具备提供管控定时任务管理基于时间的任务的能力。

（6）容器组管控：需具备对管控容器组应用程序的基本执行单元进行管控，具备创建或部署的对象模型中最小和最简单的单元。

（7）服务管控：需具备对容器组的逻辑集合和访问策略进行的管控。

（8）应用路由管控：需具备具备对应用路由提供的聚合服务的方式进行管控。

5、配置中心

需具备对容器平台中的密钥和静态配置进行管理，包括展示资源的名称、所属项目、资源类型、配置项数量、创建时间等信息。可以对上述资源进行编辑、创建、删除等操作。主要功能包括：

（1）密钥管控:需提供对密钥这种包含少量敏感信息的资源对象进行管控。

（2）静态配置:需提供对配置集此类常用于存储工作负载所需的配置信息进行管控，对配置文件、命令行参数或环境变量中的配置信息进行管控。

（3）热更新配置:需提供热更新配置能力。

（4）网络策略管理:需具备通过配置网络策略，允许在同个集群内实现网络的隔离，具备某些实例之间架起防火墙。

（5）自定义资源 CRD 管理:需具备对容器平台自定义资源进行管理，可以查看 CRD 资源的类型、名称、作用范围、创建时间信息。并且可以进一步查看该自定义资源的资源列表。

（6）邮件服务器管控:需具备为平台邮件发送服务提供设置。

（7）日志中心:需具备查看云原生管控中心内操作日志情况。

6、存储管理

需具备对容器平台的存储卷和存储类型进行管理，进本信息展示，创建和删除。主要功能包括：

（1）共享存储管理：

共享存储为容器平台的底层存储提供方，容器平台需具备通过存储类型进行网络存储绑定，然后通过控制器监听容器平台对该存储类型的请求，当有新的存储卷对该存储类型进行资源申请时，控制器会自动创建持久卷，并将持久卷与存储卷进行绑定，并在共享存储中创建相应分区。

（2）存储类型：需具备集群管理员配置存储服务端参数，并按类型提供存储给集群用户使用。

（八）流程服务中心

需具备对运维服务管理过程中的资源申请、资源变更、故障申报、告警处理等业务流程进行管理。

1、工单数据统计

需具备对总工单、我创建的、我相关的、我的待办、我已完成的工单统计数量的展示；近 7 天内超期工单、新增工单的数量展示，折线图展示；今日总工单、未处理工单、已处理工单的数量展示，按照平均处理耗时维度计算处理工单排行的榜单正序展示。主要功能包括：工单相关数据展示、工单超期、新增数量统计展示、工单办结率、SLA 数据统计展示。

2、工单处理工作台

需具备通过工作台创建、查看和处理工单，覆盖的工单种类包括变更、故障、发布等。具备基于历史工单来创建工单，实现工单的快速创建。主要功能包括：工单申请、我的待办工单、我创建的工单、编辑我创建的工单、我相关的、所有工单。

3、工单后台管理

需具备对不同属性的流程进行分类管理，方便申请工单选择对应分类流程，同时提供低代码创建模板的能力，通过创建模板字段信息完成对工单模板的创建，具备设置不同流程，满足对不同工单属性的流程自定义设置。主要功能包括：流程分类、模板管理、流程管理、任务管理、SLA 管理。

4、工单值班管理

需具备提供值班人员、班次管理、换班管理、值班管理以及值班统计等功能。主要功能包括：值班人员管理、班次管理、排班计划、值班统计。

5、问题库管理

需具备对问题库提供知识的统一创建、存储、检索和管理功能。问题库具备对主流的文件类型进行操作，具备上传、修改、查看和删除等功能，具备根据用户的权限提供不同的操作。主要功能包括：问题库、问题库编辑、问题分类、草稿箱。

6、系统权限配置管理

需具备对相关用户进行维护，可在处理工单时对用户进行指派或部门分配，具备对已创建的用户进行停用和启用，具备为不同角色设置不同权限，具备对用户分配角色、岗位、项目等，具备对短信条件及规则的设置，完成对短信通知的配置。主要功能包括：用户管理、角色管理、岗位管理、部门管理、项目管理、通知管理、菜单目录管理、菜单编辑、接口编辑。

7、系统设置管理

需具备收集不同用户的登录日志信息，对用户行为进行记录管理，具备对配置信息的设置，具备自定义修改系统信息，具备对个人信息的设置，维护管理个人基本信息和密码，具备设置工单通知消息，对相关处理人员下发处理消息。主要功能包括：登录日志、系统设置、个人信息、工单消息、全局搜索。

（九）运维管理系统

1、集中运维门户管理

需具备从后台调用卡片列表接口，前台展示。主要功能包括：

（1）门户应用卡片管理：需具备从后台调用卡片列表接口，前台展示。

（2）个人信息接口：需具备先调用个人信息接口，展示个人的详细信息，然后提供修改接口修改个人信息。

（3）密码接口：需提供修改密码接口。

（4）登录接口：需提供单点登录，登录一次，能进入展示的所有应用。

（5）版本信息：需具备获取门户里展示的所有应用的版本信息。

2、应用系统后台管理

需具备单点登录、接口调用权限管理，提供添加应用、单个删除应用、批量

删除应用、修改应用、搜索应用信息、搜索应用信息展示、重置搜索应用条件、开通应用、关闭应用等功能。主要功能包括：

（1）应用管理：具备单点登录、api 调用权限管理，提供添加应用、单个删除应用、批量删除应用、修改应用、搜索应用信息、搜索应用信息展示、重置搜索应用条件、开通应用、关闭应用等功能。api 必须具备与省上相关应用的对接。

（2）应用配置服务管理：需提供配置权限、应用配置信息调用、应用 URL 信息调用、开通服务、关闭服务等应用配置服务管理功能。

3、资源管理

需具备提供接口管理、菜单管理、按钮管理等功能，接口必须具备与省上相关应用的对接。主要功能为：

（1）接口管理：需具备对应用的接口进行统一管理维护，提供 api 接口供其他应用调用。api 必须具备与省上相关应用的对接。

（2）菜单管理：需具备对应用的菜单进行统一管理，实现不同角色拥有不同的菜单权限。

（3）按钮管理：需具备对应用的按钮进行统一管理，实现不同角色有不同的按钮权限。

4、用户权限配置管理

需具备提供组织管理、用户管理、角色管理等功能。实现用户的创建、角色的赋予，用户数据权限管理，组织关系维护等管理功能，主要功能为：

（1）组织管理：需具备根据业务系统和组织架构关系对组织集中管理。

（2）用户添加管理：需具备具备对用户进行增删改，提供分配组织、分配角色，重置密码功能。

（3）用户角色配置：需具备对应用角色进行自定义设置，具备角色绑定菜单资源。

（4）用户信息查询：需具备用户信息根据需要自行查询信息。

（5）角色管理：需具备对用户分配不同角色来实现用户与菜单资源的绑定关系。

5、安全管理

需具备对应用私钥进行修改；具备对私钥进行配置实现单点登录。主要功能包括：

（1）修改密码：需具备对应用角色进行自定义设置，具备角色绑定菜单资源，具备对用户分配不同角色来实现用户与菜单资源的绑定关系。

（2）证书管理：需具备对应用私钥进行修改；具备对私钥进行配置实现单点登录。

6、用户审计管理

需具备对用户的操作行为进行记录，可对用户的操作记录及行为溯源，强化对用户操作行为的管理。主要功能包括：

（1）用户轨迹管理：需具备记录用户在系统上的操作行为。

（2）记录用户轨迹状态：需具备记录用户一系列操作的轨迹。

7、系统设置管理

需具备自定义修改系统图标、系统名称等系统信息，具备对系统信息进行重置设置。提供个人信息修改入口。具备面向平台管理员的管理/维护功能。主要功能包括：

（1）系统信息设置：需具备自定义修改系统图标、LOGO、系统名称等系统信息，具备对系统信息进行重置设置。

（2）个人设置：需具备个人信息修改入口，可修改个人信息、重置个人信息。

（3）全局设置：需具备面向平台管理员的管理/维护功能，可修改全局入口。

2．政务云运维平台

具体技术（参数）要求
政务云运维平台 政务云运维平台应对市政务云浪潮节点、移动节点、电信节点、联通节点、自主可控平台、异地灾备平台等 6 个市级平台进行统一管理，与黑龙江省多云纳管平台对接，实现与省多云纳管平台政务云资源数据交互。系统实现多家云厂商多种云计算资源的集中管理，从监控、成本、运维、云资源全生命周期等多个维度提供统一运维管控，从而进行灵活的资源管理与运维。哈尔滨市云基础设施运

维管理系统应实现全市政务云资源管理，规范应用系统上云业务流程，按政务云资源实际使用量计费，提供政务云资源运维服务功能，对政务云服务商服务能力和服务质量等进行监测和评价，通过对政务云资源的多维度数据分析为管理层决策提供数据支撑。系统建设内容包括统一门户、运营管理、运维管理、统计报表、数据可视化、服务商能力考核、权限管理、全市云平台纳管接口适配、数据共享接口、服务治理等功能。

（一）统一门户

统一门户对全市使用单位、云服务商、云管理工作人员通过统一门户使用系统，根据登录用户的角色显示相应的功能。

1、市级管理用户中心

通过图形、表格、文字等不同形式，展示市政务云浪潮节点、移动节点、电信节点、联通节点提供的政务云资源情况，主要包括数据汇聚情况，数据处理情况，云资源使用及安全状况，提供云内资源的资源数量统计、资源配置统计、资源统计、工单统计、告警情况统计、费用统计等。

2、云使用单位服务中心

云使用单位是全市各委办局，是政务云资源的使用者，云使用单位通过订单管理，资源使用情况查看，费用情况查看：消息管理，工单查看，服务商考核打分，各类综合信息报表查看等。

订单管理：申请的资源经过评审后在服务目录中选择资源，发起采购流程形成订单。可以在订单管理位置对采购的信息进行管理。

运维工单：云资源有问题时，云使用单位可以通过运维工单发起运维工作，运维人员将工单转到对应的服务商进行处理。

费用中心：云使用单位能够通过费用中心查看本单位使用系统的计费情况。

消息中心：主要是云使用单位接收系统推送的订单消息，费用消息，服务考核消息等。

服务考核：云使用单位需要对提供云资源的服务商按周期进行考核，根据服务考核的指标给服务商打分。

云资源情况：首页展示云使用单位的整体资源情况，云使用单位可以通过云服务功能模块查看云资源详细情况。

3、云服务商服务中心

云服务商服务中心需为全市云服务商提供功能模块，通过订单管理实现云使用单位订购资源配置，工单处理，费用查看，资源情况查看等功能实现云资源的运维和运营。

订单管理：需在订单管理功能模块中云服务商需要对交付的资源信息进行补充，云服务商根据云使用单位订购的服务内容交付相应的资源信息，填写资源id进行交付提交。

工单管理：需满足云服务商用户使用运维工单功能，在待办列表中查看需要处理的工单信息内容，点击详情查看问题：处理完成问题确认后归档数据，完成本次工单反馈流程。

费用中心：需满足云服务商可以查看所有交付完成已经产生的计费情况。

通知中心：需满足云服务商在通知中心模块查看系统发送的系统消息和问题通知。

云服务：需满足云服务商通过云服务功能查看自己所提供的资源情况，包括各单位资源配置情况等信息。首页展示各类资源整体情况。

4、工作人员服务中心

云服务：需展示全市各服务商云平台基础业务模块数据的功能。通过将云平台中的基础架构资源（包括计算与存储、网络与安全）组成虚拟资源池，系统通过资源同步数据接口掌握每个业务模块的数据情况，提供展示云平台的基础资源使用情况，从而达到对云平台的资源进行监控。

订单管理：需满足管理人员通过订单管理可以查看所有购买流程记录及详情。

费用中心：需满足管理人员通过费用中心模块管理云服务商提供资源的计费情况，包括市级各单位资源费用情况，按月出账的费用情况，计费报表等。

运维工单：需满足管理人员通过运维工单模块查看各服务商各种别的运维工单和所有反馈的工单情况。

通知中心：需满足管理人员能够在系统中指定组织下的所有用户发送通知消息。填写消息标题、消息内容、选择接受组织人员可以暂时保存也可以直接发送消息内容。

（五）运营管理

运营管理是对政务云资源申请、云资源订单、云资源计费等政务云业务进行管理的功能。通过该功能模块完成云使用单位上云申请、变更、续约等上云业务，完成云资源订单、云资源计费出账业务，并对云使用单位纳管的信息进行管理等。云服务商通过运营管理完成订单配置等工作，建立政务云资源与上云单位和上云应用系统的关系，实现政务云资源的分配。

哈尔滨市云基础设施运维管理系统的运营管理功能模块是业务办理的核心部分，只适用于哈尔滨市云基础设施运维管理系统。

1、基础信息管理

纳管基础信息管理是基础设置部分，通过对服务商和服务目录的设置实现云服务商和其提供的资源的管理。

服务类型，需对采购的服务目录中的资源类型进行管理，资源以目录树的形式实现，可以在大类下添加小类。

服务管理：需对服务类型下的所有资源信息进行管理，按照服务商，服务类型添加服务信息，并可对资源信息进行修改和删除等操作。

服务标签：需对服务目录中的所有资源的属性进行管理，通过管理云资源的属性，可以在购买，订单等界面增加产品属性信息，实现资源的精准查询。

云服务类型管理：系统需对云服务商进行管理。对云服务商的政务云提供的政务外网区域，互联网区域的资源进行区分管理。

2、云资源申请管理

云资源申请管理：云资源申请管理主要是需满足云使用单位申请资源时需要填报相关信息并按照规定的流程进行资源审批，适用于新系统上云和旧系统迁移上云的需求。

云资源变更管理：云资源变更管理主要需满足针对云使用单位的系统在实际使用过程中发现资源不能满足需求或者资源闲置，这时云使用单位可通过资源变更申请修改系统资源，达到系统使用要求。

云资源退出管理：云资源退出管理主要需满足针对云使用单位的业务系统根据实际需要存在系统合并，业务撤并的情况，使用单位可根据实际情况退出云资源的使用。

云资源方案评估管理：市大数据中心受理和审核使用部门的政务云资源需求，组织第方评审机构对上云方案进行论证。为保证论证工作顺利开展，使用部门应按照市务大数据中心提供的模板编制上云方案。

云资源备案管理：需满足云使用单位系统部署、测试通过后，需要将服务合同、测试报告和安全风险评估报告报送市大数据中心备案。系统将云使用单位的系统合同等信息在系统中做备案记录管理。

3、资源订单管理

需满足云使用单位通过资源订单申请资源，云服务商按申请配置并开通资源，计费系统根据云使用单位申请的资源数量和计费规则进行计费。资源订单随变更流程自动生成和流转。

4、账单管理

管理账单，需为政务云管理单位提供所有云使用单位、云服务商、云平台的计费数据。

服务商账单，为政务云服务商生成账单，账单内容包括结算周期内服务商为云使用单位开通的资源清单和计费数据。

云使用单位账单，需为云使用单位生成账单，账单内容包括计费周期内本单位各应用系统使用的资源清单和计费数据。可以查询所有开通的应用计费情况。

5、资源管理

资源配置监控：需满足监控各云使用单位云资源的配置信息。采集并展示各云使用单位已配置资源和设备，从整体视角、云使用单位视角、应用视角等维度展示资源配置信息。

资源异常监控：需满足针对申请资源与云服务商已提供资源进行核查，核查确定两类信息是否正确匹配，给出详细匹配信息和统计数据，提供不匹配信息的信息和数据。

资源运行监控：需满足对基础设施和承载的各类虚拟资源的运行状态进行监控，主要包括云平台监控、云资源池监控、服务器监控、存储设备监控、云主机监控、云硬盘监控等。

（六）运维管理

需提升运维管理能力，面向全市云管理工作人员、全市云使用单位云服务商

提供运维管理功能。

1、工单管理

需满足云使用单位通过工单反映云服务故障或安全事件，具备工单审批、工单流转和状态跟踪，可对工单流转状态查看。实现工单提交处理流程的闭环管理。

2、告警管理

需满足采集服务资源出现异常时告警信息，资源告警的对象包括服务器、存储设备、网络设备等物理设备和云主机、云硬盘等云资源。

3、消息管理

需满足调用共性应用支撑能力建设中的“统一短信”接口，提供日常的消息管理，对云平台资源、物理设备、虚拟资源巡检变化信息，在消息模块里推送变化结果。

4、运维台账管理

对所有服务资源进行管理，首要的是建立哈尔滨市云基础设施运维管理系统的服务资源台账，包括多哈尔滨市云基础设施运维管理系统所使用的云资源、软件资源、网络资源以及各种应用服务。台账内容包括资源标识、资源名称、规格型号、位置、来源、用途、入账日期、使用年限、报废日期、当前状态、责任人等。

5、运维人员管理

对哈尔滨市云基础设施运维管理系统运维的人员进行管理，包括运维人员的增删改查，运维人员的排班管理，领班人员管理，值班管理，调班管理等。

6、考核管理

对运维人员的工作进行考核，根据运维人员的具体工作情况，对运维人员的工作进行考核，评定考核结果，可按照 A、B、C、D、E 以下进行分级考核；可以设定考核指标，在每个评定周期进行考核，提供考核结果查询功能。

7、运维档案管理

需满足对运维工作中产生的文件、文档、方案、音频、视频资料进行管理，包括档案索引管理、档案管理包括档案配置功能、档案管理业务功能、安全管理功能、系统管理功能对电子文件管理系统的基本功能进行划分。其中，档案管理配置功能是电子文件管理中建立和维护文件管理业务规范的功能，包括分类方

案、保管期限与处置表、文件类型等内容；文件管理业务功能主要基于电子文件管理业务流程展开，包括捕获登记、分类组织、鉴定处置、统计管理、存储保管、检索利用等内容；安全管理功能是保护电子文件以及电子文件管理系统安全的功能；系统管理功能是指电子文件管理系统运行所需要的基本环境支撑、工具支撑等内容。具体应包括：文件档案管理配置、档案管理、档案归档、档案调阅、档案借阅、档案质检、档案借阅审批、借阅记录查询。

8、运维知识管理

运维知识管理应包括：运维知识库目录管理、运维知识库内容管理、知识智能搜索和推荐、智能搜索和推荐算法的学习、智能搜索关系管理功能。

9、故障管理

需满足对运维工作中发生的故障进行管理，记录故障发生的时间、故障类型、故障详细信息。

10、绩效管理

需满足对运维人员的绩效进行管理，包括根据每个周期考核的指标评定每个运维人员的绩效。

（七）统计报表

统计报表为政务云管理单位提供各单位相关业务报表数据信息，不同的权限用户登录后查看所属单位的相关数据。

1、基本情况报表

基本情况报表用于统计登录用户本区域系统的基础信息，便于区域管理工作人员掌握的区域情况。

2、上云管理报表

上云申请报表，统计区域云使用单位上云申请信息，统计条件包括上云申请状态、申请时间、申请云服务商等。结果信息展示上云单位名称、应用系统名称、当前环节、申请时间等信息并能导出 excel。

3、计费报表

账期总报表，统计区域账期内费用信息，可根据年份、月份、地区等条件筛选，并能导出 excel。

4、工单报表

工单总量报表：统计区域工单总量情况，可根据年度、月份、地区等条件进行条件检索并导出 excel。

工单分类报表：统计区域不同工单的总量情况，可根据年度、月份、地区等条件进行条件检索并导出 excel。

服务商工单报表：统计区域云服务商工单总量情况，并可根据年度、月份等条件进行条件检索并导出 excel。

云使用单位工单报表：统计区域云使用单位工单总量情况，并可根据年度、月份等条件进行条件检索并导出 excel。

工单处理状态报表：统计区域所有工单的处理状态情况，可根据年度、月份、地区等条件进行条件检索并导出 excel。

5、资源报表

云资源是系统管理的主要内容，需要对区域云服务商已经提供的云资源进行多维度的分析，为管理提供依据。

6、服务商能力报表

提供服务商能力报表，系统对服务商的考核情况进行统计分析，分析内容包括当期考核和往期考核的数据，便于管理层全面掌握云服务商的考核情况。

（八）数据可视化

提供区域数据可视化功能，全面监测政务云节点的整体运行情况和业务办理情况。通过使用动态图形、动态图表、动画、视频等方式实现对各政务云节点资源使用率、云服务商服务能力、整体上云情况和服务质量的全面管理展示。

1、区域政务云整体情况

主要提供对区域政务云整体情况可视化展示。需满足包括区域政务云整体资源情况（cpu 总量、内存总量、存储总量）展示、每个云服务商整体资源情况展示、整体基础资源信息（计算、存储、网络、安全）展示、区域政务云服务目录信息展示、每个云服务商系统上云数量趋势展示、上云单位及上云系统整体进度展示、区域政务云运维管理（告警、工单、考核、订购）情况展示。

2、区域政务云服务商情况

主要提供对区域政务云的云服务商情况可视化展示。需满足包括多家云服务商的整体资源情况、不同网络区域资源情况的动态展示、多家云服务商基础资源

（计算、存储、网络、安全）信息展示、多家云服务商 cpu、内存、存储使用率展示、云服务商机房动环数据展示、云服务商机房视频影像实时展示。

3、区域政务云上云部门情况

主要提供对区域政务云的上云单位系统信息的可视化展示。需满足包括区域上云单位系统进度信息的展示、区域上云单位整体数量排行榜展示、上云系统数据排行榜展示、上云系统基础资源信息展示、上云系统资源使用率情况展示、上云系统计费情况展示等内容。

4、区域政务云运维管理情况

主要提供对区域政务云的运维监测情况可视化展示。主要包括整体费用展示、整体工单量展示、整体服务考核量展示、整体告警总量展示、各个云服务商每月计费趋势情况展示、各个云服务商工单处理量排行展示、各个服务商云平台告警级别分类总量展示、各个云服务商云平台告警信息详情滚动展示等。

（九）服务商能力考核

对全市云服务商的评估考核功能进行升级，增加功能如下：

1、考核模板管理

评估方案管理：对云服务商的评估考核的依据是云服务商评估考核方案，考核方案规定了评估的方式和方法，每期考核都要有对应的考核方案。对评估方案的管理包括评估方案名称，依据来源，年份，是否有效等信息，当方案变更时可通过方案复制建立新的方案，对方案指标进行修改即可。

评估指标管理：评估方案中的评估内容进行管理，评估内容包括评估类型，评分指标。每个方案对应若干类型和指标。类型和指标与方案对应，方案失效后指标跟随失效，有效的方案中评估类型和评估指标不能进行修改和删除。

2、考核配置管理

启动考核，新建考核表，为云服务商每家按照考核方案建立考核表，考核表建立后进行本期考核的参数设置。

3、填报考核表

需满足在考核云服务商时考核主体包括云使用单位和云管理单位，其中云使用单位是使用了云服务商提供资源的单位，所以一个云使用单位每期填报的考核表是根据其使用的资源所属服务商填报，若一个云使用单位同时使用多家云服务

商提供的资源，则需要同时对多家服务商进行考核。云管理单位需要按照要求同时填报云服务商的考核表。

4、往期考核表

需满足主要查看每期已填报的考核表情况，云使用单位可根据云服务商，考核期次等条件查看自己填报过的考核表。大数据中心用户可查看全部云使用单位填报的考核表信息，并按照条件进行检索。

5、考核报告

需满足当期考核报告，按照考核报告的标准模板生成本期对云服务商的考核报告。

往期考核报告，所有考核报告的列表信息，能够按照条件查询考核报考，并展示报告的详细信息。

（十）权限管理

权限管理需市级组织机构和流程等内容。升级后满足全市管理单位、云服务商、云使用单位的需要

权限管理使用本系统的单位、用户管理，根据工作内容建立不同的角色并分配不同的工作权限。对操作过本系统的日志等信息进行管理。

1、流程管理

流程管理主要需满足对云服务业务事件/故障管理，具体流程包括填写工单、呼叫中心、上云流程，应包含如下功能：基本信息管理、环节管理、属性配置、流程引擎。

2、区划管理

需满足实现对区划进行管理，区划管理是区分用户使用系统权限的关键信息。是每个使用系统用户的基本属性。对区划进行增删改查等操作。删除为逻辑删除。

3、部门管理

需满足每个区划下的部门管理，部门管理功能下需要选择区划，不同区划的部门信息进行管理，能够根据需要在所属区划下进行增加、删除、修改和查询部门信息。区划用树形结构展示，每个区划节点展示该区划下的所属部门。

4、用户管理

需满足具备对已注册用户账号的管理，管理员可以查看，修改和删除已注册的账号，该部分作为用户登录的基础信息，对角色权限的管理起着至关重要的作用。

5、角色管理

角色管理主要是对已注册用户的角色、权限进行管理，通过用户的角色管理，可以实现对不同的用户显示不同的信息、不同的模块功能，实现信息的分等级、分权限管理。

6、日志管理

日志管理模块主要是对系统运行日志的管理。系统运行日志不但记录网站各服务程序主要操作日志记录而且为系统管理员提供综合查询功能，如系统登录、操作、警告、错误信息的查询，可以通过记录准确定位到异常位置和问题原因，便于系统管理员及早发现异常状况，及时进行处理。

7、目录管理

目录管理主要是对功能目录进行管理，系统管理员可以通过目录管理对功能模块的显示位置及名称进行设置，同时可以实现功能目录的增加、修改、删除等操作，方便进行个性化设置。

8、字典管理

数据字典用于定义各项业务的专用名词，在数据字典中罗列了各项名词的信息项，例如“部门级别”在数据字典中则对应为“市级”、“县级”等，数据字典主要分为基础数据字典和业务代码字典。

9、接口权限管理

市级政务云平台与市政务云浪潮节点、移动节点、电信节点、联通节点都需要纳入系统进行管理，需要对纳入管理的接口类型、所属云服务商、对接权限信息进行管理，通过相关信息管理和权限配置，在适配时进行控制。具体包括：接口类型管理、云服务商管理、对接云平台信息管理、对接管理、授权管理。

（十一）全市云平台纳管接口适配

哈尔滨市云基础设施运维管理系统通过接口标准规范与全市政务云浪潮节点、移动节点、电信节点、联通节点对接，实现统一管理，一方面在计算资源、存储资源、网络资源、安全资源等资源层面实现无缝监控；另一方面做到用户权

限统一管理，资源申请和变更，资源质量统一评估优化。

1、系统对接设计

具体应包括：对接方式、接口规范设计、数据管理、完整性管理、接口双方责任、接口可扩展性规划与设计、接口安全性设计。

2、接口适配开发

具体包括：接口对接规划、接口步骤、资源同步接口、消息通知接口、资源监控告警接口、资源性能监控接口、云间安全控制接口、资源操作接口、接口适配内容、视频接入开发。

3、视频接入开发

系统接入各家服务商云服务资源机房的实时画面，根据各家实际情况分别接入视频信息。

4、机房动环数据接口开发

系统接入全市各云平台机房的动环数据，通过动环数据监测云平台的实时运行环境。

5、短信接口开发

系统需要调用云服务商短信平台的短信发送服务，并通过定制改造的方式，让系统与云服务商短信平台完成适配。

6、统一安全纳管适配

根据安全系统的要求和标准，对数据脱敏系统、4A 应用认证管控系统、密码管理系统等模块进行接口对接和适配，配合做好联调联试工作，确保应用系统自身被纳入一体化安全管理体系，并保证接口稳定可靠工作。

7、异构云平台纳管方案

政务云浪潮节点、移动节点、电信节点、联通节点、自主可控平台、异地灾备平台及市级政务云服务商提供的云平台各有不同，需要对全市异构云平台的云服务资源进行纳管。

（十二）数据共享接口

对全市政务云资源数据和业务数据共享，建立共享规范，按照规范建立与第三方监管单位数据共享机制，依申请提供政务云云资源和业务信息。数据共享接口能够实现哈尔滨市云基础设施运维管理系统与省多云纳管平台对接，使黑龙江

省级能够掌握哈尔滨市级云平台各类情况。

1、接口总体设计要求

系统作为市级政务云资源的集中监控管理系统，获取底层的计算资源池、存储资源池、网络资源池和安全资源池信息。

当同一套资源池同时与系统进行对接时，必须能够通过配置管理实现资源的有效控制，在同一时间段，不能将相同的物理资源同时分给两个地区系统。从而确保各个系统各自数据的稳定性和安全性。

2、对接接口范围

为了保证系统对全市及市级政务云资源进行有效的管理，哈尔滨市云基础设施运维管理系统与其他系统按需要从以下方面接口实现对接：计算服务方面、存储服务方面、网络与安全服务方面、资源编排方面、组织用户方面。

3、接口总体规划

系统对接采用Https，返回的数据结果封装为json格式，接口统一采用utf-8编码格式，字段名统一为驼峰式，方便解析值可以为空的字段，用“”代替 null，请求返回状态码需要遵循 RFC2616,RFC2518,RFC2817 等相关规范的定义及扩展。

4、接口设计

包括：政务云服务目录接口、全市资源监控告警数据接口、全市消息通知数据接口、全市资源性能监控数据接口、全市资源操作数据接口、全市安全运维数据接口

5、接口说明

包括：云服务商纳管接口、云主机相关接口、云硬盘相关接口、云主机快照相关接口、云主机快照相关接口、云硬盘快照相关接口、虚拟网卡相关接口、密钥对相关接口、镜像相关接口、裸金属相关接口、VPC 相关接口、网络相关接口、负载均衡相关接口、弹性公网 IP 相关接口、公网 IP 地址池相关接口、防火墙相关接口、防火墙规则及相关接口、防火墙规则相关接口、安全组相关接口、纳管云资源统计、告警资源统计

（十三）服务治理

1、服务注册与发现

微服务列表管理服务注册中心，可以查看注册服务的实例信息、环境信息、

日志信息、监控、配置等。只需要在代码中引用注册中心即可实现自动注册，并可以在微服务列表设置服务是否允许发现或隐藏。如果需要使用一些非微服务化常规服务，可以使用手动注册功能将其添加到注册中心，实现服务发现。

2、配置中心

配置中心就是一种统一管理各种应用配置的基础服务组件。配置中心用于配置的管理和下发，可为用户程序提供配置查询、存储等服务，统一管理配置。配置中心使用 SpringCloud 的分布式配置管理方案,既包含了服务端 ConfigServer 也包含了客户端 ConfigClient。配置文件被当作源代码一样管理，保存在代码仓库中，如 Gitlab，通过 push 触发更新操作。配置文件与实例的关联依赖于定义配置文件路径。

3、服务调用链

微服务架构解决了很多单体应用带来的问题，但同时也需要付出额外的代价。由于网络的不稳定性带来的请求处理延迟就是代价之一。另外，随着业务的扩展服务增多，很难洞察数据如何在蛛网般复杂的服务结构中流转。因此引入服务调用链来跟踪服务调用关系。

4、路由管理

微服务路由设计是一种透明化路由，消费者只知道当前服务者提供了哪些方法，并不知道服务具体在什么位置。服务提供者将需要发布的服务地址信息和属性列表写入注册中心，消费者根据本地引用的接口名称等信息从注册中心获取服务提供者列表。容器化部署无需考虑服务地址变更问题，所以路由规则主要用于 URL 精细化操作及失败重试。路由策略可应用于 AB 测试场景和新版本的灰度升级，主要通过路由规则来根据请求的来源、目标服务、Http Header 及权重将服务访问请求分发到不同版本的微服务实例中。

5、服务限流

由于业务系统负载能力有限，为了防止非预期的请求对系统压力过大而拖垮业务应用系统，所以要进行服务限流。系统具备 user、url、origin 三种限流方式，用户可以通过配置限流策略限制 consumer 端的请求频率，保证服务负载在正常可预期范围内。user 和 url 是从 Consumer 端限制请求指定服务的频率；origin 是根据 consumer 端的 IP 或域名限流。

6、熔断与降级

熔断，就是断开与服务器的连接，熔断器是在服务不可用的时候主动断开，以免造成更多的雪崩效应，是保护服务高可用的最后一道防线。为保证服务高可用，最先想到的是服务集群，但集群并不能完全地保证服务高可用，当某个服务出现故障时，在负载均衡的时候可能多次被调用到，调用方由于无法得到调用结果，会出现请求超时或其他异常，这时候如果不及时的熔断服务，就有可能会有更多的调用者去调用已经出现故障的服务节点，造成大量调用失败，甚至引发联级故障的雪崩。

7、认证与鉴权

服务访问控制和安全方案基于 Spring Cloud Security，具备基于 OAuth2 和 OpenID 协议的可配置的单点登录机制。Spring Cloud 通过 OAuth2 来实现多个微服务的统一认证授权，通过向 OAuth 服务发送某个类型的 grant type 进行集中认证和授权，从而获得 access_token，而这个 token 是受其他微服务信任的，在后续的访问可以通过 access_token 来进行，从而实现了微服务的统一认证授权。

8、负载均衡

接口服务需要保证可靠性和稳定性，在各种异常情况下都能够访问到接口，上报数据，通过配置客户端的负载均衡算法和服务调用，提供一系列完善的配置项如连接超时，重试等。

（八）一体化安全运营（管理）中心建设

具体技术（参数）要求
一体化安全运营（管理）中心建设 建设安全运营中心、政务外网安全监测平台、业务应用安全、密码安全，落实数字政府安全管理制度要求，强化安全管理责任，构筑全方位、多层级防护体系，保障数字政府基础设施和信息系统平稳、高效、安全运转。 一、安全运营中心 （一）基础要求 安全运营中心实现安全事件的自动分析和处置，再通过引入专业的安全服务

人员构建层次分明分工合理的安全运营服务团队;制定相关的运营流程并提供不同维度的运营服务，提升集群的威胁识别、安全监测、安全响应、协同处置的运营能力，持续平台业务的安全运行。

1、安全监测能力

包括资产测绘、漏洞发现、配置基线核查、深度威胁检测、恶意代码检测、情报关联分析、漏洞关联分析、恶意程序传播分析、外部恶意访问关联 9 项子能力建设。

2、大数据分析能力

包括批处理框架、流处理框架离线计算、批流一体计算、图计算、AI 计算 6 项子能力建设。

3、网络攻击分析能力

网络攻击分析模块具备对常见网络攻击总体情况的统计，分析当前网络攻击情况的趋势变化。进行 Web 或端口的恶意扫描、密码爆破、输入攻击、Webshell 攻击、跨站攻击、CC 攻击等 WEB 攻击行为总体情况的统计。包括高危资产识别、高危网络行为分析、攻击画像、网络攻击调查、历史高危攻击回溯、用户实体行为分析、风险隐患分析能力、流量关联分析、互联网暴露端口巡检、WEB 站点巡检、热点漏洞风险排查、弱口令风险检测、漏洞特征库管理等子能力建设。

4、溯源研判能力

包括原始日志检索、威胁告警调查取证、资产分析、业务分析、IP 分析、威胁透视等子能力建设。

5、AI 安全建模能力

提供集中的安全规则、模型以及策略的管理功能，制订统一的安全策略，并有效贯彻执行这些安全策略，不仅有助于提高安全水平，而且将这些安全策略进行上网发布也有助于知识的共享，让各级安全管理人员合理运用安全策略，有效地管理网络，保障网络的安全运行。因此，安全策略管理模块将负责全网的基本网络安全策略模板的制订，并将安全策略转换为可执行的脚本，便于安全策略的有效执行和快速部署。

主要提供规则建模、安全事件关联建模、安全事件统计建模、威胁情报建模和 AI 学习建模等分析建模方式，利用分析引擎进行数据深入分析，提升安全威

胁检测准确率。

6、安全联动能力

通过将各个厂商提供的不同设备所具有的不同网络安全能力集中起来，做到可以按照全链路平台规定的统一规则自由添加设备，并且被调用后能统一输出结果。包含挖矿处置、钓鱼邮件告警处置、僵木蠕毒处置、Webshell 处置、漏洞利用处置、异常登录处置、内网主机攻击事件调查联、动响应管理等子能力建设。

7、安全能力管理

包含能力编排、能力调度、策略管理、策略下发、场景管理、接口管理等子能力建设。

（二）具体要求

1、基础功能

（1） 具备通过单位维度、区域维度和支撑机构维度对平台用户信息进行管理，持续监控用户的访问时间、客户端信息、登录途径和使用习惯，具备对异常访问对用户账号进行锁定和强制下线操作。

（2） 具备快速导入用户清单开通账号和复制以创建的用户角色，用户信息包含用户账号、头像、真实姓名、邮箱、电话、归属单位、角色、标签等。

（3） 具备多级用户管理，授权下级用户管理员管理下级组织成员的账号开通、注销、功能和数据权限。

（4） 具备精细化控制功能权限，包括新增、删除、导入、导出等操作项级别。

（5） 具备多租户模式，每个组织只能看到归属于本组织的资产信息、安全事件、风险隐患、通报预警和安全态势。

（6） 具备通过设置数据隔离条件实现数据按照单位、地区、行业隔离存储，数据隔离条件具备与、或、非、In、Not In、exist、包含等方式灵活组合。

（7） 具备限制某个用户账号只能访问指定地区、指定行业或指定的多个单位的数据。

（8） 具备一体化系统管理功能，包括运维管理、配置管理、系统管理、分级管理、任务管理、数据管理、业务管理等业务模块。

（9） 原生防暴力破解能力，具备设置登录失败用户自动锁定策略。

（10） 原生防弱口令能力，具备设置密码强度和复杂度策略。

（11） 原生防屏幕拍照截图泄露信息能力，具备设置开启屏幕水印策略。

（12） 软件需具备国产主流硬件平台，兼容国产主流操作系统。

2、资管中心

（1）平台具备完整的资产管理功能，包括资产的录入、批量导入、管理等功能，并以多种可视化方式进行展示。

（2）具备按资产重要程度、资产区域和组织架构将资产分级分类管理。

（3）具备关基资产和重点资产一键配置，迅速将资产进行分类标记。

（4）具备资产档案管理、编辑、删除功能。

（5）具备资产与地图、风险、攻击打通，图上遍历资产情况。

（6）需提供完整的单位管理解决方案，可以直观、清晰、便捷的完成单位资产录入、资产概况总览和细分单位管理。

（7）单位资产搜索，具备通过单位名称、单位行业、单位类型、单位标签、单位简称、单位状态、联系人、备案号等信息进行单位资产检索。

（8）平台具备不低于 40 种单位行业属性标签，不低于 20 种单位类型属性标签，并具备多属性标签联合检索。

（9）单位资产信息概览，具备根据类型统计单位资产信息，包括但不限于单位总数、风险单位个数、风险单位行业分布和风险单位排名。

（10）具备在单位卡片中查看单位近期发生的安全事件和风险隐患信息，一键展开事件详情进行研判处置。

（11）需提供完整的系统管理解决方案，可以直观、清晰、便捷的完成系统资产录入、系统概况总览和细分系统管理。

（12）系统资产搜索，平台具备通过单位名称、系统域名、风险系统、系统名称、系统类型、系统标签、系统 IP、服务组件等信息进行系统资产检索。

（13）平台具备不低于 4 种系统风险标签，不低于 20 种系统属性标签，不低于 4 种系统类型标签，并具备多属性标签联合检索。

（14）系统信息概览，系统根据风险等级进行风险概况查看和风险变化趋势查看。

（15）依据等保和关保制度对单位信息展示要求，具备卡片式、缩略图方式

展示系统资产信息，展示内容包括系统名称、官网 IP、详细地址、安全事件、网络攻击、风险隐患等。

（16）具备系统资产标签展示，标签类型包括：系统属性标签、系统风险标签。

（17）具备系统便捷管理功能，包括系统档案查看、系统信息编辑、系统删除、快速扫描功能。

（18）具备系统画像快速浏览，信息至少包括系统信息、安全监测、防护情况、供应链、基础网络、人员信息、单位信息、档案时光轴等字段。

（19）具备系统档案模块与实时检测模块、分析研判模块联动，预见定位系统风险并进行分析研判。

（20）具备在系统卡片中查看单位近期发生的安全事件和风险隐患信息，一键展开事件详情进行研判处置。

3、监测中心

（1）场景化验证，包括弱口令、挖矿、勒索病毒等场景，具备通过单位名称、IP 地址、时间等多字段组合查询场景内容。

（2）场景概况展示，展示场景内等保系统、分布区域、高危单位/账号，快速定位场景概况。

（3）场景详情展示，关联场景内系统、单位、事件等基础信息和场景攻击/隐患信息，并进行快速验证，攻击溯源。

（4）场景自定义设置，自定义场景判断条件、分析周期、分析对象、场景标签，快速配置场景应用。

（5）具备告警数据自动化归并，并通过告警列表条目颜色区分“已读告警”和“未读告警”；具备查看归并告警基本信息、规则详情、原始告警列表、全部字段、PCAP 包详细信息，并具备下载 PCAP 包；具备在归并告警页面进行告警快速处置，包括忽略告警、误报处置、联动处置、人工处置等。

（6）具备对资产进行精细化评级评分计算，资产风险等级包括已失陷、高风险、中风险、低风险，资产评分为百分制，具备资产评级标签；具备查看资产最近 15 天评级评分趋势、资产威胁词云、资产评分比较等信息。

（7）需具备攻击搜索解决方案，具备攻击导入导出、攻击检索、攻击研判

分析、攻击分类等功能。

（8）攻击检索，平台具备“与”、“或”、“包含”等不低于 15 种语法检索。

（9）攻击场景聚合，根据攻击类型和攻击信息进行数据聚合分析，具备不低于 13 种攻击类型分类，具备自定义攻击信息字段。

（10）需具备原始日志解决方案，具备日志导入导出、日志检索、日志研判分析等功能。

（11）日志检索，平台具备“与”、“或”、“包含”等不低于 15 种语法检索。

（12）日志信息展示，具备接收时间、目的 IP、告警类型、事件名称、目的端口、威胁等级、起始时间、处置状态、单位名称、告警名称、数据流向、告警子类型、所属区域等信息展示。

（13）日志展示字段自定义配置，平台内置不低于 70 个字段可进行灵活进行配置展示。

（14）日志详细信息，具备日志来源、目的、摘要和其他详细信息，可根据字段自由过滤和排除可疑风险。

（15）需具备风险监测结果解决方案，具备风险检索、风险缝隙、风险处置等功能。

（16）风险检索，具备漏洞名称、漏洞等级、漏洞类型、漏洞状态、扫描器类型、IP/域名、端口、服务、CVE 编号、CNNVD、关键字等字段检索，实现多字段组合检索。

（17）需具备监测引擎管理解决方案，具备通过配置参数对接并调度主流监测引擎。

（18）具备新增、编辑、删除监测引擎，具备自动和手动检测连接状态，具备配置监测引擎的跳转链接。

（19）需具备漏洞扫描报告模板管理解决方案，内置报告模板，可通过编辑模板内容实现报告自定义，模板具备预览、重新上传、下载、删除，设置为默认的模板作为漏洞扫描报告的模板。

4、响应中心

（1）具备立体化跟踪通报全流程周期，多维度展示通报工作开展情况，对网络安全工作进行监督考核。

（2）具备看板信息展示功能，包括通报、预警信息，对整个信息发布过程进行跟踪记录。

（3）具备信息下钻，点击通报、预警信息，可以查看对应详情，如通报标题、创建时间等。

（4）具备汇总展示当前用户收到的通报总数，并根据通报的状态进行分类展示。

（5）具备汇总展示当前用户收到的预警通知数量，并根据未读、已读进行展示。

（6）具备根据时间、区域筛选通报、预警展示数据。

（7）具备对最新通报、收藏通报的跟踪展示。

（8）具备根据通报紧急程度进行统计展示。

（9）具备根据预警通知的自定义标签进行统计展示。

（10）具备根据通报的行业和单位进行排名统计。

（11）具备展示各个区域的通报情况，包括处置及时率、完结率、总量、逾期量，并以图表方式展示。

（12）具备对网络安全事件或威胁发出通知或者预警，警示相关单位。

（13）通知中具备记录通知名称、标签、级别、详情、通知对象和举证信息。

（14）通知具备草稿箱功能，发布的无效通知具备关闭和删除。

（15）新增通知可以输入文字、图片、超链接、表格、代码片段等≥种信息类型，其中文字具备设定字体大小、文字颜色，文字高亮、加粗、倾斜等>=5 种配置。

（16）发布通知/预警时，具备已读回执，通知下发后对各单位的已读情况进行查看。

（17）通知举证信息具备一键溯源，包括溯源到资产档案、系统档案、情报信息、原始日志等。

（18）预警中具备记录预警名称、标签、级别、详情、预警对象和举证信息。

（19）预警具备草稿箱功能，发布的无效预警具备关闭和删除。

（20）预警详情可以输入文字、图片、超链接、表格、代码片段等>=5 种信息类型，其中文字具备设定字体大小、文字颜色，文字高亮、加粗、倾斜等>=5 种配置。

（21）发布预警时，具备已读回执，预警下发后对各单位的已读情况进行查看。

（22）预警举证信息具备一键溯源，包括溯源到资产档案、系统档案、情报信息、原始日志等。

（23）具备根据安全事件或风险隐患发布通报，督促相关单位妥善处置网络安全事件。

5、感知中心

（1）具备按照近七天、近一个月、近三个月、本周、本月、本年维度进行统计。

（2）具备不同厂商安全日志数据的统计。

（3）具备安全事件、风险隐患、网络攻击事件的统计展示。

（4）具备安全区域和行业两个维度统计安全事件、风险隐患数量。

（5）具备区域通报情况、单位通报情况、行业通报情况的数据汇聚。

（6）具备预警中心、通报处置业务开展情况的数据统计。

（7）具备境内外、省内三个维度的访问次数、远程控制、传输流量、扫描数据的展示。

（8）具备通过综合监管态势一张屏汇聚监管对象（如监管单位、关基设施、资产底数、驻点探针、分析流量、知识案例、威胁情报、安全大数据、联动城市）、监测成果（如安全事件、风险隐患、网络攻击）资产动态（如 Apache、CDN、SSH、数据库、微软 IIS、远程桌面）、黑客动态、实时通报、资产分布和网络攻击趋势等总体情况。

（9）具备在一张屏展示网络虚拟空间、单位地理空间、单位资产空间，直观反映三层之间的关联关系，具备将攻击行为从网络空间映射到地图空间，再到单位拓扑。

（10）具备在三维地图展示安全事件，具备与后台事件调查功能联动，一键进行事件调查。

（11）具备大屏地图资产与后台信息发布一键联动，通过地图点击风险资产下发预警。

（12）具备对综合监管态势大屏展示内容进行自定义，具备自定义的内容不少于 40 种；资产统计维度包括行业分布、地域分布、开发框架等。

（13）具备通过统一的可视化界面，集中监控并展示 web 类应用系统的被访问/攻击的安全态势。

（14）统计并展示当天网站集群的进出总流量、被访问/攻击总次数，在地图上进行动态可视化呈现。

（15）以列表形式统计以下内容并进行可视化呈现：网站区域访问量排行 top5、访问 IP 排行 top5、被攻击网站排行 top50、攻击来源 IP 排行 top10、攻击类型排行 top10。

（16）实时刷新并滚动展示针对 web 业务的最新安全告警，包括攻击时间、地区/源 IP、被攻击域名、被攻击 URL、危险等级等信息。

（17）可点击钻取查看针对单个网站业务系统的攻击/访问信息。

（18）具备通过独立的大屏界面，实现对攻击者的可视化溯源。

（19）具备统计并展示包括但不限于攻击者基本信息、攻击行为分析、相似 IP 分析、攻击取证信息、日志量、攻击趋势、攻击手段，攻击告警分布等信息。

（20）具备任意攻击者信息查询，具备最近 24 小时、最近 7 天，最近 30 天、本日、本周、本月周期进行可视化溯源分析。

（21）具备生成详细的攻击者溯源报告并能够一键导出。

（22)具备通过独立的大屏界面,实现对资产被攻击状况的可视化溯源分析。

（23）具备统计并展示包括但不限于资产基本信息、被攻击行为分析、相似资产分析、攻击来源分析、资产弱点、攻击取证信息、被访问趋势、日志量、被攻击手段、攻击源 TOP 等信息。

（24）具备最近 24 小时、最近 7 天，最近 30 天、本日、本周、本月周期选择进行可视化溯源分析，并具备任意资产被攻击信息查询。

6、考核评价

（1）具备管理考核评价任务，包括启动、编辑、查看、排名、办结、删除。具备通过任务时间、创建单位、任务状态、标签、关键字（任务名称、联络

人）查询考评任务。

（2）具备编辑考核评价任务的任务名称、任务时间、任务联络人、评估模板、评估对象、评分专家、单位填报时间、标签、附件、任务说明等信息。

（3）具备展示考核评价任务的任务名称、任务状态、任务时间、单位填报时间、创建单位、任务联络人及其联系方式、考评进度、任务附件、任务说明等信息。

（4）具备通过单位名称、单位组、所属区域、所属行业、单位直属性质、单位类型选择评估对象。

（5）具备通过专家名称、所属单位、专家组选择评分专家。

（6）具备通过单位名称、单位任务状态查询考评任务的单位，具备统计各单位任务状态单位数，具备展示考评任务各单位的单位名称、所属区域、单位责任人、单位联系人、联系方式、单位任务状态等信息。具备新增、查看、删除单位任务。具备新增任务的评分专家。

（7）具备查看考评任务记录，包括新建/启动/办结任务操作的操作时间、操作账号及其所属单位、考评任务名称。

（8）具备展示单位任务状态及状态变更时间、总分、排名、材料完整度。具备展示考核表的检查项内容、提示内容、总分、检查项类型、材料、备注、评分、评分说明等信息。具备下载单位任务考核表分数明细。

具备查看单位任务记录，包括新建/启动/办结任务操作的操作时间、操作账号及其所属单位、考评任务名称和提交/操作的操作时间、操作账号。

（9）具备对考评任务排名，具备柱状图展示考评任务单位排名、饼状图展示各分数等级分布；具备展示单位排名总分列表，包括单位名称、所属区域、单位类型、单位联系人、联系方式、单位直属性质、得分等；具备展示单位排名各项列表，包括单位名称及各一级评估项小计；具备通过单位名称、单位直属性质查询单位；具备下载排名明细，包括单位总分、排名情况及各评估项得分明细。

（10）具备管理考评模板，包括新增、查看详情、编辑、删除。

（11）具备展示模板名称、模板说明、创建人、最近修改时间。

（12）具备编辑考评模板的模板名称、模板说明。具备识别并解析上传的表格，具备预览考评表、编辑考评表单元格、增加行、删去行、上下移动行，具备

下载编辑的考评表。

（13）具备查看考评模板的考评表内容，包括检查项内容、检查项等级、提示内容、总分、检查项类型。

（14）具备管理单位组，包括新增、编辑、删除。

（15）具备展示单位组名称、创建人、最近修改时间、说明。

（16）具备编辑单位组名称、说明以及选择、删除、批量删除专家组中的专家，具备通过专家名称、所属单位、专家组查询并选择专家。

（17）具备管理专家组，包括新增、编辑、删除。

（18）具备展示专家组名称、创建人、最近修改时间、说明。

（19）具备编辑专家组名称、说明以及选择、删除、批量删除单位组中的单位，具备通过单位名称、单位组、所属区域、所属行业、单位直属性质、单位类型查询并选择单位。

（20）具备按照报告来源、统计时段、创建时间等维度对考评报告进行筛选。

（21）具备一键展开报告，查看单位通报 TOP10、评分分布情况。

（22）具备对考评报告进行详情查看、下载。

7、重大安保

（1）具备新建活动，包括活动名称、活动地点、摸底、临战、备战、决战阶段的时间进度、活动负责人及联系方式、活动描述，同时具备编辑、删除、结束活动。

（2）具备下钻到具体某个活动，查看活动详情。

（3）可以快速查看活动总数及活动信息卡片，未开始、进行中、已结束的活动数量，管理每个活动的安保单位、人员、系统、驻点、应急预案等活动要素。

（4）展示活动各阶段的进程并突出当前所处进程。

（5）显示最新 3 条信息公告、功能快捷方式不少于 16 个、个人信息。

（6）列表显示待办工作，包括通报处置待办、指令待办，通报处置待办标识处置状态及通报类型，指令待办标识指令状态及指令类型。

（7）列表显示跟进工作，包括通报处置跟进、指令跟进，通报处置跟进标识处置状态及通报类型，指令跟进标识指令状态及指令类型。

（8）具备按里程碑名称、里程碑时间查询里程碑。

（9）具备里程碑进行新增、修改、查看、删除操作。

（10）指挥人员是安保活动的组织领导人员，负责领导和决策安保活动的重大事宜，包括提供筹备组织、制度信息，指挥调度安保活动。

（11）具备从已录入用户中批量选择指挥人员，人员信息包括但不限于人员名称、标签、联系方式、角色。

（12）具备单个或批量设置指挥人员的角色，包括但不限于组长、副组长、组员。

（13）具备通过人员名称、标签、单位名称、区域等条件查询人员列表。

（14）具备查看人员详情，及将人员退出单次活动。

（15）具备说明指挥单位的作用，指挥单位是安保活动的组织领导机构，负责领导和决策安保活动的重大事宜，包括提供筹备组织、制度信息，指挥调度安保活动。

（16）具备从已录入单位中批量选择指挥单位，单位信息包括但不限于单位名称、标签、上级单位、所属区域、单位类型。

（17）具备通过行业类型、标签、所属区域、单位类型、单位名称、联系人、手机号等条件查询单位列表。

（18）具备查看单位详情，及将单位退出单次活动。

（19）具备说明安保人员的作用，安保人员是安保活动的被监管单位人员，负责安保系统的日常管理和维护，落实保障工作，参与应急演练和培训，以及处置安全事件和应急事件。

（20）具备从已录入用户中批量选择安保人员，人员信息包括但不限于人员名称、标签、联系方式。

（21）具备通过人员名称、标签、单位名称、区域等条件查询人员列表。

（22）具备查看人员详情，及将人员退出单次活动。

（23）具备说明安保单位的作用，安保单位是安保活动的被监管单位，负责安保系统的日常管理和维护，落实保障工作，参与应急演练和培训，以及处置安全事件和应急事件。

（24）具备从已录入单位中批量选择安保单位，单位信息包括但不限于单位名称、标签、上级单位、所属区域、单位类型。

（25）具备通过行业类型、标签、所属区域、单位类型、单位名称、联系人、手机号等条件查询单位列表。

（26）具备查看单位详情，及将单位退出单次活动。

8、安全中台

（1）日志采集方式应具备但不仅限于 Syslog、kafka、ftp、部署代理方式。

（2）具备采集异构设备的日志数据，实现包括但不限于安全类、网络类、应用服务器类、操作系统类等至少 4 大类、50 种设备的日志接入采集。

（3）具备接入应用服务器的性能类数据，包括但不限于 CPU、内存和磁盘的使用情况数据。

（4）内置解析规则具备厂商>200 家，具备日志种类>2000 种。

（5）无需配置设备日志与设备类型对应关系，日志格式自动匹配解析。

（6）可对日志进行细粒度解析，解析后的日志根据具体日志包含但不限于：日期、发生时间、接收时间、设备类型、日志类型、日志来源、源地址、目的地址、事件类型、时间范围、操作主体、操作对象、行为方式、技术动作、技术效果、攻击类型、特征类型、协议、地理信息>=30 个字段。

（7）具备同时保存事件原始日志数据和标准化后日志数据的能力。具备对收集到的重复的日志进行自动的聚合归并，减少日志量，可由用户定义和修改的日志的聚合归并逻辑规则。

（8）具备根据业务系统、时间、责任人、数据自身逻辑、使用目的等打标签。

（9）元数据实现了信息的描述和分类的格式化，更好地对数据资产进行管理，理清数据之间的关系；以具备管理人员、业务人员和技术人员快速了解平台数据对象定义以及数据对象之间的关系。

（10）具备对 200 个以上字段进行任意形式的逻辑与或非形式组合建模，并能根据组合方式自动生成运算表达式。

（11）安全模型分析具备结合规则、关联、统计引擎，提供数据分析、求和、均值、统计、唯一值等计算。

（12）具备由分析人员提交实时任务和离线模型、算法到平台，输出结果及时反馈到机器学习模型，模型重新提交到实时流计算引擎，形成联动并最终输出

安全模型。

（13）内置包括规则模型、关联模型、统计模型、情报模型、AI 模型等在内的不少于 5 大类安全分析模型功能。

（14）具备通过独立的可视化大屏，将 AI 高级分析的结果数据进行集中呈现，具备自定义分析时间范围。

（15）利用 AI 分析算法或机器学习算法对历史的安全数据进行分析建模，拟合置信区间阈值，对周期性规律和异常突变进行识别呈现。

（16）具备同时进行 3 种或以上高级算法的组合分析和结果比对，大屏轮询播放每种算法的具体计算情况。

（17）具备预置多种 AI 分析场景，对包括但不限于勒索挖矿告警数异常、安全设备日志数异常、疑似 DNS 隐蔽信道、网络会话数异常、inBound 流量异常、域名请求数异常、网址访问失败异常的安全场景实现深度分析，并给出异常的具体原因以待查验。

（18）具备异常信息钻取进行问题定位，查看异常时间点前后 10 分钟的原始日志数据，深度追溯具体异常原因。

（19）具备信息发布、目录检索、资源统计、任务监控、交流反馈、消息接收、资源监测等功能，及与外界的统一交互。

9、分析研判

（1）具备界面化交互式完成安全建模，模型类型包括统计模型、规则模型、情报模型、关联模型 >=4 种；系统出厂内置模型>200 个，模型具备标签化管理，具备单个模型的启用禁用控制，具备一键查看模型的输出结果；多个模型可以形成串并联关系，前一个模型的输出结果可以作为后一个模型的输入。

（2）模型具备对数据中任意字段进行多种方式计算，字段包括源地址、源端口、目的地址、目的端口、传输层协议、应用层协议等>100 个，算子包括过滤、正则、分组、统计、唯一值等>10 种。

（3）模型中的判断条件具备类 SQL 语言输入和 key/value 条件树可视化配置 2 种创建方式，类 SQL 语言输入过程中提供语法和字段联想，两种方式创建的条件内容具备一键转换；判断条件具备与、或、非、In、Not In、exist、包含等方式灵活组合。

（4）模型具备选择数据源和输出字段，输出字段赋值时具备界面化编程，通过建立多层判断条件满足不同场景下的输出要求，告警描述和处置建议具备关联内置知识库。

（5）情报模型具备 IP、域名、文件 Hash、邮箱情报碰撞方式。

（6）黑白名单误报调优具备任意字段配置组合条件生成黑白名单过滤规则，具备规则数>=100 条。

（7）具备实体间网络关系的多级钻取，具备>10 跳的流量关联关系分析，具备通过端口、协议、异常访问类型过滤关联关系。

（8）实现实体间网络互访关系的多级钻取，具备通过端口、协议、异常访问类型、攻击链等过滤关联关系，具备实体间网络互访关系的多级钻取，通过“一键溯源”按钮进行威胁关系的自动拓展。

（9）具备可视化图表类型>=15 种，包括但不限于时序图、饼图、柱状图等。

（10）统计类图表具备展示升序或降序的 TOP5 到 TOP100，可针对数据中任意字段的计数、平均值、求和、最大值、最小值、唯一值等>=5 种算子的统计结果配置可视化图表。

（11）可视化图表可通过拖拽配置组装成仪表盘，仪表盘不少于 7 种布局类型，每张仪表盘可包含>=50 个可视化图表，可视化图表具备导出 WORD、PDF。

（12）仪表盘展示时具备时间范围自定义选择，具备放大聚焦某个图表。

（13）具备报告内容自定义，包括标题、图表、报表自定义，其中具备的图表类型>=15 种。

（14）具备导出日报、周报、月报和自定义时间范围内的安全分析报告。

（15）报告订阅具备通过邮件方式在设定时间点发送日报、周报、月报到不同邮箱，可配置订阅规则数量>=10 条，报告格式具备 WORD、PDF 等。

（16）内置漏洞知识库包含漏洞等级、漏洞名称、漏洞分类、CVE 编号、CNNVD 编号、漏洞解决方案、参考网址等信息。

二、政务外网安全监测平台

（一）基础要求

满足《黑龙江省数字政府建设 2023 年工作方案》中一体化安全运营中心和

《政务网络安全监测平台总体技术要求》（T/CIIA 005-2019）《政务网络安全监测平台技术规范》等相关要求。

完成与省级平台进行数据级联对接，落实网络安全协同防御、联防联控的要求,我市政务网络安全监测平台的建设需按照国家电子政务外网的统一要求，规范化进行设计、建设和运行管理。平台开发建设需按照要求和省级政务安全监测平台进行数据的级联对接，实现包括安全事件数据上报、预警通告下发、威胁情报共享，以及应急处置联动等。满足国家及主管部门对于网络安全整体防护、联防联控的要求。

政务外网安全监测平台负责监测本级广域网核心、本级政务云、本级城域网汇聚（核心）、本级互联网出口、县级广域网出口、县级城域网核心，实现政务网络安全监测的全覆盖（必要时电子政务外网接入单位需要按照省市两级管理纳入安全监测范围）。包括市属双平面 9 区 9 县政务外网出口、5 朵政务云政务外网出口、互联网出口以及政务外网核心区域流量等。建设内容包括安全监测平台控制中心、各分支节点部署流量采集探针，并实现与国家、省多类数据识别和收集、多种安全接口的对接。

具体安全监测内容：广域网、城域网核心设备链路监测、骨干网流量监测、拒绝服务攻击监测、病毒与木马监测、网站监测、互联网行为监测、信息系统监测、认证与授权监测、核心设备性能监测、原始日志存储、脆弱性监测、服务器工作性能监测、运维操作审计等。

1、安全能力建设

（1）数据采集预处理子系统

数据采集预处理子系统主要应实现通过部署流量探针、日志探针、资产探针、脆弱性扫描探针、第三方导入、API 接口等手动发现或自动发现方式获取政务外网区域的流量威胁数据、日志数据、资产数据、漏洞数据、弱口令数据、配置弱点数据、威胁情报数据、第三方平台数据等数据，并进行数据解析预处理，以供进一步深入分析使用。子系统功能应包括：数据集采范围及对象、日志数据采集预处理、流量数据采集、资产数据采集、脆弱行数据采集、威胁情报数据采集、知识数据采集和第三方平台数据采集等部分。

（2）大数据计算存储子系统

大数据计算存储子系统应主要实现对各子系统采集、分析、展示等维度的结构化数据、半结构化数据、非结构化数据等数据根据冷热数据存储策略进行数据存储处理，可提供稳定的数据接入、数据存储、数据计算、数据分析、数据应用、数据运维管理、安全防护等材料数据和结果数据的存储。

大数据计算存储子系统应对数据采集预处理系统提供数据计算存储的关键，为威胁事件分析子系统、态势展示子系统等系统提供数据计算存储能力。子系统功能应包括：分布式存储、数据仓库、分布式索引、关系型数据库、存储资源管理和数据类别等部分。

（3）数据总线子系统

数据总线是实现网络安全监测平台中数的采集、存储、分析、展示与应用等各模块之间，以及与外部系统之间规范化数据共享和交换的协议和接口集数据总线实现。

数据总线子系统设计参考国家信息中心发布的《政务网络安全监测平台数据总线规范》团体标准要求及国家信息中心发布的《第三方协同接口（市对省协同接口）》规范要求，以完成市级平台和省级平台对接。

数据总线中共享和交换的数据主要包括流量元数据、设备日志、资产数据、告警数据、威胁情报、安全事件、工单报表等。子系统功能应包括：内部数据交换口、数据采集接口、级联接口和数据共享接口等部分。

（4）威胁事件分析子系统

威胁事件分析子系统主要实现对采集预处理后的数据进行数据分析，产生威胁事件告警，并对告警数据进行各种维度的统计分类分析，分析方式包括但不限于特征分析、关联分析、资产风险分析、威胁情报分析、基线分析、实体分析、攻击者分析、攻击链分析、数据挖掘分析、威胁预警分析等分析方式。威胁事件分析子系统分析出的安全事件结果可以给事件响应处置子系统、预警通报子系统提供事件输入，给态势展示子系统提供数据输入。子系统功能应包括：关联分析、资产风险分析、威胁情报分析、基线分析、实体分析、攻击者分析、攻击链分析、数据挖掘、威胁预警等部分。

（5）事件响应处置子系统

事件响应处置子系统应具备实现对数据采集预处理子系统、威胁事件分析子

系统等子系统产生的脆弱性分风险及安全事件告警进行响应处置，包括事件调查、工单流转、处置联动等，形成安全风险及安全事件的处置闭环。

事件处置响应子系统对威胁事件分析子系统的分析结果进行处置响应。子系统功能应包括：调查工作台、工单、白名单和处置联动等部分。

（6）预警通报子系统

预警通报子系统主要实现对政务外网、政务云等系统中的攻击告警事件、漏洞、威胁情报、异常流量、弱口令、配置弱点等进行预警通报。平台运营人员可以通过本子系统依照设定的流程发布信息通报，以快速同步相关风险信息及预警处置结果信息，完成安全风险信息的传递及闭环处置。子系统功能应包括:预警分级、信息通报、消息通知和预警自定义等部分。

（7）态势展示子系统

态势展示子系统应主要应实现对政务外网不同安全态势数据指标及运营指标的展示，通过使用地图、饼图、柱状图、折线图、3D 图、雷达图等形式对关注的不同资产类型、不同业务区域等维度进行安全状态和趋势的评估、统计、分析和展示，可快速了解整个政务外网各项运营监测指标的整体态势，展示方式包括仪表板、报表、态势大屏等形式。子系统功能应该包括：仪表板展示、报表展示和态势感知大屏展示等部分。

（8）运营管理子系统

运营管理子系统设计为主要对政务外网日常运营中应包括攻防演练及本级政务网络安全监测平台租户分权分域管理等。子系统功能应包括但不限于：攻防演练和分权分域部分。

（9）威胁情报子系统

应实现对政务外网包括勒索病毒、远控木马、挖矿主机、僵尸网络、APT 等已知和未知威胁的检测分析。威胁情报应依赖于平台是否集成有强大的、持续更新的本地威胁情报库支撑能力及云端威胁情报查询能力。子系统功能应包括:威胁情报数据生成、威胁情报数据组成、威胁情报数据使用和威胁情报数据更新等部分。

（10）安全管理子系统

安全管理中心子系统应具备对政务外网安全监测平台运行配置管理，包括用

户管理、配置管理、运行监控、身份鉴别、授权管理、安全审计等。子系统功能应包括:用户管理、配置管理、运行监控、身份鉴别、权限管理、安全审计和安全性。

2、安全监测运营支撑服务

（1）安全检测运营支撑应提供驻场运营支撑服务

安全运营服务应以驻场运营服务人员为载体。梳理运营工作需要开展的具体事务，驻场运营服务人员会依托政务网络安全监测平台开展的资产管理、漏洞管理、威胁分析、预警通知等工作，通过持续开展运营工作可掌握自身的资产情况，及时发现面临的内外部威胁风险等，提高自身的安全体系健壮性，并定期对运营实施过程中的风险进行评估并改进，确保安全运营工作的质量。

（2）服务内容

应对各类资产进行梳理，识别资产属性，对资产应用识别、资产攻击面分析、资产变更进行管理、资产数据备份。资产管理作为安全运营的基础性工作，驻场运营服务人员应协助政务外网相关管理部门进行资产梳理工作，并协助录入政务网络安全监测平台。主要内容需包括：资产管理服务、告警监控服务、威胁分析服务、关联优先规则服务、遇境告知服务、安全事件管理服务和政务网络安全监测平台运维服务等部分。

3、自身安全性建设

（1）自身安全特性

1）安全性措施

安全性措施应满足以下方面。

Web 安全性方面：应采用 HTTPS 进行网络传输，并遵循公钥标准规范与流程。以保障从平台对外的所有提供业务的链路加密。确保数据在传输过程中的安全性。

网络安全方面：应从出场就默认采用端口最小集合的开放方式。保障只对外开放必须的端口，防止不必要的漏洞利用和其他攻击事件。

授权访问控制方面：应采用 ACL 规则和策略，基于账号授权功能和角色配置进行受限功能授权，保障每个账号的业务权限符合最小授权法则。

通信安全方面：应采用 HTTPS 的 server 端证书为私有证书。流量探针与服

务端通讯采用对称秘钥加密。

业务安全方面：应基于安全会话管理和登陆超时机制，保障账号在其生命周期以外的操作是被阻止的。于此同时，还具备 IP 绑定、登陆锁定和登陆验证码来防治暴力破解和试探行为。

秘钥管理方面：应采用公钥进行加密、保障公钥存储于磁盘。

升级安全方面：应采用对称秘钥加密和代码集成密钥，确保交付升级包具备防篡改安全保障。账号密钥安全性方面，应采用加盐算法，保障账号密码不可猜测和存储安全。

账号安全性：账号设置需要考虑通用的账号管理策略，以对账号安全性进行加强，防止账号破解，异常登录等情况发生。政务外网相关管理部门可以根据实际使用需要，自行配置账号安全性要求。

2）安全分析

政务外网安全监测平台应进行安全性分析，内容应包括：第三方组件安全、输入验证、会话管理、文件管理、访问控制、通讯安全、错误处理、日志安全、业务逻辑、数据安全、密码安全、验证码安全。

3）系统高可用性

政务外网安全监测平台应采用冗余性架构部署，应采用服务器（云主机）集群每台服务器设计至少有 2 块固态硬盘作为系统盘，系统盘应通过 Raid1 进行硬件高可用性保障，当主系统盘故障后，备系统盘可无缝接管系统管理工作。

政务外网安全监测平台服务节点故障之后，保障平台基本服务继续可用。

政务外网安全监测平台相关数据存储组件应至少保留有 2 份数据副本，如单块系统盘出现故障，保障系统内置的软件备份机制将保障数据不会出现丢失等情况。

4）自身安全性加固

政务外网安全监测平台部署时应进行自身安全性加固，加固包括但不限于限制开放环境端口，防止被随意登录、篡改和破坏系统和业务数据。

（2）合规性安全建设

哈尔滨市政务外网安全监测平台根据自身安全需求参照网络安全等级保护三级相关要求进行安全建设。

安全监测平台需要采集的日志数据、流量信息、威胁情报、资产信息、漏洞信息等安全数据通过分布式采集器采集完成后，应采用 SSL 加密的方式传输至大数据分析平台和数据存储系统。

安全监测平台可对安全性配置进行修改，主要包括登录异常锁定、密码长度及强度要求、页面超时时间、密码更换策略等。

安全监测平台可对自身平台的运行状态进行监控，有状态异常可以通过发送运行设备状态进行告警提示。

政务外网安全监测平台应采用分布式存多副本备份机制，利用多副本技术，数据条带化放置，多时间点快照和周期增量复制等技术为分布式存储的高可靠性提供保障。

4、平台整体部署说明

政务网络安全监测平台：采集市本级全网数据，告警数据和边界安全及终端安全设备进行处置联动，和省级平台进行数据共享交换等。

流量探针：监测本级广域网核心、本级政务云、本级城域网汇聚（核心）、本级互联网出口、县级广域网出口、县级城域网核心，实现政务网络安全监测的全覆盖（必要时电子政务外网接入单位需要按照省市两级管理纳入安全监测范围）包括：包括市属双平面 9 区 9 县政务外网出口、5 朵政务云政务外网出口、互联网出口以及政务外网核心区域流量等。流量探针部署不少于 33 个，流量探针放置区域节点越多，威胁检测越全面，特别是对区域内部的数据汇聚数据检测。流量探针威胁告警数据、流量元数据将会发送给政务网络安全监测平台进行后续安全大数据处理和分析。

日志探针：安全设备、流量探针日志源可直接将日志数据发送给政务外网安全监测平台日志探针模块。

资产探针：对资产数据进行主动扫描发现，并把扫描结果发送给政务外网安全监测平台处理。

（二）具体要求

（1）满足《信息安全技术政务网络安全监测平台技术规范》、《黑龙江省政务外网监测平台技术方案》等相关技术要求。

（2）需提供至少 1 名驻场人员依托政务网络安全监测平台开展的资产管理、

漏洞管理、威胁分析、预警通知等工作，通过持续开展运营工作可掌握自身的资产情况，及时发现面临的内外部威胁风险等，提高自身的安全体系健壮性，并定期对运营实施过程中的风险进行评估并改进，确保安全运营工作的质量。

（3）安全威胁方面应具备实现对整网的安全风险进行统计、安全态势监控、安全事件分析、恶意文件分析、威胁分析、漏洞管理等。

（4）市级安全监测平台在完成本级监测的功能基础上，须与省级安全监测平台对接，将本级的相关安全信息上传至省级安全监测平台，并接收省级安全监测平台下发的安全威胁通告和安全风险预警。

2、安全数据治理

（1）风险分类覆盖《GB/Z 20986—2007 信息安全技术信息安全事件分类分级指南》中定义的所有风险类型。在分类分级的基础上具备拓展细化的三级风险类型，形成对风险的细粒度描述，平台的日志、事件、告警信息均采用统一的风险描述规范。

（2）具备对采集的原始数据进行格式标准化处理，消除日志字段间的表述差异。

（3）具备为日志丰富化资产相关信息以便于按资产/组织结构检索、丰富地理位置以便于后续分析和呈现。

（4）具备对日志数据的关键字段数值进行修正，消除无效值和错误值，根据设备类型对事件类型、风险等级等信息进行校对和映射。以实现对数据进行统一分类和描述。

（5）具备日志数据的查询，具备查询策略的维护、检索条件可选可填，具备二次检索(时间、字段）、数据透视分析、网络通联分析展示、详情查看、溯源分析、内网 IP 画像分析、导出、自定义列展示。

（6）具备对日志、事件、告警、脆弱性等安全信息按照多个条件自由组合查看、搜索展示，并具备查询结果导出，具备 IPV6 信息采集展示。对于分析聚合结果具备下钻查看原始信息或流水。

（7）具备接入漏扫设备数据联动同品牌漏扫、驱动主流厂商漏扫、手动导入漏洞扫描报告三种方式实现漏洞扫描器的扫描结果导入和管理，具备扫描结果自动关联资产并对漏洞结果进行解析，以增添识别资产脆弱性能力。

（8）具备对于多个逻辑隔离网络的统一数据汇聚和统一监控，具备保障各网络内相同 IP 地址无冲突/混淆的情况下对多个隔离网络的信息进行呈现、分析、关联。

（9）具备对相似的、重复的告警和事件进行不同层级不同细粒度的消重和去冗余，以大幅降低系统呈现的海量信息，提高信噪比。

3、安全数据分析

（1）具备根据检测日志和全要素日志持续监控行为体和执行体信息，形成安全百科，具备通过安全百科快速溯源定位疑似初始渗透资产、精准圈定疑似初始渗透的数据时间范围，有效帮助对海量数据进行排查。具备在事件、告警、仪表盘页面内快速呼出安全百科。具备对安全百科进行快速下钻。具备百科的对象包括：IP 地址、资产、设备、网站、域名、文件、邮件、应用用户、系统用户、组织机构。

（2）具备对攻击来源、外部攻击、内部攻击进行研判，标记研判结论、风险等级、威胁标签等信息。具备自动化形成内部高可信情报，对高风险行为体进行持续监控，发现后生成高可信告警。

（3）具备通过内置威胁算法动态监测网络攻击威胁后对威胁行为体进行画像，画像内容包括威胁行为体监控情况、威胁行为体攻击次数、攻击手法、事件链路、告警情况、历史研判情况、威胁追溯情况等信息。

（4）具备通过内置风险算法汇总资产风险，形成资产安全画像，以资产维度关联告警、事件、漏洞、根据资产重要性、资产遭受风险，资产防护情况等维度对资产安全风险进行度量。

（5）具备通过事件融合模型对采集到的日志进行融合，分组降噪去杂获取事件信息，根据不同事件类型对事件要素进行聚合分析，具备按照事件地址、协议、端口、事件级别、事件类型等进行分析，事件分析包括但不限于：外联威胁、横向威胁、外部威胁、内网穿透威胁、网站风险，并对事件列出详细信息、流量包及其他检测依据、关联安全百科和安全画像信息以便于溯源取证，具备事件向日志的下钻分析，具备查询结果导出。

（6）具备通过告警分析模型，形成对象化语义化的告警，从攻击方、影响方、举证信息、风险信息、记录信息几个维度对告警形成清晰的对象化描述方法，

其中具备的对象包括但不限于：告警来源、风险类型、风险名称、风险等级、IP地址、网专、处理状态、检测依据、域名、文本等。

（7）具备通过告警来源、攻击方、影响方、风险信息等维度消除告警误报，具备批量追溯近期告警。

（8）具备对事件分视角剖析，包括威胁诱捕、高级威胁、外部威胁、横向威胁、外联威胁、内网穿透、网站挂马、搜索劫持、敏感词、可用性、攻击者分析、暴露面分析等，具备对不同视角给出专项的风险描述、数据透视分析及处理建议。

（9）具备对告警关键要素进行关联分析形成对象化的时序关联序列，具备下钻进一步分析和研判。

（10）具备以攻击方视角关联告警，展示攻击次数、涉及风险类型、风险等级、处置情况等信息，具备以攻击方维度对告警进行快速处理，并具备查询结果进行导出。

（11）具备以资产维度关联告警、安全事件、漏洞，具备根据资产的告警数量、安全事件数、漏洞数量等维度对资产进行排序，一目了然的展示当前资产遭受风险类型、遭受风险等级，便于管理员进行重点处置，并具备查询结果进行导出。

（12）具备基于流量特征、行为状态进行网络安全分析建模，对流量侧信息进行场景化的威胁检测，通过分析发现扫描探测、恶意 IP、恶意域名、DDOS 攻击、境外通讯等风险识别。

（13)具备场景关联规则,具备虚拟专用网络对其他网络攻击进行关联识别,发现高风险内网穿透攻击，同时自动化对高风险用户进行溯源。

（14）具备配置告警生成策略，包括告警生成周期、重点关注风险。

4、安全监测

（1）电子政务外网监测平台软硬件一体化设备 3 台，设备应采用鲲鹏、龙芯、飞腾、海光等自主可控硬件平台，CPU≥128 核，内存：≥256GB。系统盘：≥960GB SATA SSD*2 RAID1,4T SAS HDD *12。网卡：≥4 千兆电口、2 万兆光口。提供冗余电源。

（2）具备安全监控仪表，包括综合感知、告警检测、资产监测、资产风险

等。

（3）具有重保中心，具备对重要安全保障或对抗场景形成重保全局策略配置，具备自动化或一键切换配置，具备设置重保时期。依托政务外网安全监测平台及专业安全工程师，对政务外网及相关云资源和基础资源进行保障工作，其中包括安全检测、安全值守、安全监测、安全加固、应急演练、安全培训，以资产为核心了解当前资产受攻击面，为整体防护举措全面覆盖提供支撑。

（4）全网态势展示的主题包括：资产概况、资产活跃度、日志源监控、脆弱性、地图实时攻击事件展示、告警趋势、安全事件趋势、告警统计、最新告警、热点事件等。并具备态势大屏中相关信息下钻跳转到对应的详细页面。

（5）安全底图

具备从脆弱性总体情况、漏洞类型分布、漏洞级别分布、高危漏洞类型排行、高危漏洞排行 TOP5、最新漏洞发现趋势、漏洞排行 TOP10、漏洞级别对比等多个维度展示整体网络的脆弱性态势。

（6）具备基于安全报告模板管理生成策略，系统内置模板具备日、周、月等维度生成安全报告，具备生成自定义报告。

（7）具备对各类导出报表进行汇总管理。

5、安全处置

（1）具备对告警处置结果进行记录跟踪，包括但不限于处理记录、忽略、误报等。

（2）具备对误报告警基于攻击方、影响方、举证信息、风险信息或检测信息组合形成误报消除策略。

（3）具备告警信息进行预警提醒，具备根据预设定的规则，根据风险类型、风险名称、风险等级、涉及资产、涉及机构、时间自动化形成告警通知，告警通知具备分组通知和专项通知。

（4）具备登记资产或机构的责任人，具备在告警列表、告警详情快捷查看联系人信息卡。

（5）具备通过邮件定时推送每日安全日报、高危风险预警。

6、资产管理

（1）具备通过主动探测和被动流量感知自动发现资产，并根据发现方式对

资产的类型和来源进行标签处理。

（2）具备资产信息的全量导入导出，从全局视角实现资产的全生命周期管理，具备资产信息维护等。

（3）具备资产环境识别，具备主动或被动无感的识别资产应用软件、端口和服务信息。

（4）具备漏洞、弱口令信息管理，可从漏洞状态、级别、涉及资产组、资产类型等维度进行监控，具备漏洞详情描述关联漏洞知识库，展示关联到的详细信息、处置建议等信息为处置提供依据，具备展示漏洞影响资产范围，并具备查询结果导出。

（5）具备私有 IP 段和自定义 IP 段资产自动识别匹配，通过监测流量中的资产 IP 信息进行资产备库，通过管理员审核后添加到资产库，具备自动审批。

（6）具备复杂网络环境，具备多网络管理，具备 IPv4 和 IPv6 地址空间管理，多个网络间 IP 地址可重复，具备对事件、日志告警中的地址自动化识别所属网络，保障不同网络空间内地址不会混淆或冲突。

（7）具备建立资产通联拓扑知识，具备根据汇总的流量数据自动生成资产间联通情况，每日自动更新，具备对资产网络通联情况进行查询和标注。

（8）具备资产的新增，删除，编辑和查看，资产详情中将展现资产属性基本信息、资产相关告警信息、资产相关漏洞信息，可视化呈现资产的多维度信息。

（9）具备关注重点资产，重点资产在告警、事件内具备进行专项统计、过滤和标记。

（10）具备通过信息卡的形式展示资产信息及组织结构信息，以便于快速查阅，具备通过信息卡下钻至资产详情或资产画像。

7、系统管理

（1）具备系统维护，包括邮箱配置、License 信息、磁盘管理、定时配置等维护。具备管理系统存储策略，可设定存储告警阈值、存储空间清除阈值，及日志和流量的保存天数。具备定时任务的增、删、改，提供相应的配置。

（2）具备角色管理和用户管理，具备三权分立，具备密码策略变更。

（3）具备共享管理设置，共享管理为日志转发方式提供配置，包括但不限于 syslog、kafka。

8、流量探针

（1）具备丰富的协议识别及解析能力，包括但不限于 TFTP、NFS、HTTP、IMAP、SMTP、MSFFILE、FEIQ、FTP、SMB、POP3、IEC_MMS、IEC_60870_104、PGSQL、MYSQL、RLOGIN、LDAP、ICMP、TELNET、UDP、TCP、ARP、BGP、SSH、TLS、DNS、MQTT、TDS、DNP3、modbus、oracel_TNS、AMS 等协议。

（2）具备注入攻击检测的能力，至少可检出 SQL 注入、宽字节注入、延时注入、代码注入、命令注入、表达式注入、文件注入、LDAP 注入、CRLF 注入、OGNL 注入、XML 实体注入等注入攻击。

（3）具备其他类型的 WEB 攻击检测的能力，如目录穿越、目录遍历、弱口令、默认口令、权限绕过、信息泄漏、文件包含、篡改信息、任意文件写入攻击、钓鱼攻击、拒绝服务攻击、数据库登陆（至少包含 SQL、Oracle、DB2、Mysql）、自定义路由、下载组件、非法 web 访问等攻击检测。

（4）具备基于模型算法的 HTTP 隐蔽信道检测、IP 分片隐蔽信道检测、DNS 隐蔽信道检测等能力，可对单个隐蔽信道检测功能开启/关闭。

（5）具备基于机器学习，语音学概率、传输数据熵值等元素的建模分析技术的 DGA 随机域名检测的能力。

（6）具备 UDP 木马心跳报文异常分析模型检测的能力，可开启/关闭。

（7）具备 OA 系统应用漏洞利用检测，包含但不限于致远 OA、泛微 OA、蓝凌 OA、万户 OA、一米 OA、信呼 OA、用友时空。

（8）不少于 370 类文件格式的识别与还原，文件分类包括文档、可执行程序、脚本、压缩包、文本、图片、多媒体、软件数据。

（9）具备挖矿木马专项分析的能力，可从检测信标、挖矿行为、木马家族、矿池类型、资产 IP、事件次数等方面对挖矿事件进行告警分析。

（10）具备独立的勒索软件分析功能模块，具备以柱状图、折线图的形式展示家族 TOP5、文件告警趋势等内容，以家族维度对告警事件智能聚合。

（11）具备独立的恶意邮件分析模块，至少可对邮件主题、发件人、收件人、抄送人、投递者、邮件正文、附件信息、附件行为信息等内容进行分析，发现钓鱼邮件等邮件通讯中存在的威胁。至少可提供发件人 TOP10、收件人 TOP10、威胁等级趋势等维度的统计图。

（12）具备独立攻击源分析功能模块，具备以地图炮的形式展示攻击源分布情况，柱状图的形式展示攻击源 TOP10。具备基于攻击源和攻击源事件列表两个维度进行分析。

（13）具备独立的恶意文代码分析功能模块，具备以柱状图、折线图的形式展示文件威胁类型 TOP5 分布情况、文件告警趋势等内容，具备基于恶意代码传播和恶意代码事件列表两个维度进行分析。

（14）具备检测结果标签化的能力，至少可体现威胁类型、通讯特征、核心行为、自定义标识等信息。具备标签组合筛选的能力，帮助安全分析人员快速定位威胁信息，提高分析效率。

（15）具备基于威胁画像的事件关联分析能力，具备生成关联分析报告，至少应包含对相关事件、攻击资源、攻击载荷、受害主机、漏洞利用情况的统一呈现。

（16）具备威胁事件向网空威胁框架展示的能力，包括但不限于 ATT&CK，nsacss。

（17）具备兼容 snort 语法规则的管理能力。可手动添加规则或批量导入规则。自定义规则应具备查看、编辑、禁用/启用、导出、删除的能力。

（18）提供与其他设备的数据联动接口，包含但不限于 HTTP 消息推送、SYSLOG 日志发送、kafka 消息推送、NAT 日志联动、STIX2 信息推动、IDMEF 消息推送。

（19）检测可具备不少于 6 万家族、1500 万余变种的恶意代码。

（20）系统应具备数据备份的能力，至少包含配置、自定义规则、流量检测规则、用户管理、日志数据的备份与恢复。

9、攻防演练服务

依托政务外网安全监测平台及专业安全工程师，进行常态化的自检、巡检、整改等工作，协助大数据中心迎接监管单位检查、漏洞扫描、渗透测试、安全加固、基线检查等工作，通过安全检查和渗透等自检手段对发现的漏洞协助修补和加固。

（1）演练前备战工作

准备工作、安全检测、安全加固、应急演练、安全培训，以资产为核心了解

当前资产受攻击面，为整体防护举措全面覆盖提供支撑；排查网络空间存在威胁以及对应威胁对抗能力等级；对已知威胁进行封堵，对客观因素无法直接封堵的，采用加强监控，缓解措施的方法进行处置，由人工持续跟进。

（2）演练迎战工作

可针对演练期间出现的新漏洞、新威胁进行综合性分析，包括传播手段、技术原理、危害程度、演变趋势等，结合不同场景进行威胁评估，形成综合性分析报告。

针对影响网站及系统运行的重大隐患进行实时监控，监控内容包括网页篡改、挂马、暗链、域名劫持、后门、关键字等；对目标网站进行全天候的安全监测，若发现异常及时通报并处置。

演练期间提供现场值守服务，通过政务外网安全监测平台实时捕获的流量测威胁进行检测、发现、定位、响应、溯源。

演练期间提供应急响应服务，针对演练中可能发生的木马事件、感染式病毒事件、蠕虫事件、后门事件、网络攻击事件、网络扫描事件、网站挂马事件、网页篡改事件、拒绝服务攻击事件、网络钓鱼事件、信息泄露事件等威胁事件进行紧急安全措施，恢复业务系统到正常服务状态。

针对威胁事件进行专项分析，根据事件响应与处置以及安全设备监测结果进行取证分析；对涉及样本进行动静态分析、溯源分析、事件威胁评估；根据事件处置的建议与现有安全防护体系，给出事件处置与体系优化建议。

（3）演练后总结工作

将演练期间的工作内容、成果、问题进行总结与分析，输出《攻防演练服务总结报告》。

（4）服务配置：配置人员不少于 10 名，全年 1 次工作，每次 30 天，每天 8 小时推进，每年不少于 300 人天。

（三）参数要求

1. 安全监测体系-安全威胁态势感知系统平台技术参数：

指标项	技术要求
性能要求	根据网络建设规划带宽设定，并满足数据分析的需要；
接口要求	根据实际互联网情况设定；

可靠能力	具备冗余设计；
功能具备	1. 能够与国家、省安全监测平台对接； 2. 具备省级、市（地）二级级联部署及平台对接； 3. 具备安全风险统计分析； 4. 具备安全态势监控； 5. 具备检测加密流量恶意软件攻击及攻击详情； 6. 具备攻击链分析； 7. 具备攻击事件分析； 8. 具备威胁情报； 9. 具备以每天、每周、每月的周期自动导出报表。
2. 安全监测体系-安全威胁态势感知系统探针技术参数：	
指标项	**技术要求**
性能要求	根据网络建设规划带宽设定，并满足数据分析的需要；
接口要求	根据实际互联网情况设定；
可靠能力	具备冗余设计；
功能具备	1、 具备全流量方式获取监测信息； 2、 提供全面的流量检测能力，可检测常见的攻击行为； 3、 具备与感知平台联动。
3. 安全监测体系-脆弱性扫描系统技术参数：	
指标项	**技术要求**
性能要求	根据网络建设规划带宽设定，并满足数据分析的需要；
接口要求	根据实际互联网情况设定；
可靠能力	具备冗余设计；
功能具备	1. 内置漏洞库不少于 15000 种； 2. 具备多种类型对象扫描的能力； 3. 具备报表功能，可生成报表； 4. 具备联动安全威胁态势感知系统。
4. 安全监测体系-运维审计系统技术参数：	
指标项	**技术要求**

性能要求	根据网络建设规划带宽设定，并满足数据分析的需要；
接口要求	根据实际互联网情况设定；
可靠能力	具备冗余设计；
功能支持	1. 具备广泛的应用接入，具备单点登陆和审计接入； 2. 具备静态口令认证、手机动态口令认证，USBkey（数字证书）认证，AD 域认证、Radius 认证等认证方式； 3. 具备设置一级或多级审批人； 4. 具备定期变更目标设备真实口令，具备自定义口令变更周期和口令强度； 5. 具备命令审批规则，用户指定高危命令时需要管理员审批后才允许执行。

5. 安全监测体系-运维审计系统技术参数：

指标项	**技术要求**
性能要求	根据网络建设规划带宽设定，并满足数据分析的需要；
接口要求	根据实际互联网情况设定；
可靠能力	具备冗余设计；
功能支持	1. 具备广泛的应用接入，具备单点登陆和审计接入； 2. 具备静态口令认证、手机动态口令认证，USBkey（数字证书）认证，AD 域认证、Radius 认证等认证方式； 3. 具备设置一级或多级审批人； 4. 具备定期变更目标设备真实口令，具备自定义口令变更周期和口令强度； 5. 具备命令审批规则，用户指定高危命令时需要管理员审批后才允许执行。

6. 安全监测体系-日志审计系统技术参数：

指标项	**技术要求**
性能要求	根据网络建设规划带宽设定，并满足数据分析的需要；
接口要求	根据实际互联网情况设定；
可靠能力	具备冗余设计；

功能支持	1. 具备添加、修改、删除资产；对资产的基本属性进行维护； 2. 具备审计国内主流厂商安全设备，主流操作系统，主流数据库，主流应用系统，具备主流的网络设备等； 3. 具备 Syslog、Syslog-ng、SNMP Trap 等主流方式采集日志； 4. 日志保存时间不低于 180 天。

7. 安全监测体系-安全管理平台技术参数：

指标项	技术要求
功能支持	具备 SNMP 协议管理； 具备互联网出口网关及部门接入安全网关等设备的可视化管理。

三、业务应用安全

（一）基础要求

1、关键应用系统检测与防护

（1）API 资产发现与管理能力

API 资产发现能力：具备根据流量特征自动识别 restful、GraphQL、websocket、MQTT、gRPC、JSON-RPC、XML-RPC 的 API 类型，并可以提供自定义配置方式，可以通过关键特征发现预期 API 资产，并标记标签。

API 资产管理能力：具备主动标记 API 资产的标签和应用，并具备导入、导出及编辑 API 资产列表的能力，包括标签、属性等信息，同时也具备风险 API 资产管理能力威胁检测功能。

（2）API 网络威胁监测能力

1）API 漏洞攻击检测能力：

针对事件型漏洞：应依据已知的 API 事件型漏洞的原理和攻击特征检测网络中利用已知 API 事件型漏洞的攻击行为。并具备攻击结果的研判,结果包括失败、尝试、成功和失陷。

针对通用型漏洞：应依据典型的漏洞原理及攻击特征检测网络中的漏洞攻击行为，包括但不限于命令执行、SQL 注入、跨站攻击（XSS）等。并具备攻击结果的研判,结果包括失败、尝试、成功和失陷。

针对授权类漏洞:应依据漏洞的产生原理及其特征检测网络中的授权类漏洞攻击行为，包括但不限于弱口令,后门账户等。并具备攻击结果的研判,结果包括失败、尝试和成功。

针对配置异常问题:应依据配置异常所产生的数据特征检测 API 配置异常的接口,包括但不限于配置异常所导致的敏感信息泄露、接口滥用等。该类型问题出现告警时，结果为成功。

2）API 逻辑异常攻击检测能力：

通过访问日志训练用户访问行为基线,并检测用户绕过流程的行为,包括但不限于登录流程绕过,验证码流程绕过等。并具备攻击结果的研判,结果包括失败、尝试和成功。

基于凭证识别、用户访问行为基线技术,检测网络中已知或未知的未授权访问行为。并具备攻击结果的研判,结果包括失败、尝试和成功。

3）API 异常行为检测能力：

具备根据单个用户及用户群体日常访问物理地点建立基线的能力，并具备在此基线的基础上发现特定用户访问地址变化或者访问群体出现访问地点离群值的情况，同时产生相应的异常告警。

具备根据单个用户的日常访问时间建立基线的能力，并具备在此基线的基础上发现特定用户访问时间变化的情况，同时产生相应的异常告警。

具备根据访问来源 IP 的范围建立基线的能力，并具备在此基线的基础上发现离群源 IP 的情况，同时产生相应的异常告警。

具备对于撞库、密码暴破、用户名暴破、验证码暴破、跨因子认证、批量注册等登录认证/注册功能异常访问行为的检测能力，同时产生相应的异常告警。

具备对于同一会话期间访问物理地址发生跳变的异常行为的检测能力，并产生相应的异常告警。

具备针对于特定接口的访问速率建立基线的能力，并具备在此基线的基础上发现高频率异常访问行为的能力，并产生相应告警。

4）API 数据流转异常及泄露检测能力：

具备根据用户群体使用系统业务功能的下载行为建立基线，需具备在此基线的基础上发现特定用户下载非正常业务所涉及敏感文件行为的能力，并产生相应

的告警。

具备根据单个用户及用户群体日常访问系统时间建立基线，需具备基于此基线发现特定用户在非工作时段下载大量敏感文件行为的能力，并产生相应的告警。

具备对 API 接口响应数据是否包含大量 API 接口路径、账号密码、身份证号码、电话、住址等敏感信息进行检测，并产生相应告警。

5）API 未知威胁检测能力

具备具备根据各类 Web 漏洞利用载荷特征提取通用检测规则以应对未知的 Web 类型的漏洞检测的能力。

具备具备根据异常检测模型对未知威胁行为进行发现的能力。例如，对登录阶段的页面跳转流程建立基线以通过发现违反该基线的行为来发现认证流程绕过漏洞。

具备对 HTTP 协议中的请求头、请求体、响应头、响应体中的内容进行识别。需详细记录识别出来的信息。

具备用户自定义检测规则。

具备识别能力动态升级的功能，以便快速提高识别能力。

（3）API 安全防护能力

具备黑名单过滤功能，具备源 IP、目的 IP、HOST、URL 等单个条件或组合条件的过滤能力，对于命中的黑名单的流量，在串接部署场景下直接阻断相关流量数据，并根据配置生成相关审计日志。

具备白名单过滤功能，具备源 IP、目的 IP、HOST、URL 等单个条件或组合条件的过滤能力，对于命中白名单的流量，在串接部署和旁路部署场景下直接放行相关流量数据，并根据配置生成相关审计日志。

具备基于 HOST、URL、HOST 及 PATH 组合筛选条件的应用内容筛选能力，对筛选后 API 应用内容做后续的更细粒度的检测，对于未被筛选到的流量，在串接部署场景下直接阻断相关流量数据，在旁路部署场景下放行相关流量数据。

具备基于请求方法、源 IP、目的 IP 内容的管控能力，对于命中管控功能的流量，在串接部署场景下阻断当前流量，在旁路部署场景下放行当前流量，并根据配置生成相关审计日志。

（4）API 敏感数据识别能力

具备对 HTTP 协议中的请求头、请求体、响应头、响应体中的内容进行识别。需详细记录识别出来的信息。

应具备对非结构化、半结构化、结构化数据类型的检测。

具备对通过 API 接口传输的图片中的内容进行识别。图片类型包括但不限于 webp、bmp、pcx、tif、gif、jpeg、tga、psd、png、ico、dib、ras、jp2、exr、dxf、pbm、pgm、ppm 等类型。

具备对 HTTP 协议传输的文件中的内容进行识别。文件类型包括但不限于 doc、docx、ppt、pptx、xls、xlsx、rtf、wps、et、dps、odt、ods、odp、odf、pdf、txt、html、csv、chm、xml、eis、eip、eit、uop、uos、uot、ceb、cebx、eml、eio、xps、mobi、dwg 等。

具备对压缩类型文件检测，且可具备对多层级压缩文件的检测。压缩文件格式包括但不限于 RAR、ZIP、7Z、BZ2、TAR、GZIP、CAB、ISO、ARJ、JAR、XZ 等格式。

内置一些常用的检测方法。包括但不限于个人敏感信息、重要数据等。

具备自定义敏感信息检测功能，包括但不限于关键字、正则表达式等方式。

具备识别能力动态升级，以便快速提高识别能力。

具备对识别后的结果进行统计分析。

（5）API 安全分析能力

异常行为关联分析能力：异常行为通常需要结合人工分析以进一步确定触发异常行为的原因以及该异常行为是否确实预示着某种攻击的发生。为了节省分析成本，减小分析人员压力，分析平台应具有以下关联分析能力。

1)应可以根据攻击源 IP 或者会话标识将异常与相关告警聚合成事件，从而确定该异常与安全事件关联。

2)应可以在异常的基础上结合接口属性进一步细分告警，比如某接口出现了高频访问的异常则此时因细分告警为“接口滥用”。

2、关键业务系统代码安全检测

（1）具备多种编程语言的源代码缺陷检测

为满足哈尔滨的众多新建政务业务系统源代码检测，代码检测系统应具备源

代码静态分析技术对软件源代码进行自动化分析，从源代码层面发现软件中的安全缺陷。主要功能应包括：缺陷分析、源代码审计、检测报告、统计分析、系统管理。

（2）兼容多个安全编码标准的源代码合规检测

为满足哈尔滨市数字政府多类型的政务业务系统，合规检测应具备多个国际、国内相关安全编码标准的检测，包括应用软件安全编程指南国家标准（GBT38674-2020）、国军标 GJB 8114-2013、国军标 GJB 5369-2005、联网软件安全编程规范、CERT C/C++/JAVA 等。

（3）第三方工具集成与兼容

在不改变哈尔滨数字政府业务系统现有开发测试流程的前提下，可以与多种开发工具或系统进行集成，将源代码安全检测融入开发测试流程中，实现自动化周期性的源代码缺陷检测。第三方工具集成包括软件版本管理系统（SVN、Git、TFS、Gerrit、FireFly、ClearCase、StarTeam 等）、持续集成系统（Jenkins、GitLab-CI 等）、构建系统（Gradle、Maven 等）、Bug 跟踪系统（Bugzilla、Jira、禅道、TFS 等）。同时还需要提供多种 Restful API 接口，满足哈尔滨进行灵活化集成。主要功能应包括：单点登录、与持续构建系统融合、与缺陷管理平台融合和开放 API 等四部分。

（三）具体要求

关键应用系统安全建设涉及范围为本次哈尔滨市数字政府业务系统使用。

基于云原生架构，基于发现、检测、分析、响应的方法论来构建一套闭环的能持续监测响应 API 安全检测与分析体系。

1、关键业务系统 API 分析系统

API 安全分析系统具备对 API 资产管理、威胁检测与分析、敏感数据泄露风险分析等功能，并具备向 API 检测系统下发检测策略和管控策略。

具体参数如下：

硬件规格：不低于标准 2U 机架设备，设备应采用鲲鹏、龙芯、飞腾、海光等自主可控硬件平台，内存≥256G，硬盘≥SSD 1T，硬盘≥48T SAS，网络接口：≥2 个 SFP+万兆光口、≥4 个 SFP 千兆光口，冗余电源。2 台。

1）具备接收 API 检测系统对接，收集 API 检测系统相关检测日志和告警。

2）具备 NTP 服务器配置。

3）具备通过对访问流量进行分析，自动发现流量中的 API 资产和敏感接口。

4）具备根据流量特征自动识别 API 类型（如 restful、GraphQL、websocket、MQTT、gRPC、JSON-RPC、XML-RPC、SOAP 等）、API 用途（文件上传、文件下载、登录等）、API 公共组件类型（KAFKA、Elasticsearch、Hadoop、Kubernetes、ClickHouse 等）。

5）具备自定义 API 接口规则，快速、精准的进行 API 接口自动识别、API 接口样式提取和分组。

6）具备通过 API 发现功能，自动将 API 按照域名进行分组管理。也可以根据业务情况手动分组，并指派责任人和部门。

7）具备获取 API 请求响应状态信息，包括但不限于请求成功、客户端请求失败、请求重定向等。

8）具备获取 API 调用行为信息，包括但不限于访问时间、请求类型、访问源、请求/返回报文信息等。

9）具备对 API 访问状态、接口性能、调用行为等信息进行统计和展示。

10） 具备对 API 访问量、访问状态异常的检测与告警，并提供异常访问行为的详细信息。

11） 具备定义 API 调用行为规则，并对异常行为进行检测与告警。

12） 具备对 API 接口的访问行为建立基线。

13） 具备提取 API 访问行为的异常特征，进行威胁建模。

14） 具备 IP 粒度的行为特征模型构建，具备基于 IP 粒度行为特征模型的异常行为检测与告警。

15） 具备异常行为模型应覆盖 API 主要威胁，如：未授权访问、越权访问等。

16） 具备对 API 异常调用行为的安全事件进行分类标注。

17） 具备自定义异常访问行为，具备维度包含访问关系（访问源、目的 IP）、访问时间、具体的业务 API、访问频次、敏感数据访问条数等，以发现深层次潜在异常行为。

18） 具备自动生成 API 威胁事件，可根据时间跨度（天，周，月，自定义）自动关联聚合生成攻击事件，包含攻击事件名称、攻击者、攻击过程、事件

等级、事件描述、攻击结果、处置建议等信息。

19） 具备对 API 敏感数据泄露事件进行告警，包括但不限于大量数据外传、API 接口违规开放到公网导致数据泄露、爬虫批量抓取数据等行为。

20） 具备自动生成 API 敏感数据传输事件，可根据时间跨度（天，周，月，自定义）自动关联聚合生成敏感数据传输事件，包含访问者、访问时间、敏感数据类型、条数、API 访问次数、对应业务系统等信息。

21） 具备全局检索针对不同的用户提供多种检索模式，快捷模式和高级模式，快捷模式中具备预定义数据字段进行快速搜索，高级模式具备分析人员按语法输入查询条件，全局检索按照用户的属于进行数据检索。全局检索有常用检索、历史检索、自定义表头、字段聚合统计、时间轴统计、查看详情等功能。

22） 具备结合 API 历史相关告警、API 标签、API 授权情况等因素综合分析 API 接口存在的风险，并且具备以主机、应用、风险类型、多个维度的展示。

23） 具备以 API，业务应用，访问者、敏感数据类型不同视角进行切换，从不同视角作为切入口进行分析溯源。

24） 具备对 API 安全事件提供详细的信息和相应的安全处置建议。

25） 具备 IP 粒度的 API 安全审计与溯源。

26） 具备基于威胁情报信息辅助的 API 安全审计与溯源。

27） 具备 API 安全事件溯源分析。

28） 具备审计到应用请求的请求状态（成功或失败）、执行时长、请求头、请求体、请求 cookie、响应头、响应体、响应 set-cookie、请求 URL、请求方式、请求参数、会话（token）、用户账号、接口 URL、数据标签、风险规则、风险等级等内容。

29） 具备应用管控日志、应用威胁日志、API 敏感信息日志、业务访问日志、文件传输日志、API 登录行为日志、应用系统日志。

30） 具备还原用户行为记录，利用前沿的异常检测技术，从多个维度来识别异常数据访问行为，并形成最终的风险评分，对高风险行为进行预警。

2、关键业务系统 API 检测系统

API 检测系统具备对业务访问流量经过 API 类型识别、深度 DPI 还原解码、威胁检测、行为异常检测、敏感内容检测等功能，并且具备将 API 安全检测系统产生的业务流量日志、威胁告警日志、敏感信息访问日志等数据上传至 API 分析

平台。

具体参数如下：

1）具备与 API 分析系统对接，并上传相关检测结果，便于分析系统分析。

2）具备旁路镜像部署模式。

3）具备 5Gb/秒的 API 流量以上处理能力。

4）具备自动检测 API 因设计或配置不当等原因产生的安全风险，包括但不限于未鉴权、敏感数据暴露等。

5）具备提供 API 安全风险详细信息及修复建议。

6）具备识别出的 API 安全风险进行分类和威胁等级标注。

7）具备 Web API 漏洞的自动发现能力，包括但不限于命令执行、代码植入、SQL 注入等常见漏洞。

8）具备中间件 API 漏洞的自动发现能力，包括但不限于多种开发语言、框架、中间件、代码库等引入的漏洞。

9）具备对通过 API 接口传输的非结构化数据进行识别与检测，类型包括但不限于图片类（如 webp、bmp、jpeg、png、等）、压缩文件类（RAR、ZIP、7Z、BZ2、TAR 等）、文档类（如 doc、docx、ppt、pptx、xlsx、rtf、wps、et、dps、odt、odp、等）每种类型不少于 3 类。

10） 具备 API 自动聚合，聚合方式参数包括但不限于 ip、ip:port、uuid、sha、md5、时间、日期、时间戳等自动聚合方式。

11） 具备 API 脆弱性检测能力，如未授权、弱口令、明文密码传输、过量数据暴露等能力。

12） 具备 API 攻击检测，攻击检测能力可覆盖 OWASP API security TOP 10 的攻击检测（如代码执行、SQL 注入、命令注入、文件上传等的漏洞利用攻击），通过内置模型可发现接口参数遍历、登录接口爆破、敏感数据批量爬取等 API 风险。

13） 应具有攻击结果研判能力，具备针对发现的攻击事件进行研判，研判结果包括企图、成功、失败等。

14） 具备对 API 安全监测生成对应的日志类型方便分析溯源。如业务访问日志，威胁告警日志，文件传输日志，业务登录日志，涉敏访问日志类日志，具备对各类日志自定义列进行展示，如威胁告警日志包含攻击者、受害者、威胁

分类、威胁名称、攻击结果、攻击链阶段、战术阶段、危害等级等关键字段。具备直接展示威胁详情，包含威胁告警基本信息，威胁描述，威胁危害、解决方案等信息。

15） 具备快速日志检索模式，通过点击具体日志字段可自动带上搜索条件进行快速查询，如点击多个字段，可自动生成与关系的查询条件，通过简单修改条件就可快速查询原始日志。

16） 具备 API 流量交互中敏感信息的识别。

17） 具备 API 请求和响应数据中敏感信息的识别。

18） 具备生成 API 接口与敏感数据映射，显示敏感数据通过 API 接口被访问的情况。

3、关键业务源代码检测系统

源代码检测系统应包含安全管理平台、检测引擎、IDE 插件等相关模块，实现源代码检测任务的统一管理、源代码分析引擎的调度分析、代码审计、报告输出等。

具体参数如下：

硬件规格：不低于标准 2U 机架设备，设备应采用鲲鹏、龙芯、飞腾、海光等自主可控硬件平台，内存≥128G，硬盘≥4T，网络接口：≥2 个 SFP 千兆光口，冗余电源。1 台。

1）满足本次哈尔滨市数字政府新建系统的对于源代码检测技术需求与要求。

2）系统具备 B/S 架构，具备多用户同时使用浏览器访问，具备不低于 4 个检测任务并发执行，检测任务并发数可通过可视化界面配置。具备自定义角色权限。

3）具备实时查看系统运行状态，包括 CPU、内存、硬盘、数据库等信息，引擎内存可通过产品界面配置。

4）具备 C/C++、Objective-C、C#、Java、PHP、Swift、Go、Python、Cobol、Node.js、Kotlin、SQL（Oracle、SQLServer、MySQL、HiveQL 等类型）、Ruby、Scala 等主流编程语言开发的软件源代码的缺陷检测。

5）具备代码注入、跨站脚本、输入验证、危险函数、代码质量、API 误用、密码管理、异常处理等常见安全缺陷问题的检测，二级缺陷类型不低于 2000 个。

6）具备用户对源代码缺陷分析模板的灵活配置，具体到每一个缺陷类型。

7）具备函数白名单功能，检测过程中自动识别白名单函数进行路径裁剪，减少误报。

8）具备文件/文件夹白名单功能，可以对多个文件或文件夹进行过滤，不统计该文件和文件夹下检测的问题结果，提高系统检测精准性。

9）具备根据检测语言类型配置可信数据源，提高检测准确性。可信数据源包括命令行参数、web 表单、json 字符串等，界面可选可信源配置类型应不少于15 种。

10） 具备具备对检测失败的任务重新发起检测，无需重新上传代码。

11） 具备通过产品界面下载单个检测任务的检测日志。

12） 具备检测完成后将检测结果以邮件方式通知到代码相关人，具备任务失败时提醒。

13） 具备任务访问权限控制：可将任务查看权限授予个人或部门。

14） 具备个人凭据统一管理，可页面添加 SSH 私钥、Token 等访问凭据。创建检测任务时，可以选择已有凭据，简化任务创建步骤。

15） 具备配置单个检测任务的回调地址，检测任务结束后，可以主动通知第三方系统检测任务状态和任务摘要信息。

16） 具备对源代码安全扫描结果进行汇总，并按照问题的严重性和可能性进行威胁级别的划分，如高、中、低等多个级别。

17） 具备针对同种类型的安全问题成因路径进行统一展示，便于找到最佳修复节点。

18） 具备迅速定位某一特定源代码安全问题所在源代码行，对问题产生的整个过程进行跟踪。

19） 具备提供中文的源代码安全问题分类、问题描述及修复建议。

20） 具备对当前问题进行审计，修改问题等级以及修改问题状态为是问题、不是问题、遗留问题。

21） 具备记录结果的审计信息，包括人员、时间和审计信息等。

22） 具备对检测结果按照缺陷类型、审计状态、文件名进行过滤查询。

23） 能够对检测结果列表进行全文检索。

24） 具备审计信息携带，能够将上一版本的人工审计信息携带到下一版

本的检测结果中，无需重复审计，降低审计成本。

25） 具备缺陷合并展示：对于文件路径相同，爆发行相同的缺陷进行合并展示。

26） 具备根据任务名称、创建者、开发语言、检测状态、检测开始时间、问题数量等多种条件对源代码检测任务进行查询，针对每一个源代码检测任务能够展现相关信息，如任务名称、开发语言、检测开始时间、检测完成时间、检测状态、问题总数、等级分布以及创建者。

27） 具备根据检测时间、检测方式、任务类型、缺陷等级选择一至多个检测任务进行统计，统计显示各部门任务数、总代码行数、缺陷总数、平均缺陷密度等信息。

28） 具备缺陷类型维度的数据统计，能够展示出现次数最多的 TOP10 缺陷类型及数量。

29） 具备配置缺陷类型集合作为统计分析模板，可以统计指定缺陷类型的检测结果。

30） 检测报告应能够根据用户角色分为概要报告和详细报告。概要报告主要包括问题等级及问题类型等基本统计信息，详细报告除了包括问题等级及问题类型等基本统计信息外，还应包括问题分类、问题描述、修复建议、风险点、问题跟踪信息、审计日志等详细信息。

31） 报告内容应可对问题等级、问题类型、修复建议、跟踪路径、审计日志根据需求进行定制，可提供包括 word、excel、pdf 等多种格式的检测报告。

32） 具备检测任务队列管理，可以通过界面对排队中的任务实行队列置顶、暂停操作，可以删除正在执行的任务。

33） 具备提供系统操作日志，记录用户的关键操作。能够提供系统错误日志，记录关键的错误信息。

34） 具备自定义检测规则功能，自主添加检测规则用于源代码缺陷检测。

35） 具备缺陷知识库在线查看，能够根据缺陷类型、关键词、威胁等级等条件进行搜索，分语言和类型显示该缺陷的等级、详细信息、修复建议和参考信息内容。

36） 具备缺陷知识库维护功能，可上传文件导入检测规则知识库，实现知识库的在线更新。可对任意一条缺陷的威胁等级、详细信息、修复建议进行修

改和重置，同时可以一键重置全部已修改的知识库。

37） 具备系统级数据统计功能，可查看系统使用状况，可展示系统使用的部门数、用户数、激活用户数、月活跃用户数，项目数，源代码数。

38） 具备按照时间段、部门、缺陷审计状态批量导出审计日志表单，表单中提供项目名称、审计人、审计时间、审计前后的缺陷严重等级等详细信息。

39） 具备检测模板管理功能：具备按语言配置检测模板，具备模板的复制、导入、导出功能。

40） 具备系统级日志报告导出功能，可导出和下载指定时间段内的日志报告。

41） 系统具备本地直接发起检测任务，也可以从 SVN、GIT、StarTeam、AzureDevOps、ClearCase 等代码仓库获取代码发起检测任务，同时源代码来源具备 FTP 和共享目录。

42） 具备构建工具集成，如 Maven，Gradle，具备自动获取被测源代码的第三方依赖进行检测。

43） 具备从 VisualStudio、Eclipse、intelliJ 直接发起检测任务并查看检测结果，对结果进行审计。

44） 具备对接 LDAP 用户体系，实现用户的持续同步。

45） 具备中文界面，易操作，具有中文问题描述、修复建议。

四、密码安全建设

（一）基础要求

1、密码应用框架

基于国产密码标准体系和密码管理体系，结合哈尔滨市数字政府建设的实际情况，基于《GB/T 39786-2021 信息系统密码应用基本要求》，建设以保护业务系统的身份认证及数据资产为中心的、自主可控的密码服务体系，通过核心的密码技术、密码模块、密码产品、密码基础设施等产品服务，为网络基础资源、信息设施、计算分析、应用服务、网络通道、接入终端、设备控制等提供身份鉴别、访问控制、机密性、完整性、抗抵赖的密码服务。

2、密码基础服务层

基于各密码产品组成密码基础服务层的主要目的是为上层应用提供密码基础服务支撑，实现上层应用的密码安全增强。在密码基础服务层中，使用符合国家密码法规和标准规定的商用密码算法，使用经过国家密码管理局核准的密码产品，遵循 GB/T39786-2021《信息安全技术 信息系统密码应用基本要求》。密码基础服务层整合服务器密码机、签名验签服务系统、通用统一密码等产品能力，打造服务化、场景化，易于行业快速对接集成的密码服务能力，实现密码基础服务统一、集约化建设，密码服务按需获取，弹性扩展。

3、密码应用层

（1）终端安全密码应用：采用智能密码钥匙解决用户在登录系统和业务操作的身份鉴别，保证了身份的真实性。

（2）网络接入安全密码应用，部署 SSL VPN 安全综合网关，实现终端身份鉴别和数据传输加密保护；在 PC 端部署 VPN 客户端，建立数据安全传输通道。

（3）系统业务安全密码应用，主要为业务应用提供身份验证服务、数据加密服务、完整性验证服务、数据安全存储服务。

（二）具体要求

围绕密码应用相关管理办法中的密码应用要求，综合考虑物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，设计合规、正确、有效的密码服务平台，满足云租户业务系统密码使用需求，需要满足 GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中三级指标的物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全要求。

1. 统一身份认证系统

统一身份认证系统具备身份管理、授权管理、身份发布、认证管理、身份认证、系统管理等多维度认证功能，并且具备适配自主可控、云环境等高适用性。

具体参数如下：

(1)　身份管理，具备 1)组织机构管理。2)人员管理。3)人员分组。4)应用管理。5)应用子账号。6)设备管理。7)设备分组。8)网络资源管理。9)法人管理。10）自然人管理 11)人员属性动态扩展。12）身份敏感数据加密存储。

(2)　授权管理，具备 1）同时具备应用、设备、网络资源的授权管理以及人访问应用、人访问设备、人访问网络资源、应用访问应用服务、设备与网络资源等不同场景的授权管理。2）具备自定义业务授权模板，当人员/设备满足模板

属性时，自动赋予该模板拥有的访问权限。

(3) 身份发布，具备 1)按数据范围、字段范围订阅可发布数据范围。2)身份、权限信息推送。3)身份、权限信息查询。4)服务接口。 5）基于国密算法的数据保护方式为应用系统提供身份数据同步以及基于密码的对接 SDK。

(4) 认证管理：具备 1)用户认证策略控制、认证方式灵活排序、凭证复杂度及更换周期控制。2)应用认证时间/ip 范围控制。3)设备认证策略控制。4)WIFI 接入认证。5)认证互信。6)认证凭证管理。7)票据管理。8）应用二次认证管理。9）具备多 CA 证书认证。

(5) 身份认证：具备 1)同时提供数字证书、短信、用户名/口令、在线扫码、离线扫码、动态码，用户名口令+证书等多种身份认证方式。2)具备二次认证。3）具备 PC 端基于软密码模块的口令+软证书的安全认证方式。4）具备针对不同应用设置不同安全级别认证方式。5）具备自定义认证页面。

(6) 移动端能力：具备 1)具备移动端身份认证、单点登录及接入 SDK。2)具备移动端数字证书申请签发，具备协同签名。3)具备基于 PKI 体系的在线扫码、离线扫码能力。4) 移动 app 用户证书管理。

(7) 具备与数字证书认证系统集成，可在统一身份认证系统中快速进行用户身份数字证书申请、签发，实现用户证书凭证便捷管理。

(8) 具备龙芯系列，鲲鹏系列，飞腾系列自主可控芯片。具备中标麒麟、普华、统信系列操作系统。具备人大金仓、达梦、南大通用系列数据库。

(9) 云环境支持：具备在云环境上安装部署,具备云服务器密码机。

(10) 系统管理：具备 1)三员管理。2)管理员权限管理。3)日志审计管理。4）数据库备份/还原。5）具备多个 CA 证书可信。

(11) 性能要求：1)用户容量:不低于 100 万。2)不低于每秒认证:口令认证：不小于 3000TPS、证书认证：不小于 2000TPS（单机）。

2. 时间戳服务器

时间戳服务器具备时间管理、时间戳证书管理、密钥安全存储、设备管理、访问控制、真随机数生成、日志审计和设备自检等功能。可以满足应用系统的签发时间戳、验证时间戳、同步可信时间的要求。

具体参数如下：

(1) 不低于标准 2U 机架，冗余电源，≥1 个管理口、接口≥4 个

10/100/1000 自适应电口。

(2) 具备管理员、操作员、审计员多级权限控制。具备管理角色登录口令的有效期控制。

(3) 具备多机并行：具备同时有多台服务器密码机为同一台业务服务器提供密码服务，提高处理的效率，防止因一台服务器密码机出现故障导致整个服务终止，提高服务可靠性。

(4) 具备基于 OCSP、LDAP 进行证书有效性验证，也可基于本地证书链、CRL 进行证书有效性验证。

(5) 具备连接白名单：通过连接白名单的支持，实现密码机对应用服务器的授权认证，进一步提高系统的安全性。

(6) 具备网口绑定，提高设备的服务可靠性。

(7) 具备通过管理页面对设备进行在线升级。

(8) 签名(SM2)产生性能：应不低于 12000TPS;验签(SM2)产生性能：应不低于 3400TPS;签戳(SM2)性能：应不低于 2300TPS;验戳(SM2)性能：应不低于3200TPS。

3. USB Key

USBKEY 应具有设备管理、应用管理、容器管理、证书存储、权限控制等功能，具备 SM1、SM2、SM3、SM4、SM7、SM9 等密码算法，密钥在芯片内部产生，私钥无法导出，通过口令验证保证密钥使用者的合法性。

具体参数如下：

(1) 具备 PC 端/服务器端，具备自主可控终端。

(2) 具备商密 SM1/SM2/SM3/SM4 算法。

(3) 具备 ECB/CBC/OFB 等模式。

(4) 具备高速数据流加解密功能。

(5) 具备 WCSP SDK、SKF 接口。

4. 国密堡垒机

国密堡垒机具备对维护过程进行全面跟踪、控制、记录、回放；具备细粒度配置运维人员的访问权限，实时阻断违规、越权的访问行为，同时提供维护人员操作的全过程的记录与报告。

具体参数如下：

(1)　硬件要求：不低于标准 1U 机箱。标配网口：GE 电管理口≥2 个，GE 电业务口≥4 个；硬盘容量≥2T；USB 口：USB2.0≥2 个；串口：RJ45 口≥1 个；电源：单电源。

(2)　性能要求：授权资产≥100 个。硬件性能：并发字符连接数≥100 个。并发图形连接数≥20 个。

(3)　具备用户多角色划分功能，如系统管理员、部门管理员、运维员、审计管理员、密码管理员等，对各类角色需要进行细粒度的权限管理。具备自定义用户权限。

(4)　具备 AD、LDAP、RADIUS、主流认证系统联动登录堡垒机。具备多个 AD 域认证源。具备自动同步 AD/LDAP 用户。

(5)　具备标准化对接 CAS、JWT、SAML2、OAuth2 单点登录认证，且具备配置是否自动创建堡垒机中不存在用户。

(6)　具备设置用户密码的长度、复杂度、相关度和检查历史密码。具备密码过期前告警。具备用户密码错误策略的自定义调整，对用户及来源 IP 进行锁定，防止暴力破解。

(7)　具备认证窗口的全局设置：可以选择启用哪种或者哪几种认证登录窗口。

(8)　具备常用的运维协议：SSH、TELNET、RDP、VNC、FTP、SFTP、rlogin、X11。可通过应用发布的方式进行协议扩展，如数据库 Oracle、MSSQL、MySQL、VMware vSphere Client、浏览器等客户端工具。

(9)　具备自动收集设备 IP、运维协议、端口号、账号、密码、与用户的权限关系，可自动完成授权。

(10)　具备 DB2、Oracle、MySql、SQL Server、PostgreSQL、KingbaseES、DM、GBase8a、GBASE8s 的协议运维代理，可实现自动登录，自动登录可直接调用本地 windows 系统的数据库客户端工具，无需应用发布前置机。

(11)　具备同时对数据库会话记录图形审计及命令提取，并且实现点击任意一条数据库命令，自动跳转到对应的录像片段。

(12)　具备运维人员向管理员申请需要访问的设备，申请时可以选择：设备 IP、设备账户、运维有效期、备注事由等，并且运维工单以邮件方式通知管理员。

(13) 具备密码工单管理，可通过工单申请相应资源的密码，具备通过邮件的方式通知管理员及申请人。具备工单授权到期后的自动密码回收。

(14) 具备多项资产安全的检查，包括主机、主机账户的发现，主机状态和主机账户状态的检查。具备手动、定期和周期性对数据中心内的资产进行整体的扫描检测。

(15) 具备发现自定义网段内未纳管设备的主机 IP、操作系统，同时具备记录该设备发现时间。发现的主机可一键纳管至堡垒机，并可将结果进行导出。

(16) 具备对已纳管的主机进行主机账号扫描，发现主机上未纳管到堡垒机的账号，同时记录相关账号名称、使用协议。发现的账号具备一键纳管至堡垒机中，并可将结果进行导出。

(17) 具备定期自动修改 windows 服务器、网络设备、linux/unix 等目标设备密码功能，且自动改密不借助于 Agent，无需开放 445、135、139 等高危端口。

(18) 具备基于国密算法的动态令牌/USBkey 进行双因子认证。

(19) 具备国密 TLS 双向认证通信，使用国密算法保证 HTTPS 协议层面的数据机密性和完整性。开启后需同时使用具备国密算法的浏览器、国密 USBkey 才能访问堡垒机，只使用国密浏览器无法访问堡垒机，以此种方式对发起连接的客户端身份进行验证。

5. 数字证书认证系统（属于自主可控目录产品，该产品另行采购）

数字证书认证系统具备包括初始化、系统管理、证书模板管理、RA 管理、CA 证书服务、CRL 管理、证书签发、注册审核、系统管理、日志审计和接口服务等。

具体功能如下：

证书签发系统功能：

(1) 具备证书签发功能,具备个人证书、机构证书、设备证书的签发。

(2) 算法具备国密算法 SM1.SM2.SM3.SM4。具备国际算法 RSA1024,SHA1,SHA256。

(3) 系统具备数字证书的签发。具备用户证书更新、撤销、恢复、冻结、解冻等证书全生命周期的操作。

(4) 具备证书制作服务功能：具备修改、删除等证书模板，具备双证书，

包括签名证书和加密证书。

(5) 系统配置管理：具备提供目录服务器地址、端口、连接用户名和口令等相关信息进行配置管理。

(6) 具备数据库备份与恢复，用户可使用系统管理中的系统备份与恢复功能对系统的数据库进行全量备份。

(7) 具备管理员双因子同时认证，其中一种因子为证书方式。

注册审核系统功能：

(1) 证书申请的类型具备个人证书、机构证书、设备证书。具备基于 P10 的证书申请。

(2) 算法具备国密算法 SM2/SM3/SM4，具备国际算法 RSA1024, SHA1,SHA256。

(3) 具备完善的管理手段和管理界面：

1）证书的审核具备自动、手动两种模式。

2）录入证书请求，包括人员证书、设备证书和机构证书，可批量录入请求。

3）下载制证，具备 SKF 类型的 USBKey、TF 卡、贴芯卡等证书介质制作。

4）系统日志查询审计。

5）证书发放数量和情况统计。

(4) 具备证书申请服务的方式：

1）具备离线证书全生命周期维护服务。

2）提供在线证书服务，应用系统可以在线申请制证并进行全生命周期的证书管理。在线接口形态包含 restful 和 webservice。

(5) 具备数据库的备份与恢复，用户可使用系统管理中的系统备份与恢复功能对系统的数据库进行全量备份。

(6) 具备管理员双因子同时认证，其中一种因子为证书方式。

(7) 具备适配第三方合规的证书签发系统，协议包含 GMT0014、spkm。

(8) 具备适配第三方在线证书签发系统。

证书状态查询：

(1) 证书状态离线查询：具备管理员登录系统根据证书序列号、证书内容查询证书的状态。

(2) 证书在线状态查询：具备应用利用 OCSP 协议，在线查询证书状态，

查询结果经过签名后返回并进行证书状态的检验。

互信互任系统：

(1) 具备跨域、跨厂商的证书互信互任。

(2) 具备在线的证书状态查询，接口形态：restful。

(3) 具备接入 CA 数量不少于 20。

(4) 证书状态查询性能：不低于 100 次/秒。

(5) 日志审计：具备提供各种日志的查询功能，供管理员对系统的运行情况进行日志审计。

(6) 具备管理员双因子同时认证，其中一种因子为证书方式。

其他功能要求：

(1) 产品应能够为 SSLVPN 产品发放设备证书。

6. 云服务器密码机（属于自主可控目录产品，该产品另行采购）

云服务器密码机具备对各类密码安全应用系统进行高速的、多任务并行处理的密码运算，可以满足应用系统数据的签名/验证、加密/解密的要求。

具体参数如下：

(1) 不低于标准 2U 机架设备，设备应采用鲲鹏、龙芯、飞腾、海光等自主可控硬件平台。

(2) 网络接口：≥2 个 SFP+万兆光口、≥4 个 10/100/1000 自适应电口、≥1 个管理口，冗余电源。

(3) 具备将密码机虚拟化为多个虚拟密码机(VSM)。

(4) 各 VSM 提供与传统密码机一致的核心密钥管理功能，以及数据加密/解密、数字签名/验证、MAC 的产生/验证、单向散列、对等实体鉴别等密码运算功能。

(5) VSM 自动组成集群，集群内置负载均衡器，集群内数据自动同步，智能发现和智能负载。通过智能化集群提供高可用、弹性伸缩的以及超过单台物理机性能的高性能密码服务。

(6) 可实现创建弹性伸缩的单机 VSM，根据业务繁忙程度对 VSM 的性能进行动态伸缩，充分利用密码资源。也可通过在集群中增减 VSM 进行弹性伸缩。

(7) 具备对称算法：SM1/SM4/3DES/AES。具备非对称算法：SM2/RSA2048。具备杂凑算法：SM3/SHA1/SHA256。

(8) 具备 VSM 用户独立进行密钥管理。

(9) 提供对使用 VSM 的租户管理员进行 USBKey+证书认证、对业务系统进行证书认证的功能。

性能指标如下：

SM1 计算速率不低于 0.6 Gbps。

SM2 签名速率不低于 48,000 次/秒。

SM2 验证速率不低于 37,000 次/秒。

SM3 计算速率不低于 1.5 Gbps。

SM4 加解密速率不低于 1.3 Gbps。

最大并发数不低于 512。

单台设备可创建 VSM 数量不少于 16 个。

7. 签名验签服务器（属于自主可控目录产品，该产品另行采购）

签名眼前服务器具备对各类电子信息数据、电子文档等提供基于数字证书的数字签名服务，并可验证签名数据的真实性和有效性。

具体参数如下：

(1) 不低于标准 2U 机架设备，双电源，接口≥4 个 10/100/1000 自适应电口。

(2) 具备多级权限控制：具备管理员、操作员、审计员多级权限控制。具备管理角色登录口令的有效期控制。

(3) 具备多机并行：具备同时有多台服务器密码机为同一台业务服务器提供密码服务，提高处理的效率，防止因一台服务器密码机出现故障导致整个服务终止，提高服务可靠性。

(4) 具备网口绑定，提高设备的服务可靠性。

(5) 具备通过管理页面对设备进行在线升级。

(6) 具备基于 OCSP、LDAP 进行证书有效性验证，也可基于本地证书链、CRL 进行证书有效性验证。

8. SSL VPN 安全网关（属于自主可控目录产品，该产品另行采购）

SSLVPN 安全网关具备安全的国际标准密码算法套件和符合国密标准的算法套件，保证传输信息的机密性、完整性和有效性，同时提供安全、完善的密钥管理机制，自身具备较强的安全防护能力。

具体参数如下：

(1) 不低于标准 1U 设备，接口≥6 个 10/100/1000BASE-T 接口，≥4 个 SFP 接口，冗余电源。

(2) 符合国密局制定的《SSL VPN 技术规范》，具备国家商用密码算法 SM2/3/4。

(3) 部署模式具备单臂模式、双臂模式。

(4) 采用国家密码管理局鉴定的硬件随机数产生器。

(5) 产品密码芯片、主板、板卡，从设计、研发、生产所有环节全自主实现，具有自主知识产权。

(6) 具备管理员分权管理，不同管理员管理不同的功能模块，可新建管理员。

(7) 具备多种认证方式，口令、证书、短信、AD、终端绑定等。

(8) 具备基于标准 SSL 的加密通道，具备应用代理、VPN 隧道多种代理方式，能有效地具备 IP 层及以上应用协议数据保护。

(9) 具备接口模式的应用系统单点登录，在 SSLVPN 客户端认证通过后，应用系统调用客户端 SDK 接口获取经过签名计算后的用户身份令牌，再通过 SSLVPN 的 WebService 接口验证身份令牌的合法性，并获取用户身份详细信息。

(10) 客户端具备自主可控操作系统，龙芯平台麒麟系统、兆芯中标麒麟系统、飞腾银河麒麟系统。

(11) 具备统一的浏览器扩展接口、具备 IE、Firefox、Chrome、Windows Edge。

(12) 加密吞吐能力≥220Mbps。最大每秒新建 SSL 连接数≥600 个。最大 SSL 并发连接数 50000。

9. 密钥管理系统（属于自主可控目录产品，该产品另行采购）

密钥管理系统具备为证书认证系统提供密钥。该密钥管理系统提供了对生命周期内的密钥对进行全过程管理的功能，包括密钥生成、密钥存储、密钥分发、密钥备份、密钥更新、密钥撤销、密钥归档、密钥恢复以及安全管理等。

具体参数如下：

(1) 不低于 2U 机架，接口：≥4 个 10/100/1000 自适应电口、≥1 个管理口。

(2) 应适配主流自主可控平台，功能丰富，具备 SM1/2/4/9 商用密码算法相关规范。符合 GM/T 0014—2012 数字证书认证系统密码协议规范。符合 GM/T 0038—2014 证书认证密钥管理系统检测规范。符合 GM/T 0051—2016 密码设备管理 对称密钥管理技术规范。具备 GM/T 0044-2016 SM9 标识密码算法。

(3) 具备自主可控平台，全面适配自主可控。

(4) 具备 SM9 标识密钥管理。

(5) 具备级联密钥管理系统。

(6) 具备密钥模板管理，具备快捷、灵活的自定义密钥模板，并可基于密钥模板创建密钥。

(7) 具备具备三员管理，可配置用户权限。

(8) 具备服务使用者采用基于 HTTPS 协议的密钥管理接口、《GMT 0034-2014 基于 SM2 密码算法的证书认证系统密码及其相关安全技术规范》、符合《GM/T 0051—2016 密码设备管理 对称密钥管理技术规范》的管理协议。

(9) 具备基于证书 CA 系统应用的国密标准接口。具备基于对称密钥管理的国密标准接口。具备基于国密安全通道的自定义密钥管理的 REST 协议接口。

(10) 具备对称秘钥管理：密钥生命周期在线管理。密钥生命周期离线管理。密钥产生、密钥分发、密钥启用、密钥更新、密钥撤消、密钥恢复、密钥归档、密钥备份恢复。

(11) 具备非对称秘钥管理：具备密钥预生成策略管理。对外提供国密标准的密钥管理服务。具备多种协议的 API 管理接口。

10. 安全电子签章系统（属于自主可控目录产品，该产品另行采购）

安全电子签章系统应符合 GM/T 0031-2014《安全电子签章密码技术规范》和 GM/T 0047-2016《安全电子签章密码检测规范》要求，应采用标准的电子印章和电子签章编码格式以及验证规范。应具有人员管理、电子印章管理、电子印章生成和下载、日志审计和设备自检等功能。可满足应用系统的签署电子印章、验证电子签章有效性的要求。

(1) 应可制作签发符合规范要求的电子印章;制作过程具有注册、注册审核、签发审核、印章签发、印章发放的业务流程;电子印章分域申请、分权审批;具备电子印章状态的签发及发布;具备电子印章状态撤销列表的签发及发布。

(2) 具备电子印冻结功能。具备电子印解冻功能。具备电子印撤销功能。

(3) 具备提供 GB/33481-2016 定义的 OES 接口。

(4) 具备对客户端进行集中配置，统一下发配置参数。

(5) 具备支撑统一下发电子印章验证数据、数字证书验证数据等。

(6) 具备登录系统具备基于密码的认证方式。

(7) 具备使用密码技术对制章数据进行防篡改。

(8) 具备使用通过认证的密码模块或设备提供密码能力。

(9) 具备为业务系统提供用章申请服务接口，实现在线用章申请。

(10) 具备用章业务审批，用章审批人对用章申请进行统一审批，有效管控电子印章的使用。

(11) 具备为业务系统提供在线验证服务接口。

(12) 具备验证电子文件中的电子签章和数字签名、电子签章数据、电子印章数据、数字证书数据等。

(13) 具备具有多 CA 接入能力，能够和多种 CA 同时对接，实现不同 CA 体系之间的证书互验。

五、服务体系建设

需建设安全服务体系，不少于 4 人具备专业资质的人员驻场 3 年，提供软件开发、安全管理、资产管理服务、互联网暴露面检测服务、威胁情报服务、协助加固服务、网站安全防护服务、重要时期安全保障、应急响应服务等。

（一）基础要求

1、预测能力建设

预测能力建设包括:资产管理服务、互联网暴露面检测服务和威胁情报服务。

（1）资产管理服务

资产管理服务应当包括：资产发现与管理服务、资产发现与管理实现方法、资产发现周期要求、资产发现运营组件、资产发现技术、资产与人员对应和服务输出等部分。

资产发现与管理服务：通过摸清建设现状，了解当前系统存在的主要问题，制定运营服务方案。通过摸清网络拓扑，梳理边界防护重点，制定流量监测方案。通过梳理 IT 资产，对 IT 资产进行业务分类、重要性分级。

资产发现与管理实现方法：通过安全运营中心的资产测绘技术，完成互联网暴露面资产测绘和内网的资产扫描。资产发现与管理主要通过下列几步实现：原有台账整理、部门自主上报、交叉扫描探测、核心资产筛选、制度落地、定期检查等步骤。

资产发现周期要求:资产发现需具备灵活的资产探测周期设置,可以选择“单次探测”、“天”、“周”和“月”等条件进行探测。常态化至少每月执行一次，特殊情况下至少每周执行一次。

资产发现运营组件：云端通过探测技术手段，实现对全网状态实时监测、高风险资产预先发现，以多维度的测绘应提供“全面”、“快速”、“精准”的互联网暴露面资产管理能力。本地部署安全运营一体机，安全运营一体机内置多种资产测绘引擎，如 Nmap、Goby、Finger 等，对内部数字资产进行快速的发现与识别。

资产发现技术应包括：根据域名探测搜索、web 资产探索、根据单位名称关键字探索、根据 IP 段进行探索和资产指纹识别等部分。

资产与人员对应:通过前期资产发现工作,结合哈尔滨市组织和人员的梳理,将资产与归属人关联起来，打通归属单位、归属个人、资产、风险的关系。

服务输出：《哈尔滨市资产台账》包括上述服务内容信息，以及各单位对应情况。

（2）互联网暴露面检测服务

互联网暴露面服务,从攻击者视角自动对资产周期性监控并对互联网资产暴露面的边界梳理，对互联网暴露面资产梳理开展一次“大体检”，摸清互联网资产底数，实时感知网络资产的安全态势，协助将盲区资产进行精准管控，通过访问控制、关闭互联网访问、减少高危端口等手段，减少不需要的暴露面减低入侵风险，也满足内部自查、上级核查和行业普查的安全需求。

服务目标：在网络入侵的起始阶段，黑客会在前期针对目标单位、以及目标子单位进行全面的信息搜集如：子域名、C 段、C 段开放资产及服务、Web 组件、Web 中间件应用、组织架构、备案信息、邮箱信息、通过前期进行资产发现，黑客会优先选择薄弱的资产或者社工的方式利用漏洞直接获取相关应用/终端的权限。

服务流程：暴露面检测服务起始前，会通过填写调研表的方式，获取互联网资产的部分信息，调研其根域名、IP 段、关键字等信息。服务人员会将相关信息输入到检测工具中，自动化对互联网资产排查，最终输出结果包括但不限于子域名、c 段、服务、邮箱、 敏感信息、WAF 指纹、红队高关注的 CMS 指纹等资产等敏感信息。在摸清资产底数之后，基于资产进行其风险识别。通过互联网暴露面检测、漏洞检测、弱口令检查、高危端口、影子资产、不活跃资产检查等技术手段，发现系统存在的所有可能被利用的攻击面。攻击面包含被入侵的所有路径，对攻击面的防御是有效防御攻击的唯一方法。哈尔滨市政务云上攻击面众多，互联网暴露面、弱口令、Web 漏洞、中间件漏洞、系统漏洞、高危端口等容易被利用的攻击面较多，对攻击面的治理亟需展开。

服务输出：《互联网暴露面服务报告》报告包括但不限于子域名、IP 段、服务、邮箱信息、组织等敏感信息。

（3）威胁情报服务

服务范围：威胁情报服务为提供权威、及时、准确的安全风险通告，第一时间将相关风险知会相关单位，并提供专业的解决建议。服务覆盖以下场景：漏洞场景：覆盖 CPU 处理器、网络设备、操作系统、虚拟化、容器、数据库、开发语言、中间件、应用组件等上百款软硬件产品的官方安全公告。

服务内容：威胁情报服务以服务包的方式进行订阅。情报服务内容包括提供最新安全漏洞、威胁（0day、系统漏洞、网络攻击），以及相关问题的详情及解决办法或处置建议。

服务方式：通过安全运营情报平台推送经安全运营中心研判后的常规漏洞风险提示供相关单位排查和处置。通过邮件订阅的方式第一时间为相关单位推送最新高危安全漏洞的预警通告，包括漏洞简介、影响范围、处置建议等。

服务流程：情报监测，通过应急响应中心、威胁情报中心、研究院、GreatMessage 平台对主流软件、系统、设备的安全漏洞等情报进行实时监测。威胁分析：经验丰富的安全专家分析产生安全漏洞/事件的原因、受影响的范围、并给出合适的解决建议。威胁研判：根据对威胁的分析，由安全专家对相关情报进行研判。威胁预警：针对常规漏洞类情报经专家研判后通过安全运营情报平台下发，重要安全漏洞经专家研判后输出安全漏洞预警报告。情报闭环，推动一线

安服、驻场工程师协助相关单位处置相关风险，完成情报的闭环。

服务输出：安全研究团队严格按照信息安全服务的流程，在服务期内，以严谨、认真、负责的态度对待每一位相关单位。对相关漏洞分析、研判后，形成《信息高危漏洞风险提示》服务报告。《信息高危漏洞风险提示》，相关漏洞爆发后第一时间推送相关单位，一年不少于 50 份。

2、防御能力建设

（1）协助加固服务

服务内容：根据整体评估测试结果，针对所发现的安全漏洞及安全风险，提出可操作性强、效果佳的整改建议，并协助所需要的单位完成安全整改。还应该包括：设备层面加固、系统层面加固、应用层面加固。

服务流程应包括：信息收集、系统备份、系统协助加固、应急恢复内容。

服务方式：采用远程或现场的方式协助所需要的单位完成对信息系统的整改工作。

服务输出：出具《安全加固方案》后，描述存在的安全问题和整改措施。协助所需要的单位完成安全整改。

（2）网站安全防护服务

1.网站防护服务采用云端 SaaS 化方式部署，无需占用本地计算资源。

2.具备通过统一界面展示网站访问次数、拦截攻击次数、网站出入总流量、疑似攻击元 IP 数量，并以时间维度展示攻击与访问趋势图。

3.具备通过服务平台以手工导入和批量导入的方式完成防护站点的添加申请，具备添加 HTTP 和 HTTPS 类型的站点，并具备自主上传网站公钥或和私钥。

4.具备 HTTP 强制跳转 HTTPS，当用户访问 HTTP 端口（如 80）时，具备强制将访问牵引至 HTTPS 端口（如 443）。

5.具备区域访问控制，限制国外用户或者国内以市为最低行政单位的区域进行访问控制。

6.具备检查提交的报文是否符合 HTTP 协议框架，如异常的请求方法、特殊字符、重点字段的缺失、超长报文造成的溢出攻击以及对高危文件的访问等。

7.具备对 HTTP 协议合法性进行验证，提供 HTTP 协议防护功能，具备对 HTTP 协议的 URI、HOST、UA、Cookie、Referer、Content、Accept、Range、其他头

部和参数在内的元素、参数进行检测与处理。且具备非法编码和解码的灵活控制与处理。

8.具备针对主流 Web 服务器及插件的已知漏洞防护。Web 服务器应覆盖主流服务器：apache、tomcat、lightpd、NGINX、IIS 等。

9.具备对用户上传的文件后缀名和文件内容进行全方面检查，杜绝 Webshell 的上传和访问。

10.具备流量监测的功能，基于用户的访问记录，实时检查被访问页面的安全状况，能够发现更深层次的暗链、Webshell 等安全事件。

11.具备提供攻击防护安全策略，具备对命令注入（包括 SQL 注入、SQL 盲注、代码注入等）、跨站脚本、SSI 指令、路径穿越、远程文件包含、WebShell 防护。

云安全防护全国的云防护节点可对黑客发起的注入、跨站、网页木马、扫描器、组件 0day 攻击、盗链等攻击进行防护，然后将正常流量转发到源站服务器。

服务内容应包括：网站防护、CDN 加速、防 DDOS、CC 攻击、永久在线、可视化防护、用户数据报表内容。

服务流程应包括:域名登记、配置防护、DNS 映射、验证网站。

服务输出：网站管理单位可访问云防护管理站点查看被防护站点的访问流量报表、安全防护报表，安全防护报表包含攻击次数态势分析、攻击者区域态势分析、攻击者 IP 统计、被攻击页面统计、被攻击域名统计、攻击事件统计、攻击威胁等级统计等报表。

（3）重要时期安全保障

服务目标：切实做好市内单位重大活动网络信息安全保障工作，全面排查关键信息基础设施和重要信息系统安全保护状况，摸清网络安全风险，堵塞网络安全漏洞，落实网络安全责任，深入贯彻落实国家网络安全等级保护制度，全面提升网络安全保障能力和防护水平，确保重大活动期间网络与信息系统安全可靠。

服务范围：在国家重大活动、重大节日、护网行动等期间，针对用户重要 IT 系统资产、包括主机、网络、应用等系统运行维护场景开展网络安全保障工作。

服务方法：

1）重保时期安全服务

包括但不限于：网络资产探测、网络安全检测评估和弱口令&默认口令。

2）供应链安全检查

为提升关键信息基础设施安全防范能力和水平，关基单位要具备软件供应链风险识别、持续检测、及时响应的能力；针对关键信息基础设施、重要网络和大数据提出服务和产品的供应链企业，需要建立健全详细的供供应链产品和企业清单，加强对供应链产品和企业的安全管理要求。

应包括：供应链产品检查、供应链企业检查、开源组建安全检查。

3）供应链安全风险管理自查服务

参照《运营者供应链安全管理风险自查表》对供应链安全管理制度、产品安全检查、开发安全流程管理、交付安全管理等进行自查，针对性地完善供应链安全管理制度，加强安全管控、化解安全风险。

协助安全加固服务：

信息安全加固工作是指：在风险评估、渗透测试、安全检测等技术评估之后，根据评估检测过程发现的中、高危级别漏洞，强化信息系统安全防范能力的重要过程。参考当前网络和系统现状，为信息安全架构的改进或升级提出切实可行的解决方案，跟进漏洞的整改情况并提供复测，直至按要求完成加固。在协助实施的同时，提高网络的安全性，提高每一个信息主体的抵抗安全风险的能力。信息系统的加固包括但不限于：系统加固、网络设备加固和应用系统加固。

重保时期值守服务应包括但不限于：威胁情报共享、安全监测值守、安全分析研判、应急响应处置、红蓝队检测服务和安全专家支持。

（4）紧急响应服务

当信息系统遇到突发的安全问题如：发生网络入侵事件、大规模病毒爆发、遭受拒绝服务攻击等，在收到的应急响应服务请求信息后，应急小组根据需求，以远程或现场的方式协助及相关人员查明安全事件原因，确定安全事件的威胁和破坏的严重程度。并根据对事件的分析及原因提供相应的解决方案。方案应该包括但不限于：事件初期、应急支撑实施及输出报告与汇报。

（5）驻场安全服务

需派出专业技术人员前往需要值守单位现场，对该网络环境进行长期的网络

安全维护与防范工作，确保单位内日常的网络安全使用以及安全产品的维护。

安全设备巡检服务：定期查看安全设备的运行状态、设备负载等是否正常；检查设备存放环境是否符合标准；对设备的版本进行检查，判断升级必要性；梳理分析设备的策略，清理过期无效策略，给出优化建议；此外还查看安全设备是否过维保期等一系列的安全检查操作。

安全日志分析：通过大数据分析平台或其他安全设备，提取日志数据进行人工安全分析，对系统遭受到的攻击方式、频率、防御有效性等方面进行数据分析总结参考。通过分析安全设备日志，包括操作系统日志及 access log 访问日志、WAF 日志、HIDS 日志等，其中操作系统日志及 access log 访问日志，这两种日志对于安全工作来说至关重要，通过分析操作系统安全日志，可以得出当前主机中正在执行的命令，当前主机登陆的用户，登陆操作的 IP 地址等信息，初步处理后，设置相应的检测规则及告警规则，能够检测主机异常行为，如爆破、执行威胁命令等动作；在不同的公司或者网络环境，access log 中包含有正常用户及异常用户的网页请求访问日志，处理 access log 访问日志，并设置相应的检测、告警规则，可发现针对 WEB 的攻击行为，如 SQL 注入、XSS、文件包含、通用扫描器行为等。

终端安全保障服务：提供接入终端安全保障服务，当接入终端出现感染病毒、恶意进程、恶意攻击、恶意行为等安全事件时确定终端安全事件的威胁和破坏的严重程度，及时进行处置。

3、服务输出

前期梳理工作得出《安全梳理与整改细则》。

在重保实时提供《重要时期保障日报》，以及提供重要保障结束后提供总结报告。

（二）具体要求

1、服务目标

通过构建安全运营服务机制，提升主动监测和防御能力，实现对安全威胁的提前感知与监测预防，对正在发生安全事件的实时防御和响应处置，对潜在安全威胁的持续主动挖掘，对已发生安全事件的分析溯源，在监测响应的过程中结合实际业务情况动态优化调整安全设备策略，最大化实现现有安全设备联防联动，

并通过通报预警机制确保通告及时、处置有效、责任到人，最终实现“看得见、用得好、管得住”的安全目标。

2、服务内容及期限

本项目服务范围为网络安全技术具备服务，服务期限计划从服务期开始，共计提供36个月服务期限，服务主要内容包含：

（1）36个月4人团队规模的安全运营服务。

（2）服务期限内对于突发网络安全事件应急处理支持。

（3）动态优化安全防护规则：根据事实安全事态调整及网络安全态势感知平台等研发后的新增功能，为实现云安全防护体系的高效、稳定运行，由专业驻场工程师持续、动态优化堡垒机、数据库审计、应用防火墙、边界防火墙等安全设备防护策略；同时每季度对信息系统进行漏洞扫描，协助加固整改；

（4）重要活动期间安全保障及资讯服务。重要保障活动期间，对管理信息大区重要业务系统、业务环境、开发测试环境等涉及网络安全的区域进行重点排查、监测与防护；结合国家网络安全宣传周等重大宣传活动提供相关资讯及意识提醒报告服务。

2、服务团队要求

（1）安全服务团队应保证 100%的团队成员熟悉我方的相关安全管理规范和业务流程。

（2）安全服务团队需配备服务负责人1人，硕士及以上学历，15年及以上工作经验，同时具备有效期内的信息系统项目管理师高级、ISO 27001主任审核员认证、网络与信息安全管理员三级、CCSK、国际注册内部控制师（CICS)、CISP认证；同时安全服务团队成员均同时具备CISP、CISAW（渗透测试）证书。

3、服务团队说明

应答方应说明对安全服务项目的具备队伍情况，服务模式，并按照下列表格格式提供详细的人员配置表（工程界面划分及项目岗位职责及配置情况表）。

项目管理人员

姓名	职务	获取资质	工作年限	工作职责

项目组成员

序号	姓名	职务	获取资质	安全领域工作年限	本项目中的职责
1					
2					
3					
4					

4、服务承诺要求

应答方应对服务质量、服务进度、资源配置、保密义务以及售后服务做出实质承诺。

5、服务能力要求

（1）驻场安全运营服务

1、建立资产台账，定期梳理资产清单；

2、完善和记录资产属性和指纹信息；

3、识别资产之间的关联关联，绘制资产关系图谱；

4、根据具体的评估对象和安全要求对资产进行分类分级；

5、根据资产的保密性、完整性和可用等安全属性等级对资产价值进行赋值。

6、漏洞检测：使用漏洞扫描工具对服务范围内各种软硬件设备进行全面扫描与分析，扫描设备检测规则库及知识库应涵盖 CVE、CNCVE、CNVD、CNNVD 等标准。扫描完成后并人工验证所发现的漏洞，并针对漏洞扫描中出现的问题，提供解决方案。

7、漏洞跟踪处理：定期漏洞检测完成后，技术人员编写安全漏洞报告和修复建议，将安全漏洞发布给相关责任人员，由其进行整改，并跟踪处理过程和处理状态（已处理待验证、已处理验证通过、已处理但需要重新整改、未处理、处理中等），需要时，对处理状态进行统计分析。

8、督促漏洞整改：对于超出协议规定时间期限的漏洞，服务团队协助同客户安全团队人员，督促网络、主机或应用团队人员进行整改。

9、日志关联分析：基于安全运营管理平台对网络流量、设备日志、系统日志、安全日志等关键信息进行统一采集和日志规范化，收到事件告警后，结合关联报文上下方和威胁情报进行快速研判，甄别策略告警误报，锁定和标记真实网

络攻击，将安全事件告警通知运营处置人员及用户相关责任人。

10、威胁协同处置：收到安全事件告警后，与业务部门、运维部门进行联合评判，根据事件影响、处置建议、业务属性制定对应的应急处置方案，并在安全运营管理平台记录事件的处置过程，直至事件的闭环解决。

11、安全通告服务内容包括提供最新安全漏洞、威胁(0day、系统漏洞、网络攻击)、黑灰产情报、暗网、安全厂商、互联网侧的资产暴露面，以及相关问题的详情及解决办法或处置建议。

（2）重要时期安全保障

在国家重大活动、重大节日、护网行动等期间，针对重要 IT 系统资产、包括主机、网络、应用等系统运行维护场景开展网络安全保障工作。及时发现存在的资产安全和漏洞风险，提供专业的安全架构设计和安全风险修复建议并进行处置；完成重要时期保障中防护工作，包括排班值守，安全监测，对发生的信息安全攻击事件进行应急响应，重要时期安全保障时期提供 7*24 小时现场具备保障服务，发现风险快速定位、快速处置，响应、分析和处置。

（3）应急响应与处置服务

安全技术人员在遇到突发事件后所采取的紧急措施和行动，恢复业务到正常服务状态；调查安全事件发生的原因，在需要司法机关介入时，提供法律认可的数字证据，避免同类安全事件再次发生。应急响应与处置服务内容包括：应急响应启动、应急响应处置、复盘总结。

（4）服务工具要求

威胁分析工具

1）需具备自主知识产权的威胁分析工具可按威胁程度等级展示文件样本 MD5、威胁指数、传播次数，病毒检测、静态检测和动态检测结果等内容。

2）可根据文件传播情况分析受感染主机、接受云端威胁情报、关键威胁行为可视化、回连主机 host 和完整沙箱分析报告。

3）可具备沙箱逃逸检测，当恶意文件进行逃逸尝试，在沙箱报告中进行体现。

4）可动态执行可疑文件，分析代码的注册表、进程、网络、文件等行为，分析其安全风险。

安全服务工具 1）具备自主知识产权的 Web 扫描工具，且参与过 web 应用安全扫描标准的制定。 2）具备自主知识产权的数据库扫描工具，且参与过数据库扫描产品安全标准的制定。 3）具备自主知识产权的网络安全事件应急处置专用工具。

（九）其他

具体技术（参数）要求
一、信息系统等级保护测评 按照《中华人民共和国网络安全法》，建设验收前需要完成信息系统三级等级保护测评。 二、商用密码应用安全性评估 根据《商用密码应用安全性评估管理办法（试行）》第三条与第十条规定，关键信息基础设施、网络安全等级保护第三级及以上信息系统。建设验收前需要完成商用密码应用安全性评估。 三、风险评估 根据《全国一体化政务服务平台网络安全管理办法（试行）》第十八条规定，政务信息系统应开展安全风险评估工作。建设验收前需要完成一次风险评估。